Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunkingwith the Avaya Communication Server 1000 release 7.0 and ACME Packet Net-Net 3800 Session Border Controller Release 6.2 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of the Avaya Communication Server 1000 release 7.0and the Windstream SIP Trunking. The ACME Net-Net 3800 Session Border Controller is used as IP-IP network border between service providers to control security and interactive communications among multimedia and data services.

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.

1. Introduction

This document provides a typical network configuration deployment of the Avaya Communication Server 1000 and the Windstream SIP Trunking service Voice & Data bundle (hereafter referred to as Windstream system or Metaswitch).The ACME Net-Net 3800 Session Border Controller is used as IP-IP network border between Windstream Metaswitch and Avaya Communication Server 1000.

2. General Test Approach and Test Results

The Avaya Communication Server 1000system was connected to the ACME Net-Net 3800 via the Network Routing Service/SIP Proxy Server (NRS/SPS). Then the Net-Net3800 was connected to the Windstream system via SIP. Various call types were made from the Communication Server 1000to the Windstream system and vice versa to verify the interoperability.

2.1. Interoperability Compliance Testing

The focus of this testing is to verify thatCommunication Server1000 can interoperate with the Windstream system. The following interoperability areas were covered:

- General call processing between Communication Server1000 and Windstream systems including:
  - Codec/ptime(G.711 u-law / 20ms)
  - Hold/Retrieve on both ends
  - CLID displayed
  - Ring-back tone
  - Speech path
  - Dialing plan support
  - Advanced features (Call on Mute, Call Park, Call Waiting)
  - Abandoned Call
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends
- Fax/Modem Pass Through is supported only with G.711
- DTMF in both directions
- SIP Transport UDP
- Thru dialing via the Communication Server1000 Call Pilot
- Voice Mail Server CallPilot(hosted on Avaya system)
- Early Media Transmission

The following assumptions were made for this lab test configuration:

1. Communication Server1000 R7.0 software and implementation oflatest patches

2. Windstream provides support to setup, configure and troubleshoot on carrier switch during testing execution.

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

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window were open during the test cases execution for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path was checked before and after calls were put on/off hold from each end.
9. Applicable files were screened on an hourly basis during the testing for message that may indicate technical issues. This refers to Avaya Communication Server files.
10. Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

2.2. Test Results

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

1. Call is made from Communication Server 1000 phone to a PSTN phone with CLID (Caller Identification) hidden. The call is being rejected with SIP error code 403 (URI not recognized) by the Windstream system (namely Metaswitch). Windstream team is investigating and providing the resolution.
2. Incoming calls from PSTN to Communication Server 1000, CLID number works intermittently. Windstream team is investigating and providing the resolution.
3. Call is made from Communication Server 1000 phone to a PSTN phone with CPND (call party name display) hidden. The call is established with 2 way speech path but the PSTN phone did not display the correct CPND of the caller. SIP Field Privacy is send ID, Metaswitch interprets as CPND private and sends. This is a design intended from Metaswitch.
4. Call is made from a PSTN phone to a Communication Server 1000 phone, which is set Call Forward No Answer to Voicemail.There is about 20-40% of early media greeting from Voicemail system being lost. The Windstream team is investigating.
5. Toll free number was not tested due to the Windstream lab environment does not provide this service.
6. The directory search number 411 service is tested with Windstream emulated 411 number where Communication Server 1000 sends and Windstream terminated as an assign mailbox number.

7. 911 emergency service is tested with Windstream emulated 911 number where Communication Server 1000 sends and Winstream terminated as an assign mailbox number.
8. Call from Communication Server 1000 phone that is programmed to reach PSTN Operator 0. This is not tested since Windstream lab environment does not have this service available.
9. Call from Communication Server 1000 phone that is programmed to reach PSTN Operator 0+10-digits. This is not applicable for Windstream, operator services are reached via Long Distance number 1-xxx-555-1212 to the area code you are wishing to lookup.
10. Communication Server 1000 phone holds/ retrieves a call will cause CLIDnot to work properly. This is a Communication Server 1000 known issue and has no plan to implement this feature.
11. PSTN1 phone calls to Communication Server 1000 phone, then phone does blind transfer to PSTN2 phone. PSTN 1 phone could not hear ringback tone from PSTN2 phone when Communication Server 1000 phone completed blind transfer. This is a limitation on Windstream because the system does not support UPDATE SIP message.

It was agreed that with Windstream that the above observations were not severe enough to fail the testing.

2.3. Support

For technical support on Windstream system, please contact Windstream technical support at:

- Toll Free: 1-800-843-9214
- http://www.windstreambusiness.com/support-center.html

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between the Communication Server 1000 and Windstream System.
For confidentiality and privacy purposes, actual public IP addresses used in this testing had been masked out and replaced with imaginary IP addresses throughout the document.

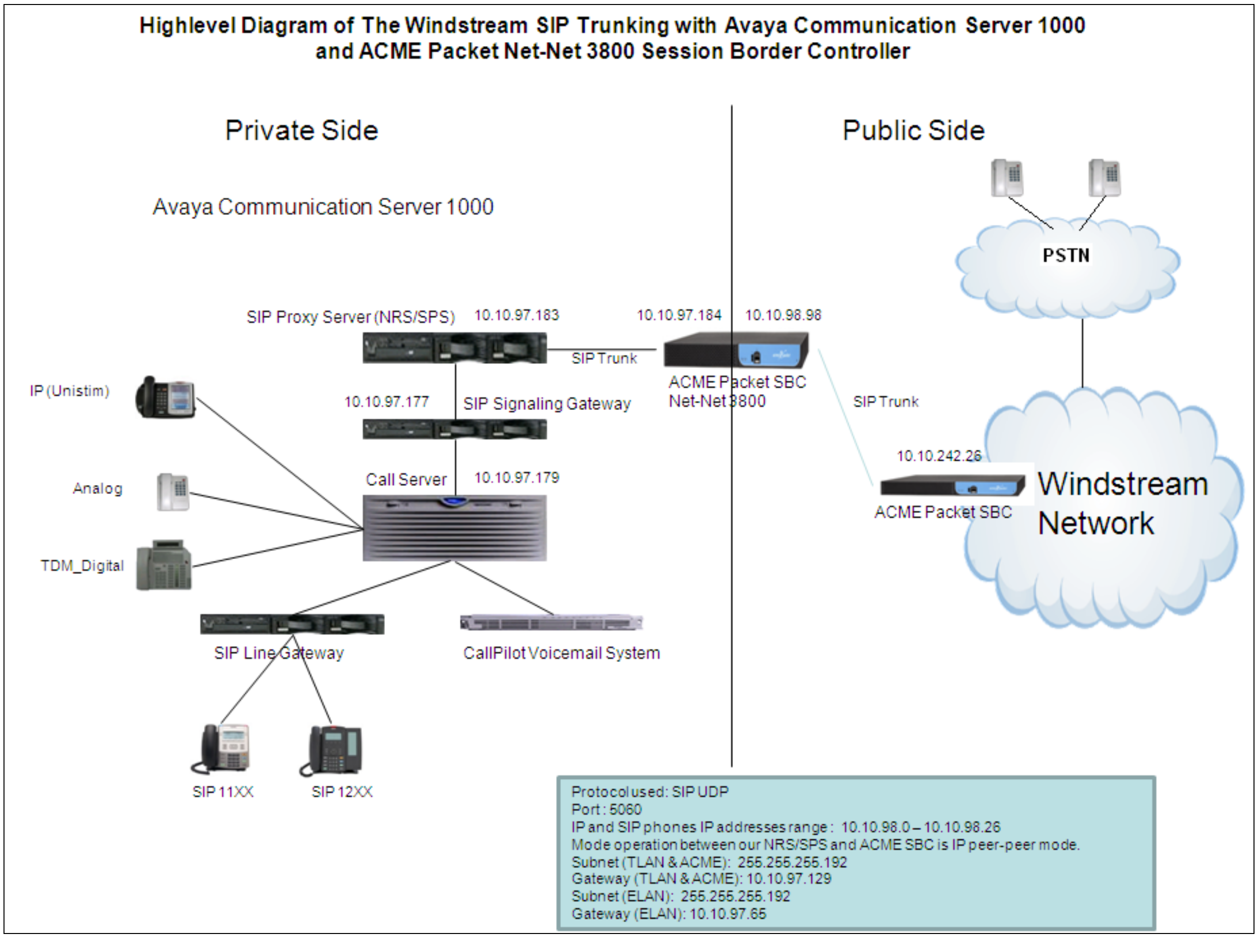

Figure 1- Network diagram for Avaya Communication Server 1000 and Windstream System

4. Equipment and Software Validated

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

Avaya system:

System	Software/Loadware version
Avaya Communication Server 1000 7.0 (CPPM)	• Call Server: 700 Q+ GA • Signaling Server: 7.00.20 GA • SIP Line Server: 7.00.20 GA • NRS/SPS Server: 7.00.20 GA
Avaya phones	• 2002 p2: 0604DCN (Unistim) • 1140: 0625C8D (Unistim) • 1120: 0624C8D (Unistim) • 2007: 0621C8D (Unistim) • 1120: 4 1 13 0 (SIPLine)
ACME Net-Net 3800	• Firmware SCX6.2.0 MR-4 Patch 3 (Build 754)

Windstream system:

System	Software/Loadware version
Metaswitch	• Call Feature Server: 7.1.01-B48 P90.41 • Universal Media Gateway: 7.1.01-SU64 P86.00 • Element Management System: 7.3.00-SU16 P86.00

Additional software and patch lineup for the configuration and active patch list on the SIP Signalling Gateway are listed as below:

Call Server: 7.00 Q+GA plus latest DEPLIST – Deplists_CPL_X21_07_00Q.zip
SSG Server:7.00.20 GA plus latest DEPLIST –Service_Pack_Linux_7.00.20_20110503.ntl
SLG Server:7.00.20 GA plus latest DEPLIST –Service_Pack_Linux_7.00.20_20110503.ntl
NRS Server: 7.00.20 GA plus latest DEPLIST –Service_Pack_Linux_7.00.20_20110503.ntl

5. Avaya Communication Server 1000 Configuration

These Application Notes used the Incoming Digit Translation feature to receive the calls and used the Numbering Plan Area Code (NPA), Special Number (SPN) features to route calls from the Avaya Communication Server 1000, over the Windstream SIP trunk to PSTN.
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 9**
The below proceduresdescribe the configuration details of Communication Server 1000 with a SIP trunk to the Windstream system.

5.1. Login to Communication Server 1000 System

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

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

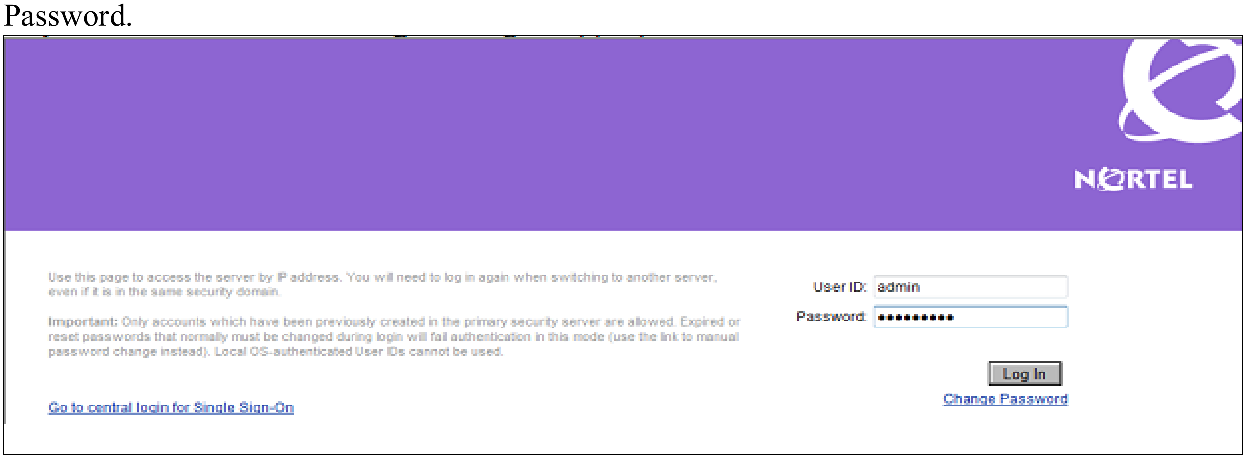

Figure 2 – Login Unified Communications Management

b) The **Unified Communications Management**screen is displayed. Click on the **Element Name** of the Communication Server 1000 Element as highlighted in red box as shown in **Figure 3**.

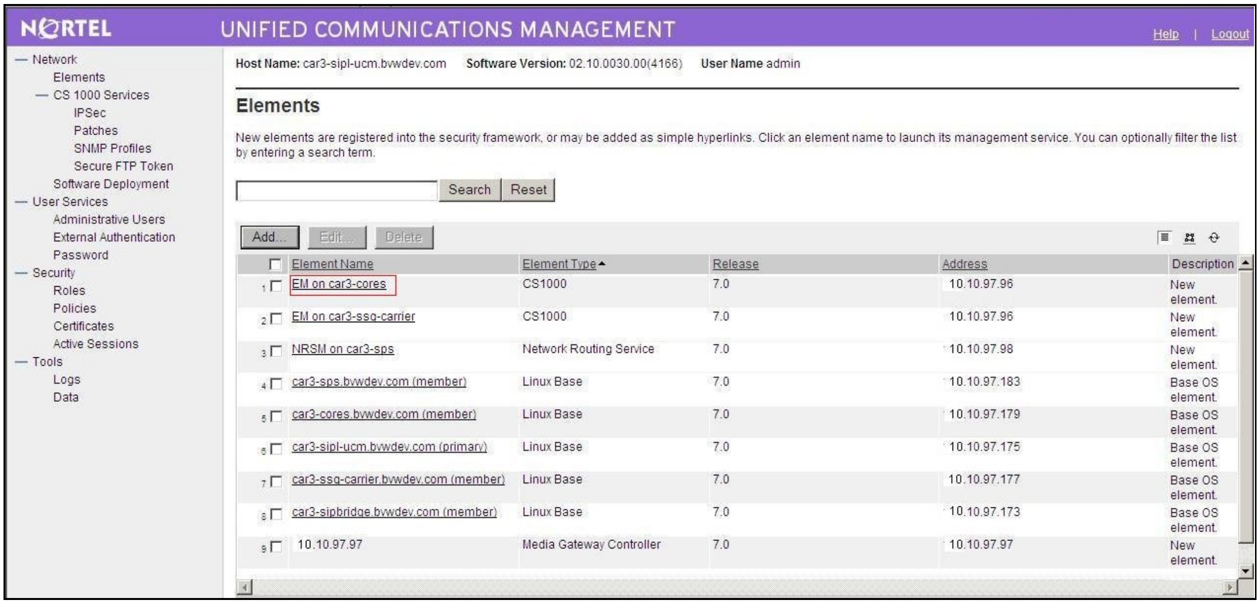

Figure 3 – Unified Communications Management

c) The Communication Server 1000 Element Manager **System Overview** page is displayed as shown in **Figure 4**.

IP Address: 10.10.97.96
Type: Communication Server 1000E CPPM Linux
Version: 4121
Release: 7.00 Q+

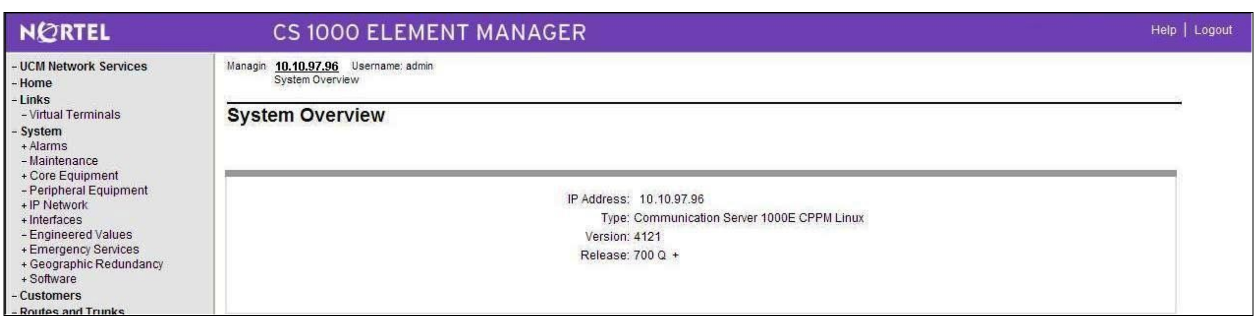

Figure 4 – Element Manager System Overview

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

a) Use Putty, SSH to connect to IP address of SSG Server with the admin account.
b) Run the command "cslogin" and login with the appropriate admin account and password.
c) Here are the logs.

```
login as: admin

   Nortel Networks Linux Base 7.00
The software and data stored on this system are the property of,or licensed to, Nortel Networks
and are lawfully available onlyto authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited andpunishable under appropriate
laws. If you are not an authorizeduser then do not try to login. This system may be monitored
foroperational purposes at any time.

admin@10.10.97.177's password:<----enter your password
Last login: Fri Jun 10 14:20:05 2011 from 10.10.98.78
[admin@car3-ssg-carrier ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authenticating
>login
USERID? admin
PASS?<----enter your password
.
TTY #08 LOGGED IN
The software and data stored on this system are the property of,or licensed to, Nortel Networks
and are lawfully available onlyto authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited andpunishable under appropriate
laws. If you are not an authorizeduser then logout immediately. This system may be monitored
foroperational purposes at any time.
 ADMIN 12:56  16/6/2011
>
```

5.2. Administer a Node IP Telephony

This section describes how to configure a Node IP Telephony on the Communication Server 1000.

5.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been administered and that Node has already been created.This Section describes the steps for configuring a Node (Node ID 3000) in Communication Server 1000 IP network to work with Windstream system. For further information on Avaya Communications Server 1000, please consult reference in **Section 9**.

a) Select **System ->IP Network ->Nodes: Servers, Media Cards** and then click on the Node ID of your **CS 1000 Element Manager** as shown in **Figure 5**.

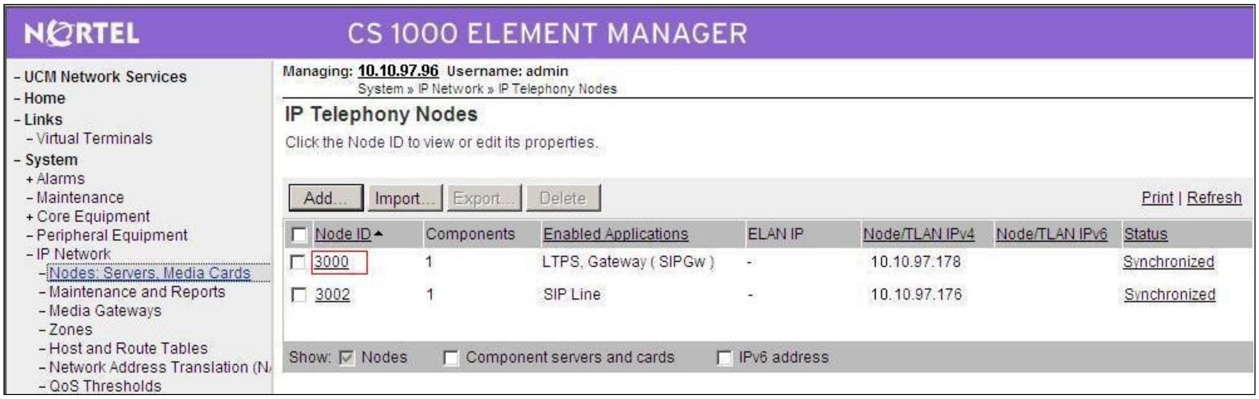

Figure 5 – IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 6a, Figure 6b**with the IP address of the Communication Server 1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this**Node IPAddress** to communicate with other components to process the SIP call.

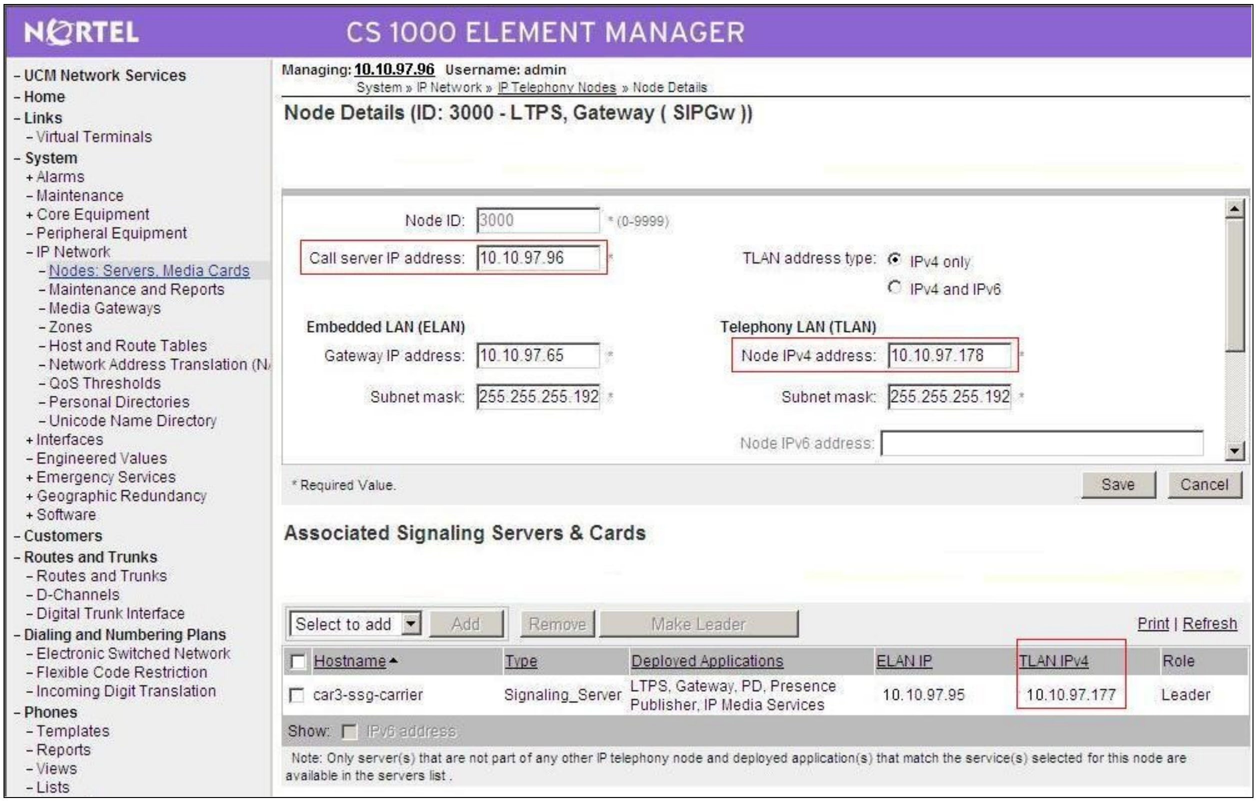

Figure 6a –Node Details

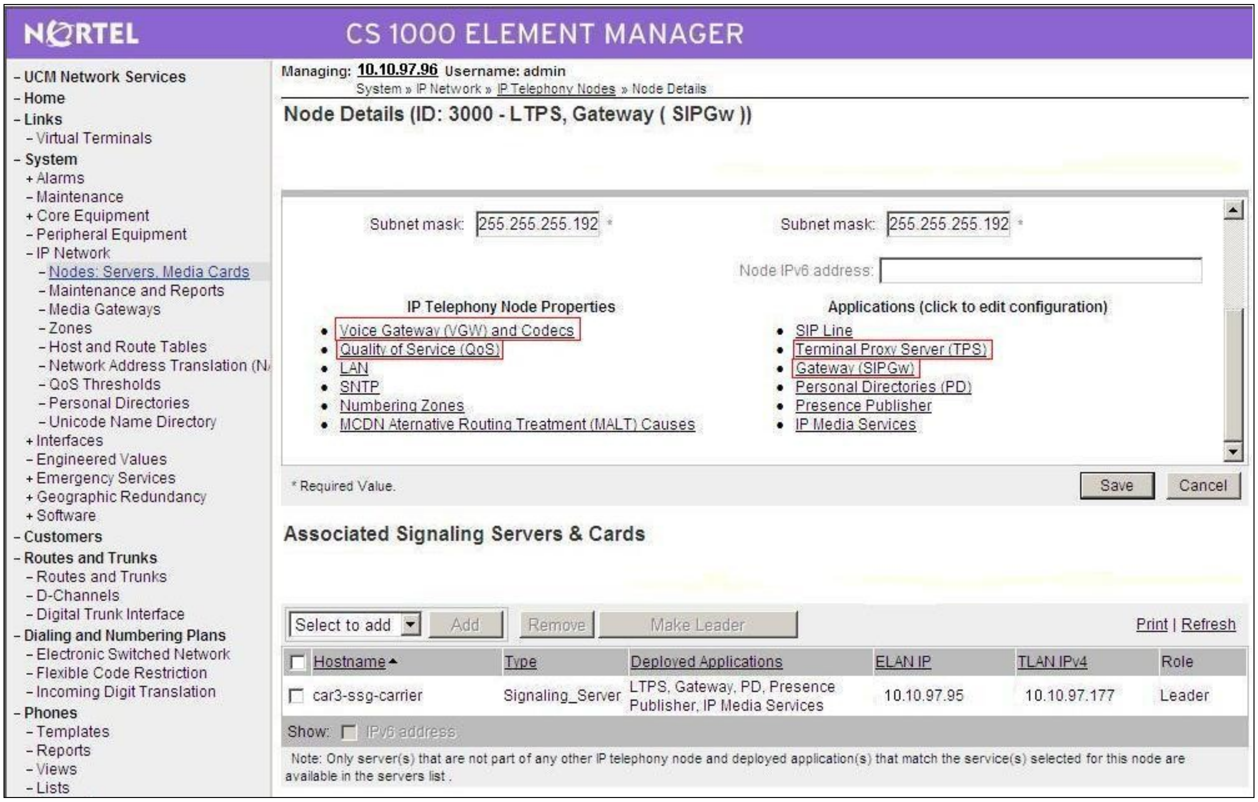

Figure 6b –Node Details

5.2.2. Administer Terminal Proxy Server (TPS)

c) Continue from **Section 5.2.1**. On the **Node Details** page, select the**Terminal Proxy Server** (**TPS**) link as shown in **Figure 6b**.

d) Check the **UNIStim Line Terminal Proxy Server**check box and then click the **Save**button as shown in **Figure 7**.

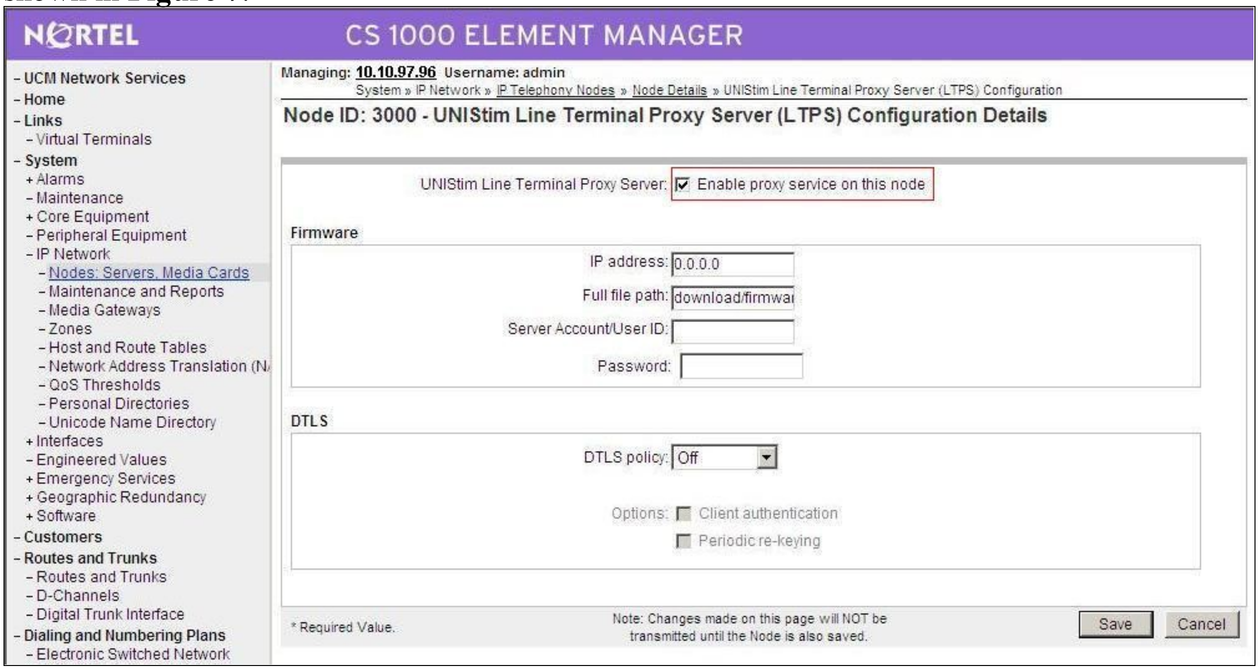

Figure 7 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

e) Continue from **Section 5.2.1**. On the **Node Details** page, select the**Quality of Service (QoS)**link as shown in **Figure 6b**.
f) The default Diffserv values are as shown in**Figure 8**. Click on the**Save** button.

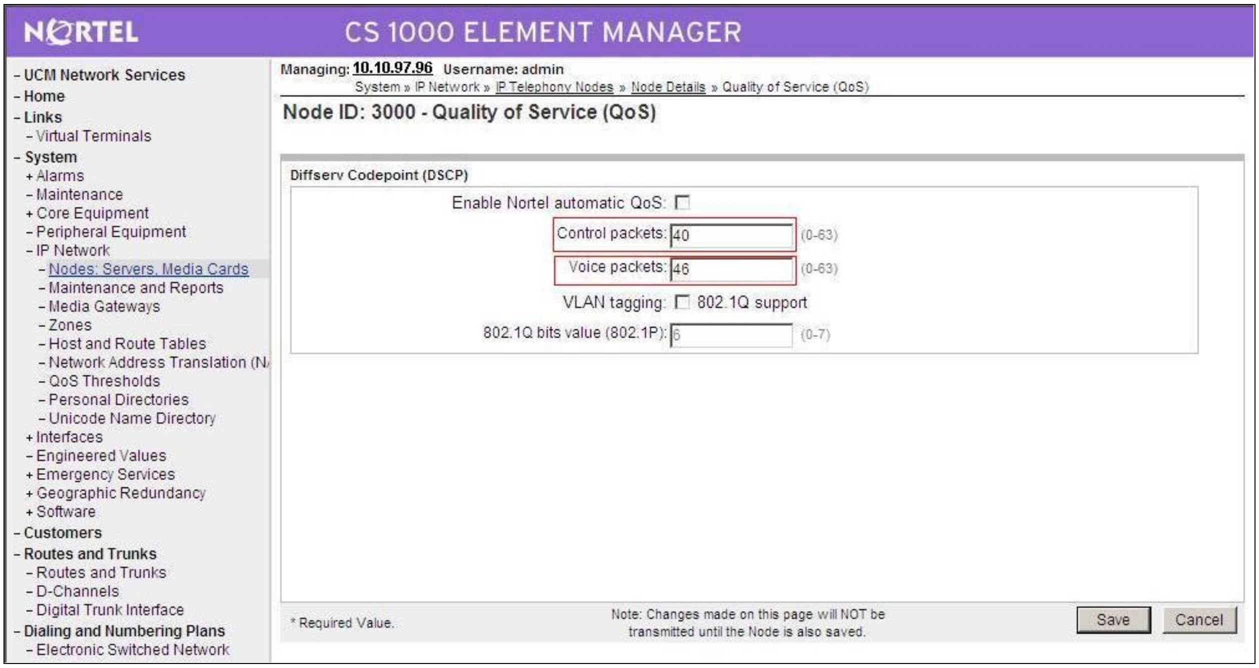

Figure 8 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

g) Continue from **Section 5.2.3**, return to the **Node Details**page (**Figure 6a**) and click on the**Save** button.
h) The **Node Saved** screen is displayed. Click on the**Transfer Now** (not shown).
i) The **Synchronize ConfigurationFiles** screen is displayed. Check the Signaling Server check box and click on the**StartSync**(not shown).
j) When the synchronization completes, check the Signaling Server check box and click on the **Restart Applications**(not shown)

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G711, Node IP Telephony.

a) Select **IP Network** ->**Nodes: Servers, Media Cards** ->Configurationfrom the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this Communication Server 1000 system. The **Node Details** screen is displayed. (See **Section 5.2.1** for more detail).
b) On the **Node Details**page as shown in **Figure 6b**, click on **Voice Gateway (VGW) and Codec.**
c) The Windstream system only supports **G711, ptime 20ms with VAD disabled**. The Windstream system does not support G729therefore the system ensures that the **Codec G729** and **Voice Activity Detection** (**VAD)** checkboxes are unchecked as shown in **Figure 9**.Then click on the**Save**button

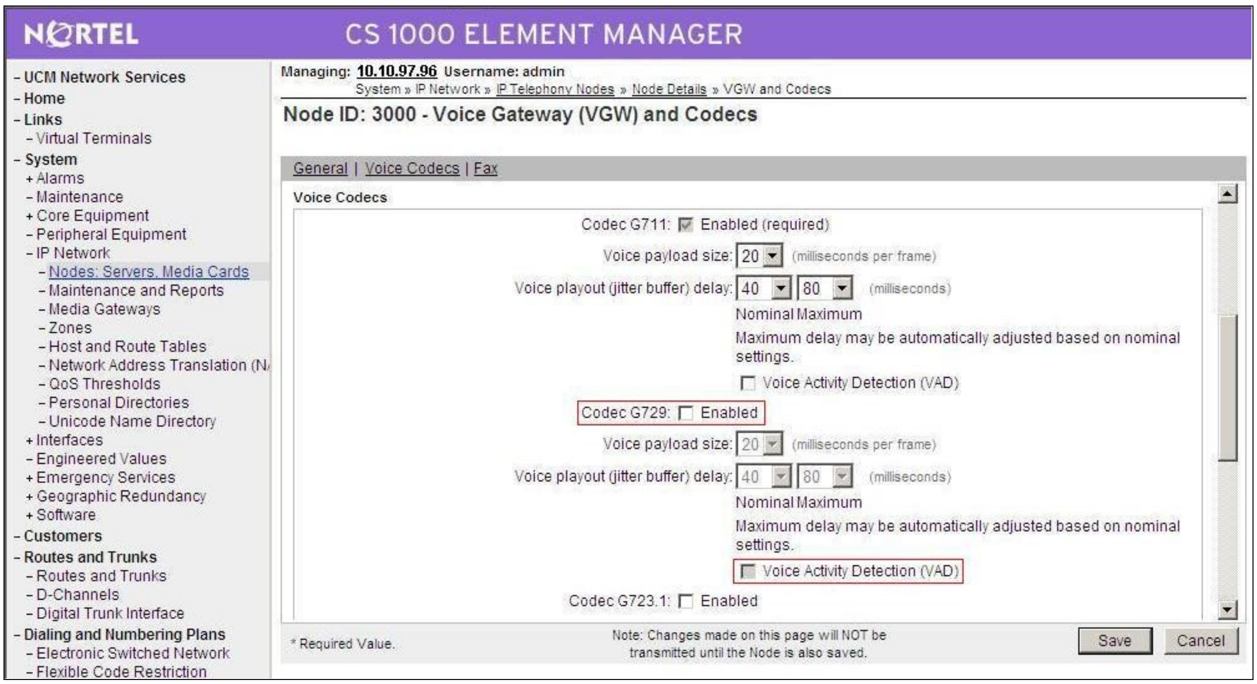

Figure 9 –Voice Gateway and Codec Configuration Details

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

5.3.2. Enable Voice Codecon Media Gateways.

a) From the left menu of the Element Manager page in **Figure 9**, select **IP Network ->Media Gatewaysmenu** item.The Media Gateways page will appear (not shown). Click on the**MGC**which is located on the right of the page.

b) In the following screen scroll down to the**Codec G711**and uncheck **VAD,** ensure to uncheck Codec G729A as shown in **Figure 10**.

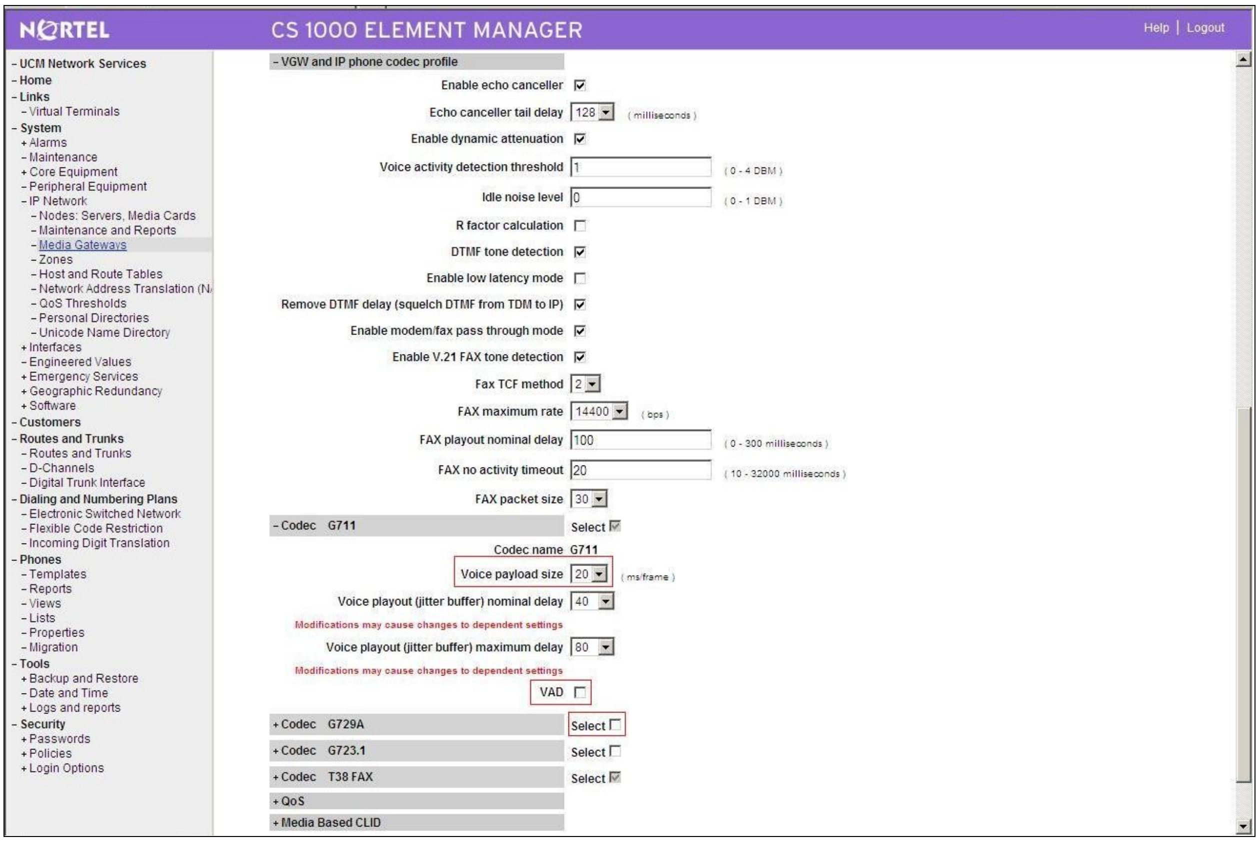

Figure 10 – Media Gateways Configuration Details

c) Then scroll down to the bottom of the page and click on the**Save** button.

5.4. Zones and Bandwidth Management

This section describes the steps to create 2 zones: zone 10 for VGW and IP sets, and zone 255 for SIP Trunk.

5.4.1. Create a zone for IP phones (zone 10)

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

a) Select **IP Network** ->**Zones** configuration from the left pane, click on the**Bandwidth Zones**as shown in **Figure 11**.

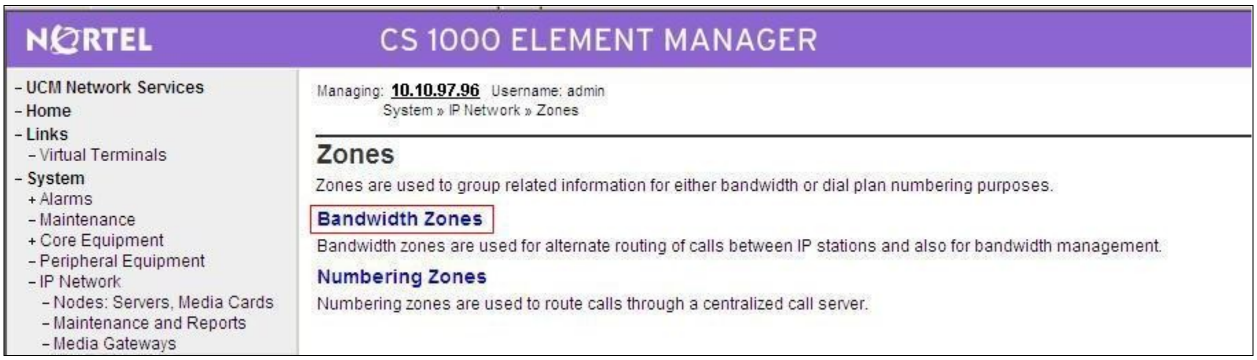

Figure 11 –Zones Page

b) The **Bandwidth Zones**screen is displayed as shown in **Figure 12**.Click**ADD** to create new zone for IP Phones.

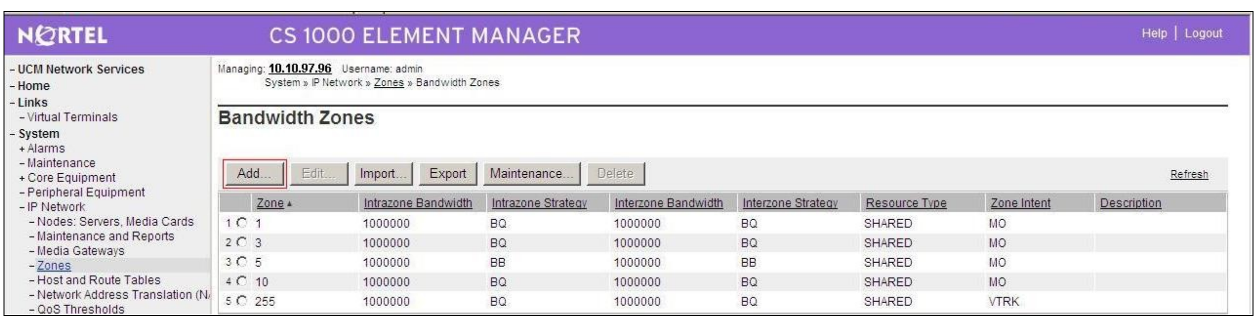

Figure 12 –Bandwidth Zones

c) Select the values as shown (in red box) in **Figure 13** and click on the **Submit** button.

- INTRA_STGY: Codec configuration for local calls.
- INTER_STGY: Codec configuration for the calls over trunk.
- BQ: G711 is first choice and G729 is second choice.
- BB: G729 is first choice and G711 is second choice.
- MO: is used for IP phones, VGW ....etc
- VTRK: is used for virtual trunk.

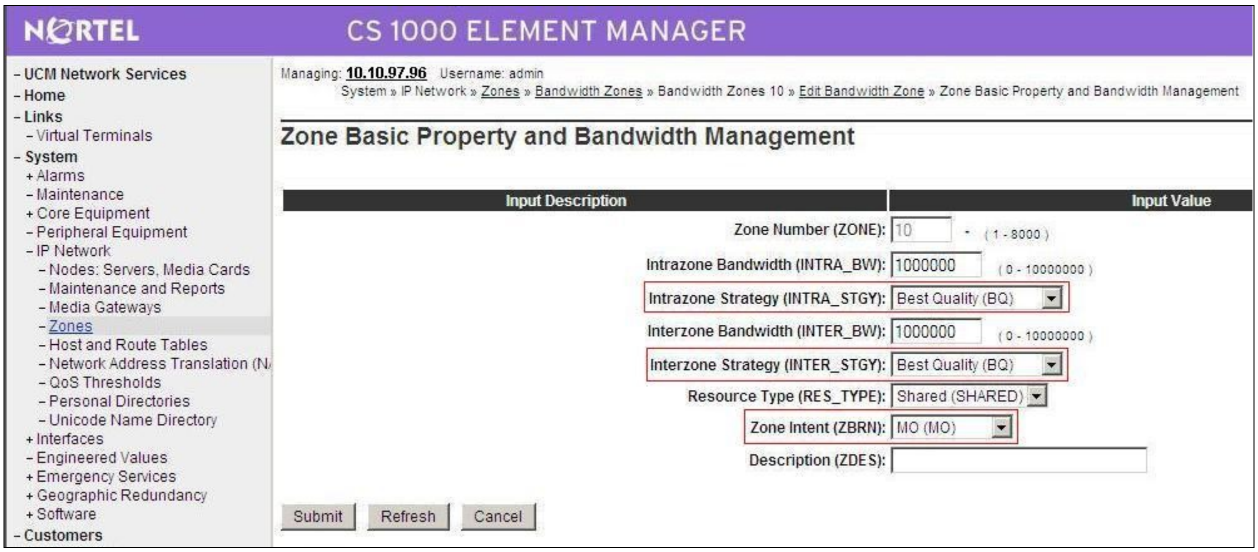

Figure 13 –Bandwidth Management ConfigurationDetails – IP phone

5.4.2. Create a zone for virtual SIP trunk (zone 255)

Follow **Section 5.4.1** to create a zone for the virtual trunk. The difference is in **Zone Intent (ZBRN)** field.Select **VTRK** for virtual trunk as shown in **Figure 14** and then click on the **Submit**button

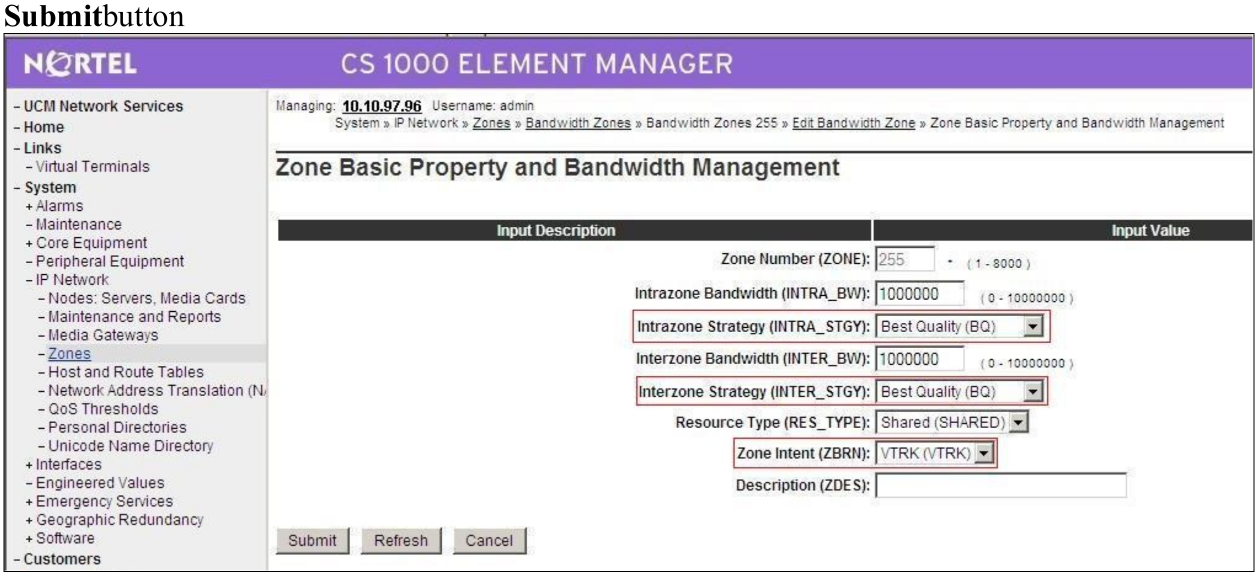

Figure 14 –Bandwidth Management ConfigurationDetails –virtual SIP trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between SIP Signaling Gateway (SSG) to NRS/SPS.

5.5.1. Integrated Services Digital Network (ISDN)

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options. The **Customer 00Edit** page will appear (not shown). Select the**Feature Packages** option from this page.
b) The screen is updated with a listing of feature packages populated below **Feature Packages** (not all features shown in **Figure 15**below). Select **Integrated Services Digital Network** to edit its parameters.The screen is updated with parameters populated below **Integrated Services Digital Network**. Click on**Integrated Services Digital Network** (ISDN), and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the**Save**button at the bottom of the page (not shown).

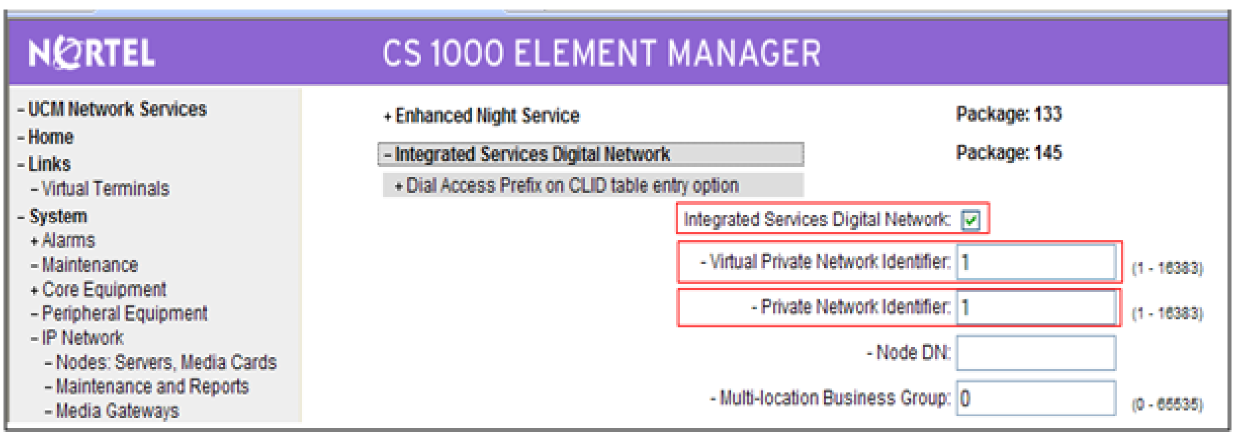

Figure 15 –Customer – ISDN Configuration

5.5.2. Administer SIP Trunk Gateway to NRS/SPS

a) Select **IP Network ->Nodes: Servers, Media Cards**configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this Communication Server 1000 system. The **Node Details** screen is displayed as shown in **Figure 6b**, **Section 5.2.1.**
b) On the **Node Details** screen, select **Gateway (SIPGw)**.
c) Under **General**tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 16**.The parameters (highlighted in red boxes) are filled in, and were obtained when a user created a SIP profile on the NRS/SPS (these are shown in **Section 5.8.2**).

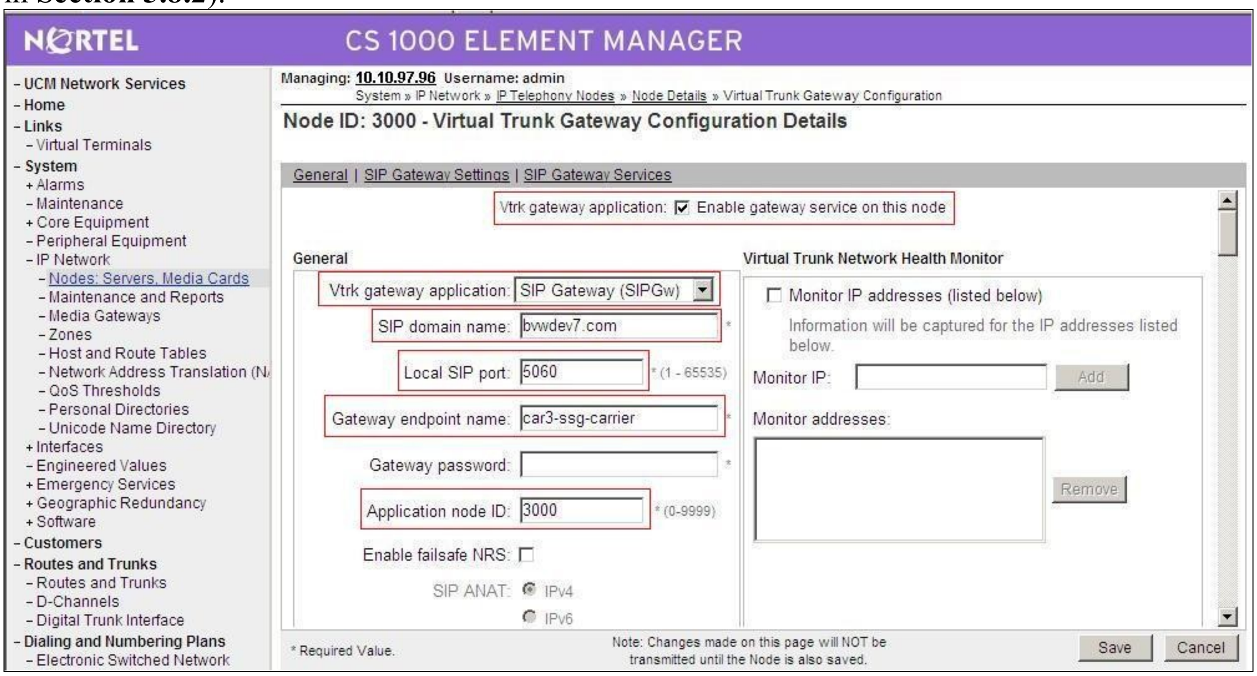

Figure 16 – Virtual Trunk Gateway Configuration Details

d) 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 17**.

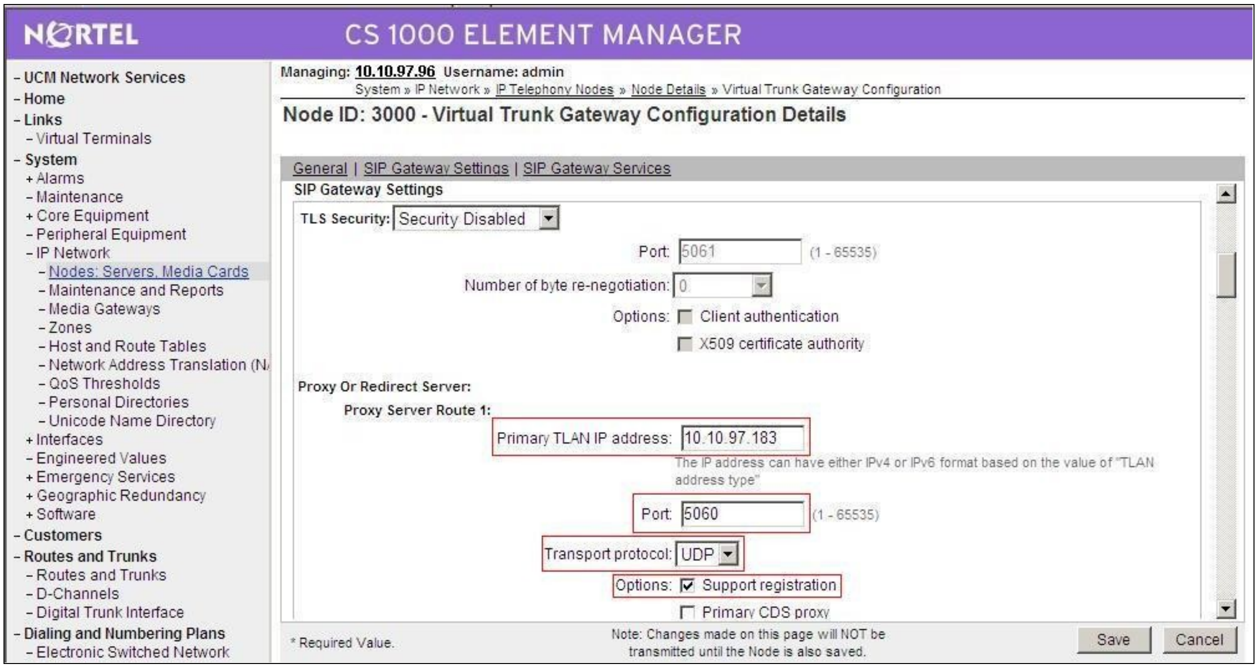

Figure 17 – Virtual Trunk Gateway Configuration Details

e) On the same page as shown in **Figure 17**, scroll downs the parameters box to the **SIP URI Map** section.

Under the **Public E.164 Domain Names**, for:
- **National**: leave this SIP URI field as blank
- **Subscriber**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Under the **Private domain names**, for:
- **UDP**: leave this SIP URI field as blank
- **CDP**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Vacant number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

The remaining fields can be left at their default values as shown in **Figure 18**. Then click on the **Save** button.

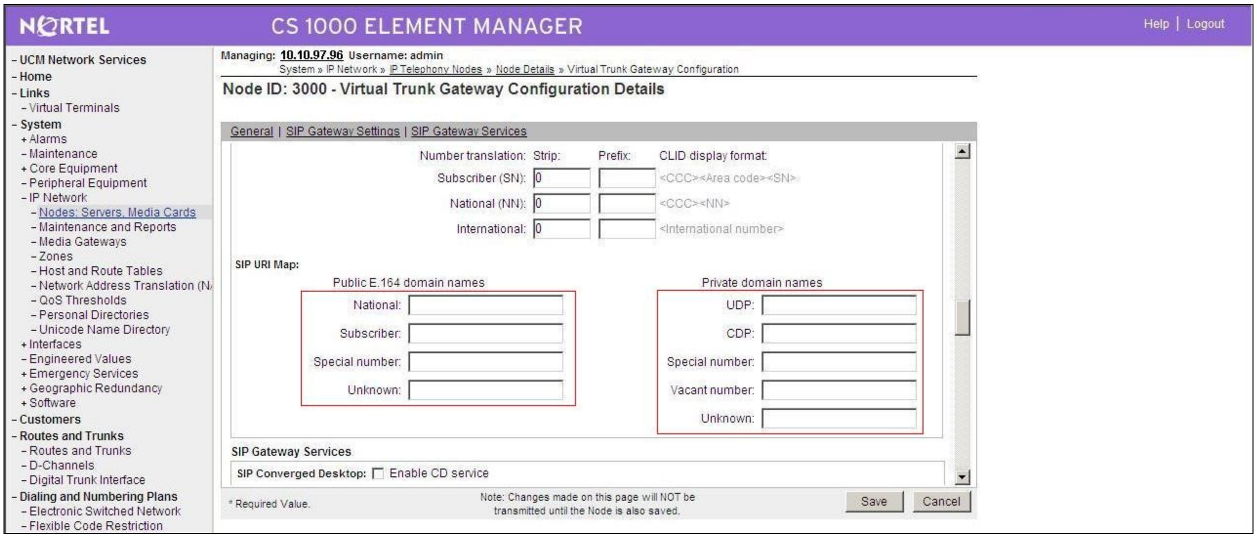

Figure 18 – Virtual Trunk Gateway Configuration Details

f) **Synchronize**the new configuration (please refer to **Section 5.2.4**).
g) After the configuration is completed on the NRS/SPS, the Gateway endpoint entry for the SSG (in this case is car3-ssg-carrier) shows the IP address of the SSG which is successfully registered to the NRS/SPS) as shown in **Figure 19**. Please refer to **Section 5.8** for more details on the NRS/SPS configuration.

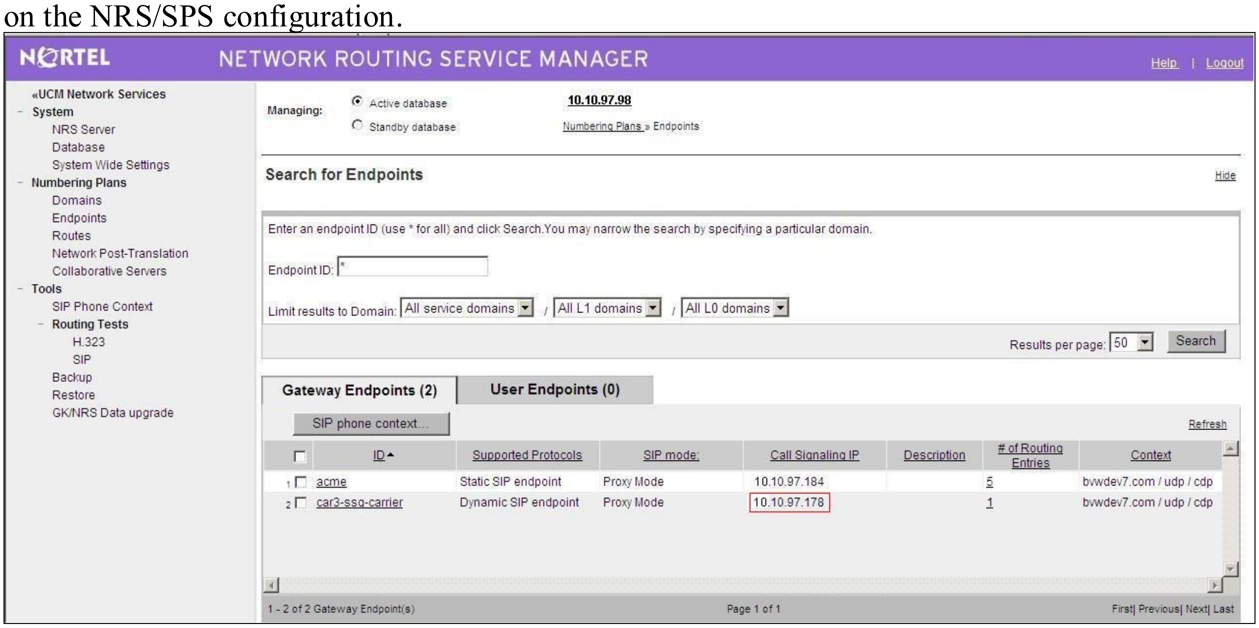

Figure 19–SSG is registered successfully to the NRS/SPS

5.5.3. Administer Virtual D-Channel

a) Select **Routes and Trunks** ->**D-Channels**from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown in **Figure 20**. Click **Add** button.

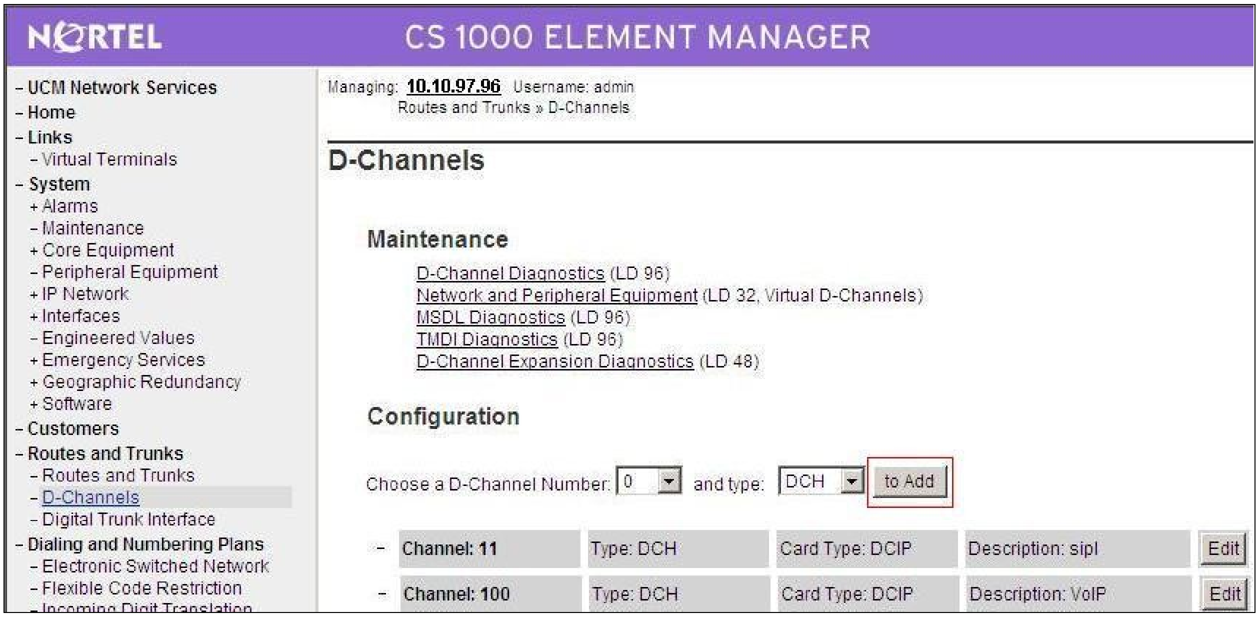

Figure 20 – D-Channels

b) The D-Channels 100 Property Configuration screen is displayed next as shown in **Figure 21**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

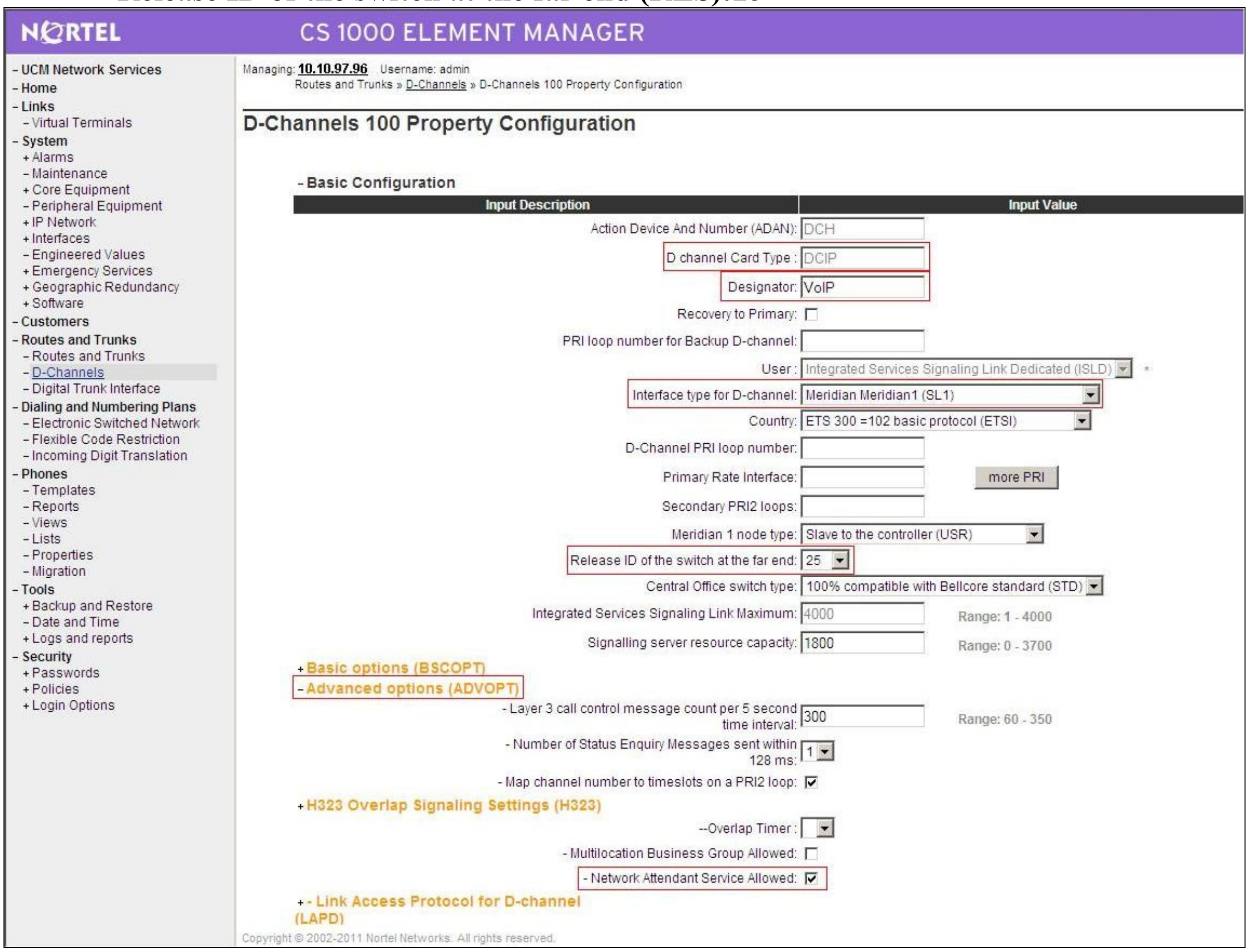

Figure 21 – D-Channels Configuration Details

c) Click on the **Advanced options (ADVOPT)**, check on the **Network Attendant Service Allowed** check box as shown in **Figure 21**. Other fields are left as default.
d) Click on the**Basic Options** and click on the **Edit** button at the **Remote Capabilities** (**RCAP**) attribute. The **Remote Capabilities Configuration** page will appear. Then check on the**ND2** and the**MWI**checkboxes as shown in **Figures 22** and **23**.

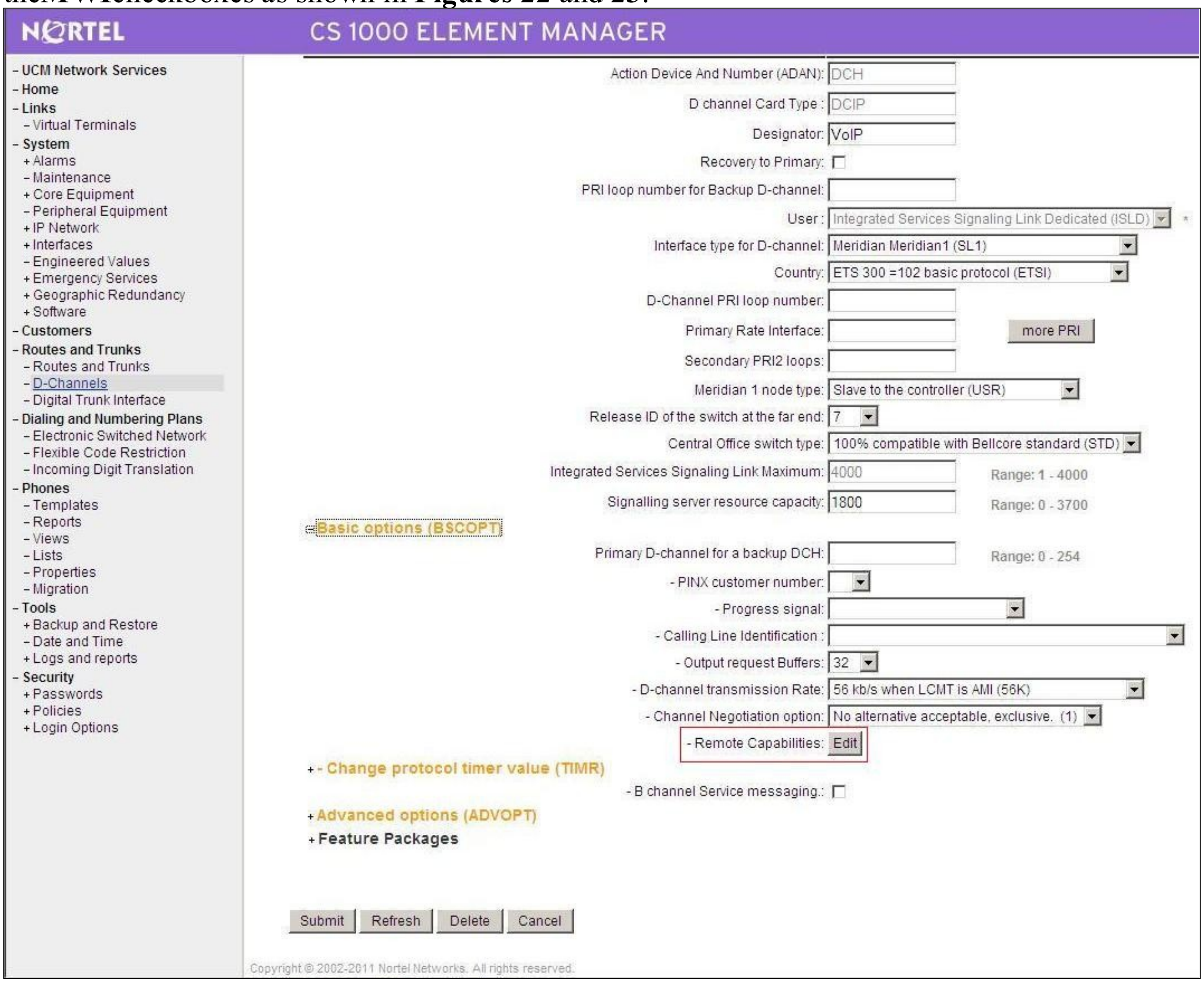

Figure 22 – D-Channel Configuration Details

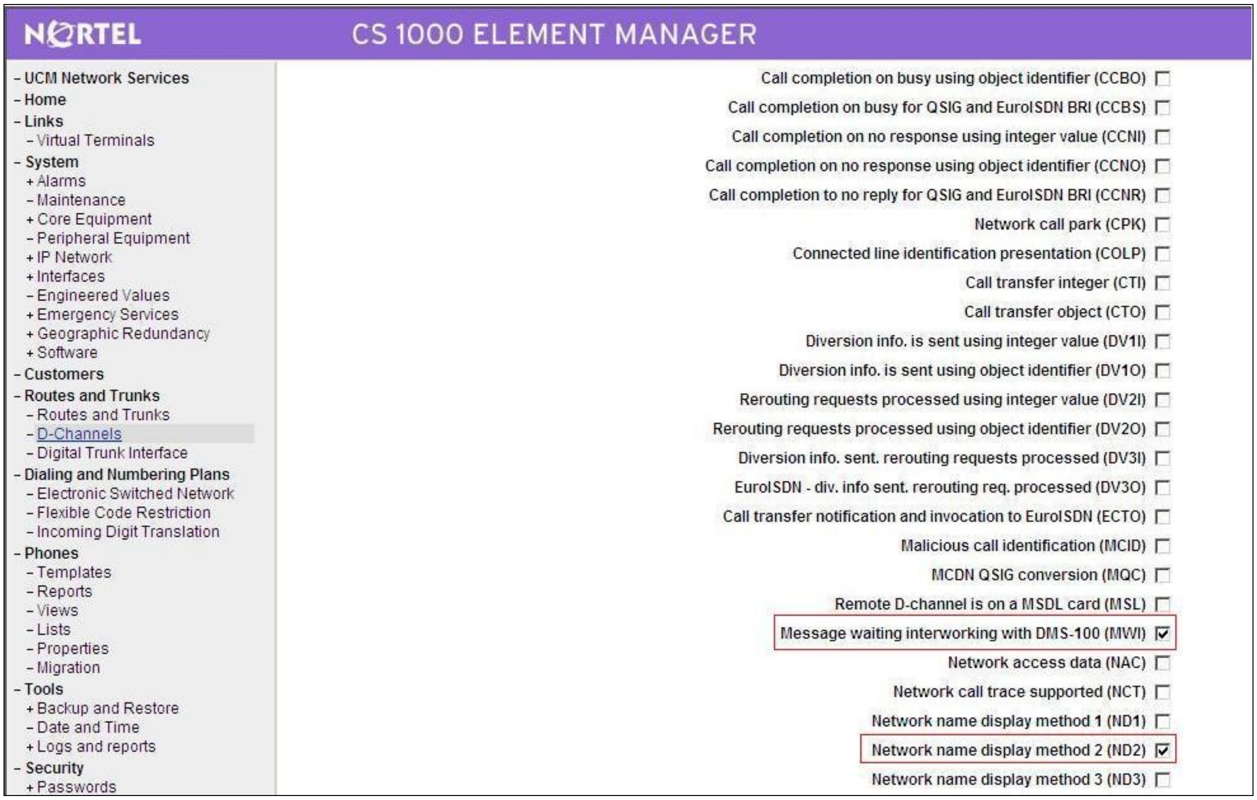

Figure 23 – Remote Capabilities Configuration Details

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

5.5.4. Administer Virtual Super-Loop

Select **System** ->**Core Equipments** ->**Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click "**Add**" button to create a new one as shown in **Figure 24**. In this example, superloop4, 96, 100 and 124 has been added and is being used.

Figure 24 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

a) Select **Routes and Trunks** ->**Routes and Trunks**from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used.Click on the**Add route**button as shown in **Figure 25**.

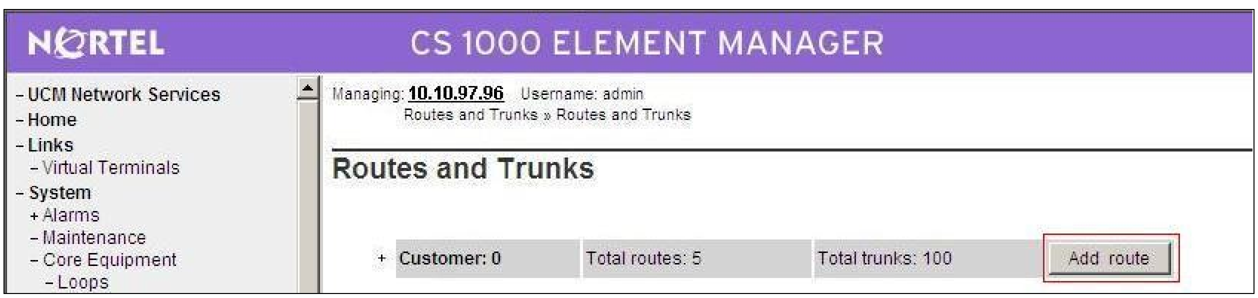

Figure 25 – Add route

b) The **Customer 0**, New **Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration**Section is displayed and enter the following values for thespecified fields, and retain the default values for the remaining fields as shown in **Figures 26**.

- **Route Number** (ROUT): Select an available route number.
- **Designator field for trunk** (DES): A descriptive text.
- **Trunk Type** (TKTP): TIE trunk data block (TIE)
- **Incoming and Outgoing trunk** (ICOG): Incoming and Outgoing (IAO)
- **Access Code for the trunk route** (ACOD): An available access code.
- Check the field **The route is for a virtual trunk route** (VTRK), to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management** (ZONE) field, enter 255 (created in **Section 5.4.2**).
- 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. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
    - **Mode of operation** (MODE): Route uses ISDN Signalling Link (ISLD)
    - **D channel number** (DCH): D-Channel number 100 (created in **Section 5.5.3**)
    - **Network calling name allowed** (NCNA): Check the field.
    - **Network call redirection** (NCRD): Check the field.
    - **Insert ESN access code** (INAC)**:** Check the field.

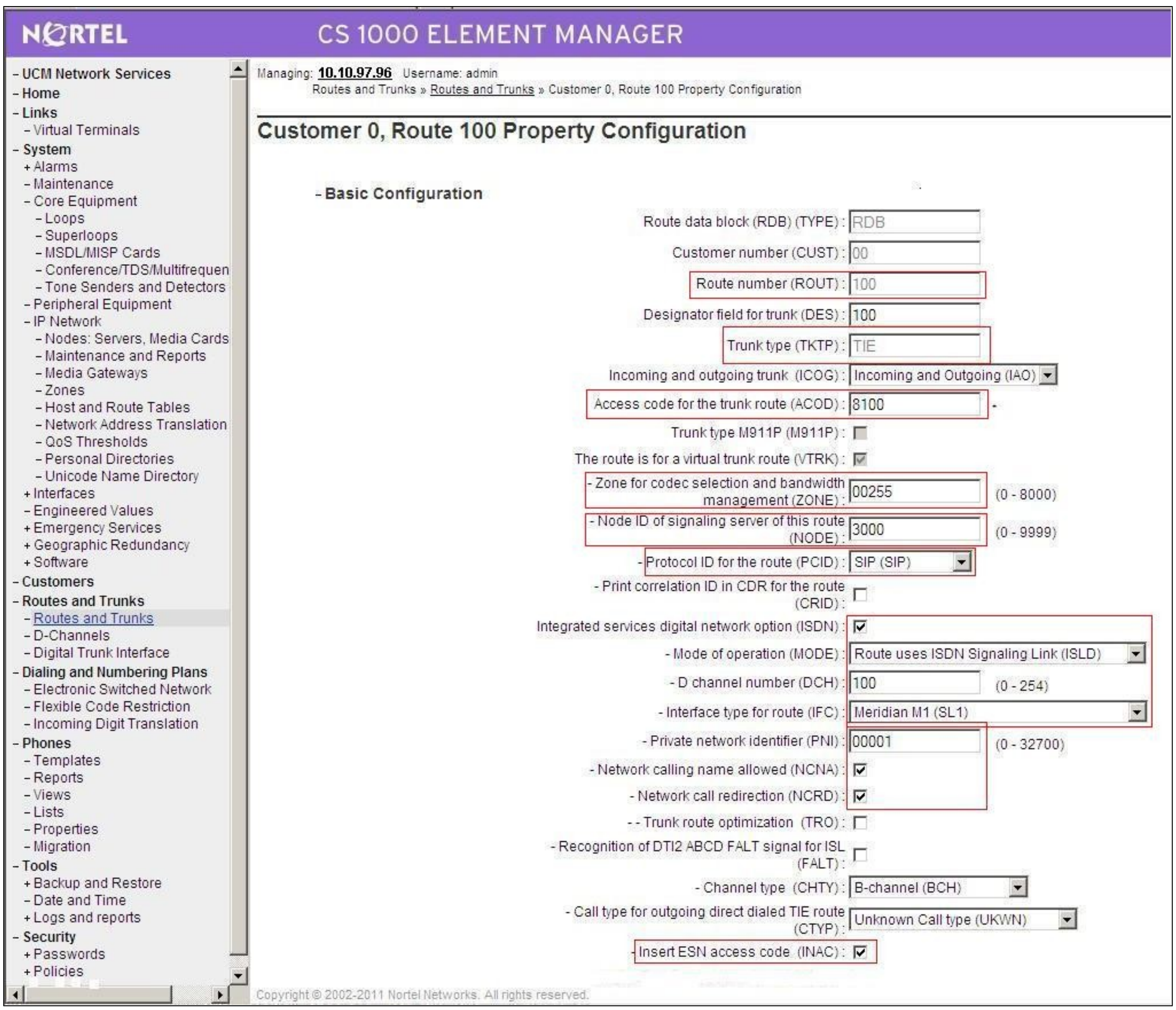

Figure 26 – Route Configuration Details

-Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 1** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown in **Figure 27.**

-

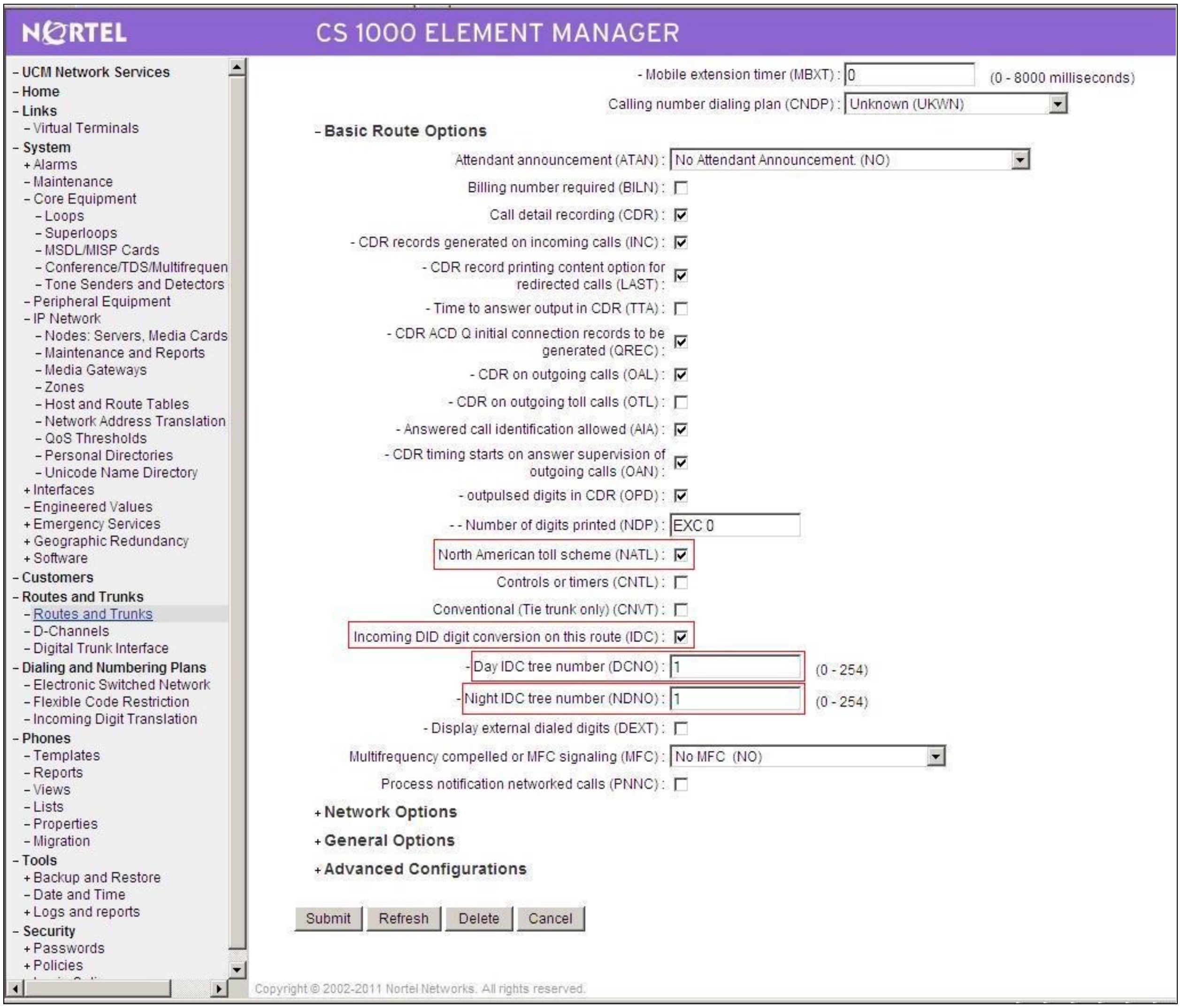

Figure 27 – Route Configuration Details

c) Click on the**Submit** button.

5.5.6. Administer Virtual Trunks

a) From the EM, select **Routes and Trunks**->**Route and Trunks**, the Route list is now updated with the newly added route. In the example, the Route 100 was being added. Click on the **Add trunk** button next to the newly added route 100 as shown in **Figure 28**.

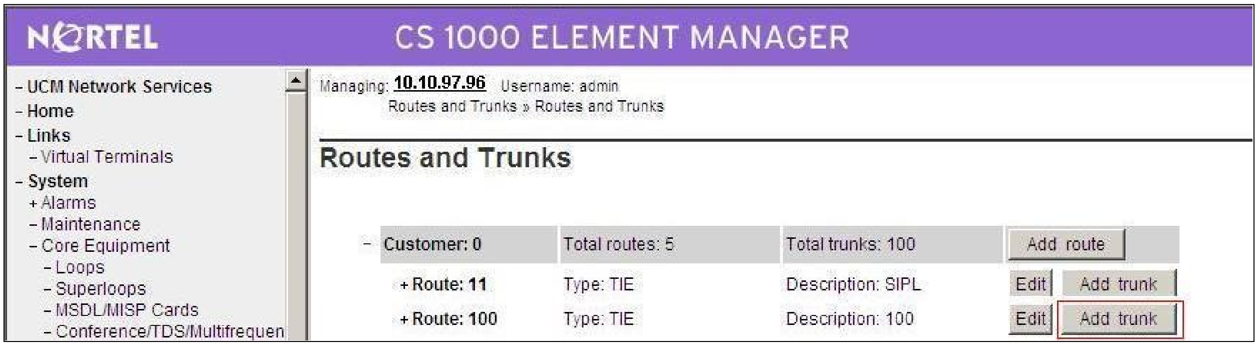

Figure 28 – Route and Trunks Page

b) The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) needs to be disabledat the trunk level by editing the **Class of Service** (CLS) at the bottom basic trunk configuration page. Click on the **Edit** button as shown in **Figure 29**.

- The Multiple trunk input number (**MTINPUT**) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.
- Trunk data block (**TYPE**): IP Trunk (IPTI)
- Terminal Number (**TN**): Available terminal number (created in **Section 5.5.4**)
- Designator field for trunk (**DES**): A descriptive text
- Extended Trunk (**XTRK**): Virtual trunk (VTRK)
- Route number, Member number (**RTMB**): Current route number and starting member
- Card Density: 8D
- Start arrangement Incoming (**STRI**): IMM
- Start arrangement Outgoing (**STRO**): IMM
- Trunk Group Access Restriction (**TGAR**): Desired trunk group access restriction level
- Channel ID for this trunk (**CHID**): An available starting channel ID

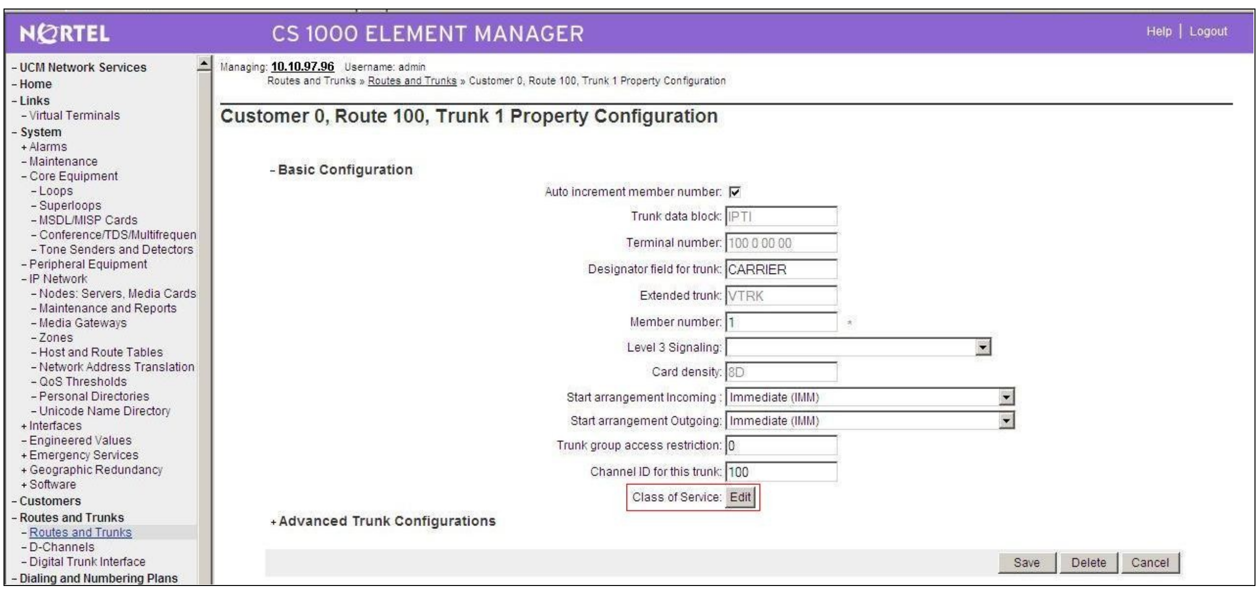

Figure 29 – New Trunk ConfigurationDetails

c) For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in **Figure 30**. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the**Save** button (not shown)

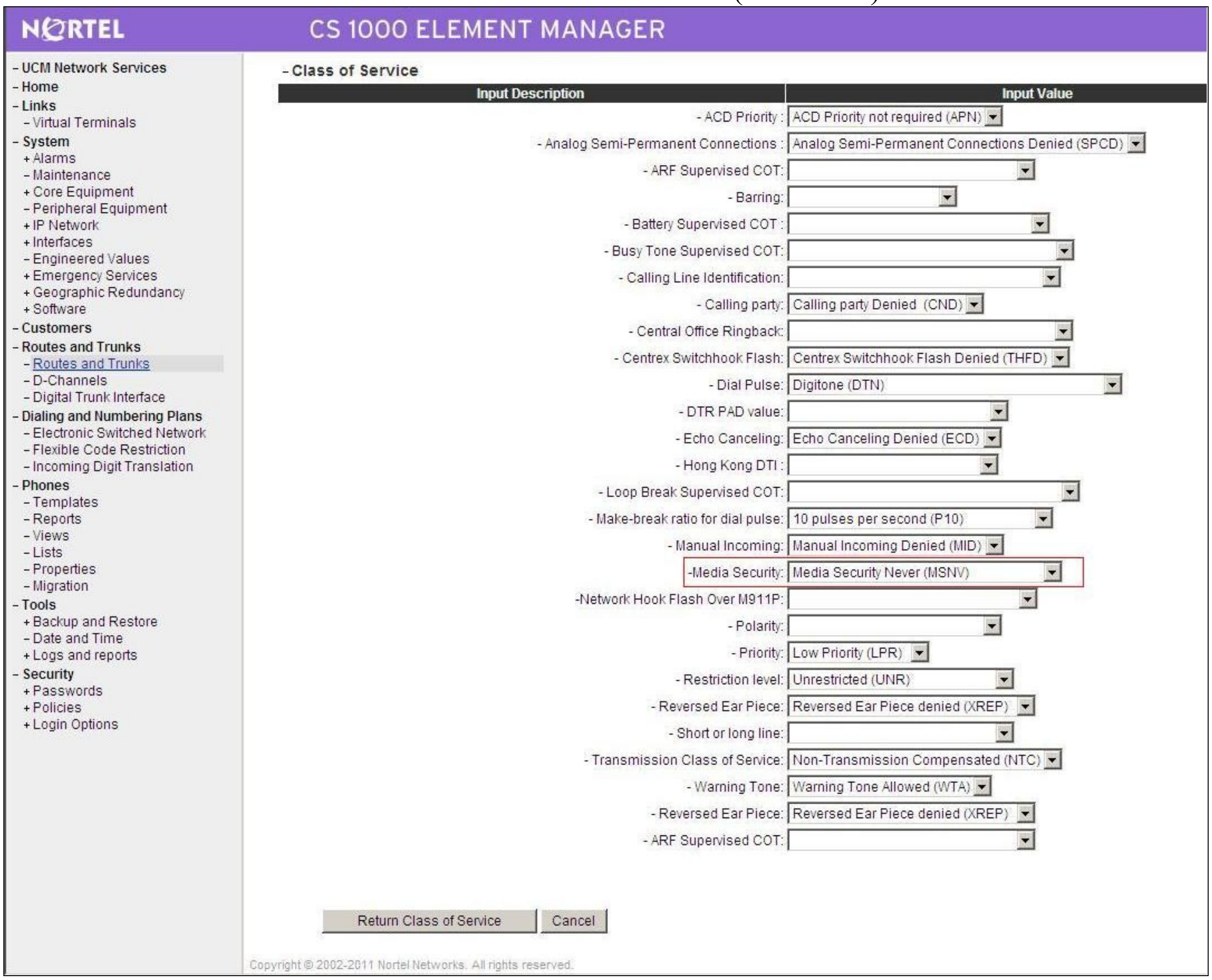

Figure 30 – Class of Service ConfigurationDetailsPage

5.5.7. Administer Calling Line Identification Entries

a) Select **Customers->00->ISDN and ESN Networking**. Click on **Calling Line Identification Entries**asshown in **Figure 31**.

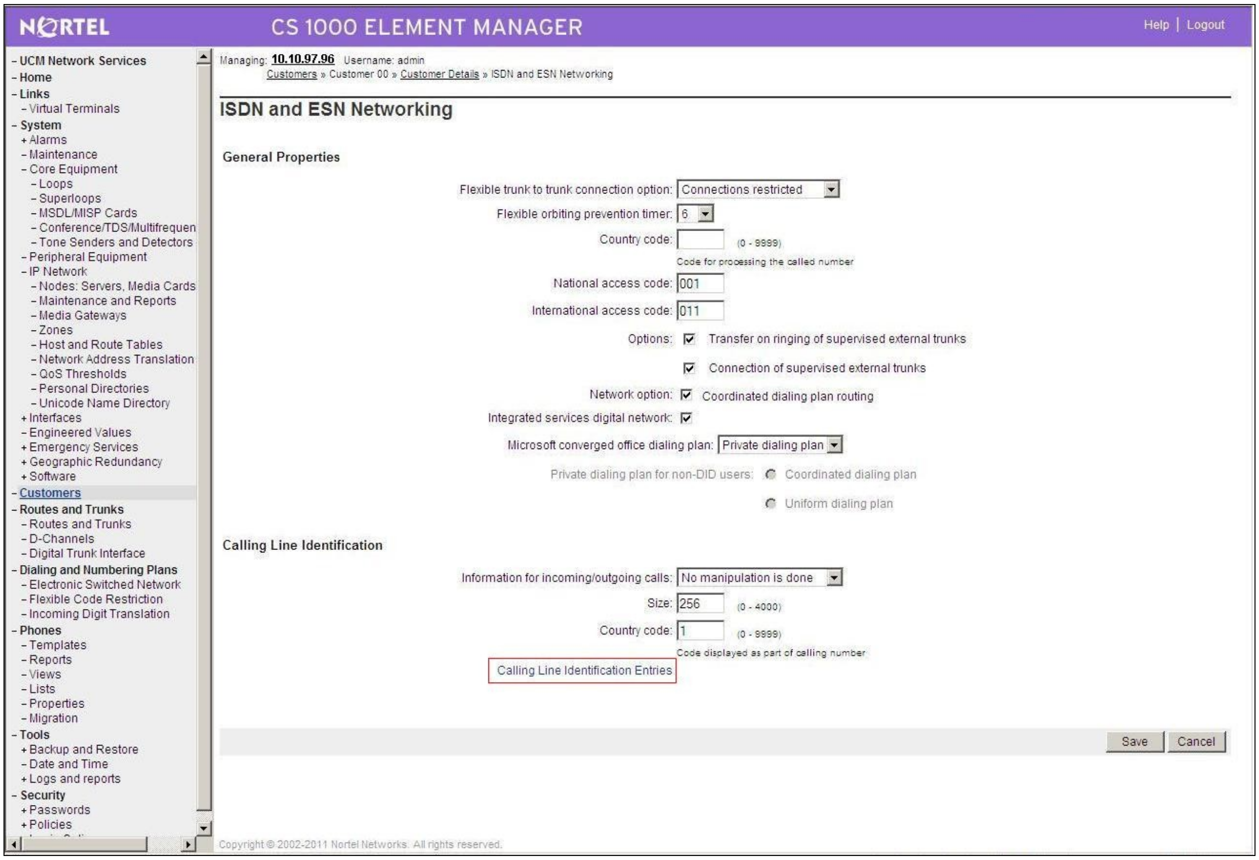

Figure 31 – ISDN and ESN Networking

b) Click on **Add** asshown in **Figure 32**.

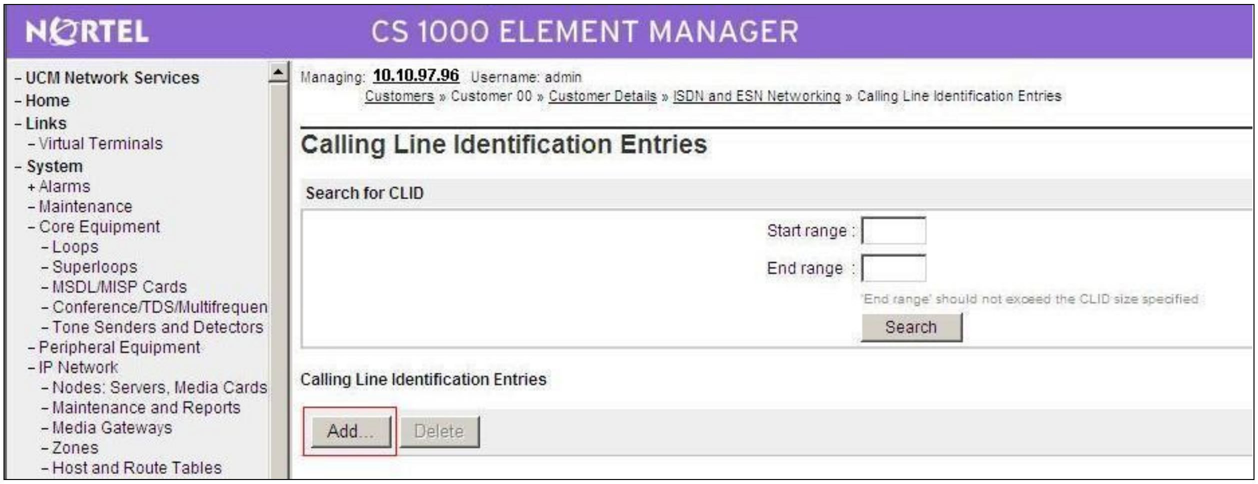

Figure 32 – Calling Line Identification Entries

c) Add entry **0**asshown in **Figure 33:**

- **National Code**: leave as blank
- **Local Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits – 501287. This **Local Code** will be used for call display purpose of outbound international call configuration in **Section 5.6.6** in which the **Special Number 011**is associated with Call Type = Unknown.
- **Home Location Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits - 501287. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits - 501287. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Calling Party Name Display**: Uncheck for **Roman characters**.

Click on the **Save** button as shown in **Figure 33.**

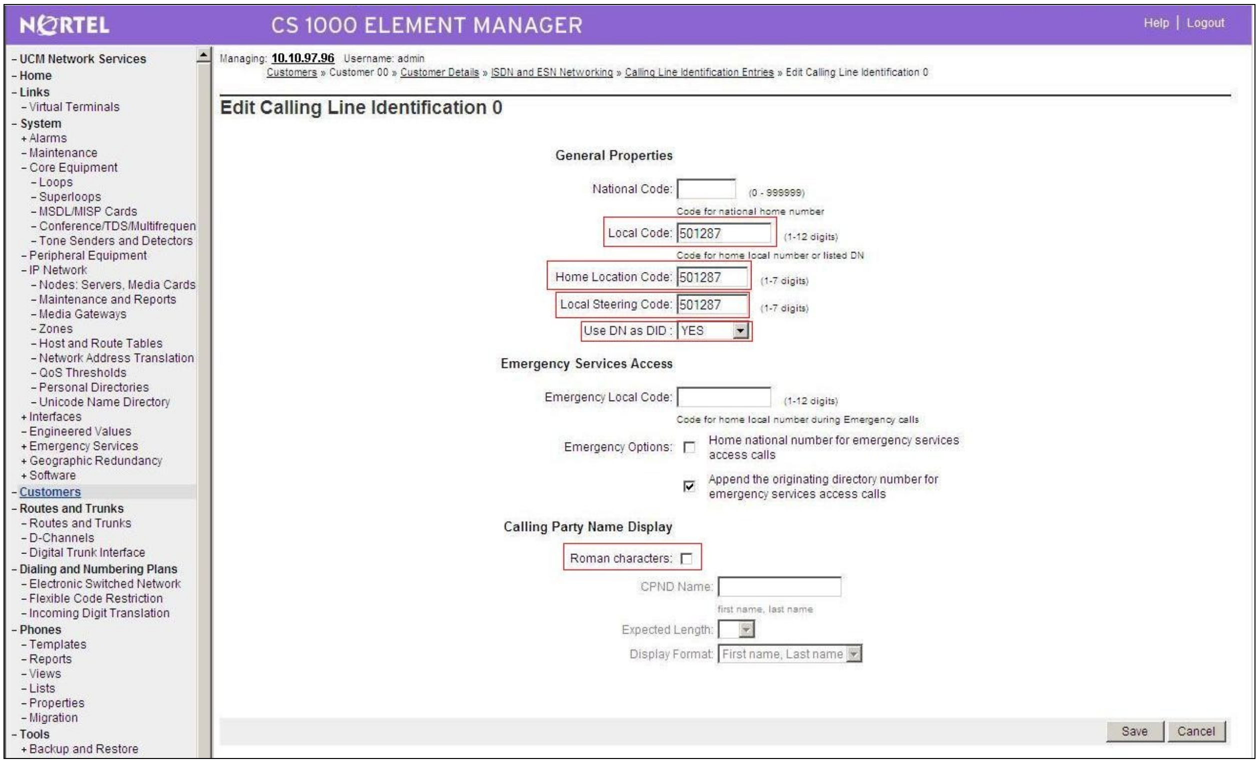

Figure 33 – Edit Calling Line Identification 0

5.5.8. Enable External Trunk to Trunk Transferring

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

a) Login Call Server Overlay CLI (please refer to **Section 5.1.2** for more detail)
b) Allow External Trunk to Trunk Transferring 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
EXTT YES
…
```

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

a) Select **Dialing and Numbering Plans ->Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen as shown in **Figure 34**

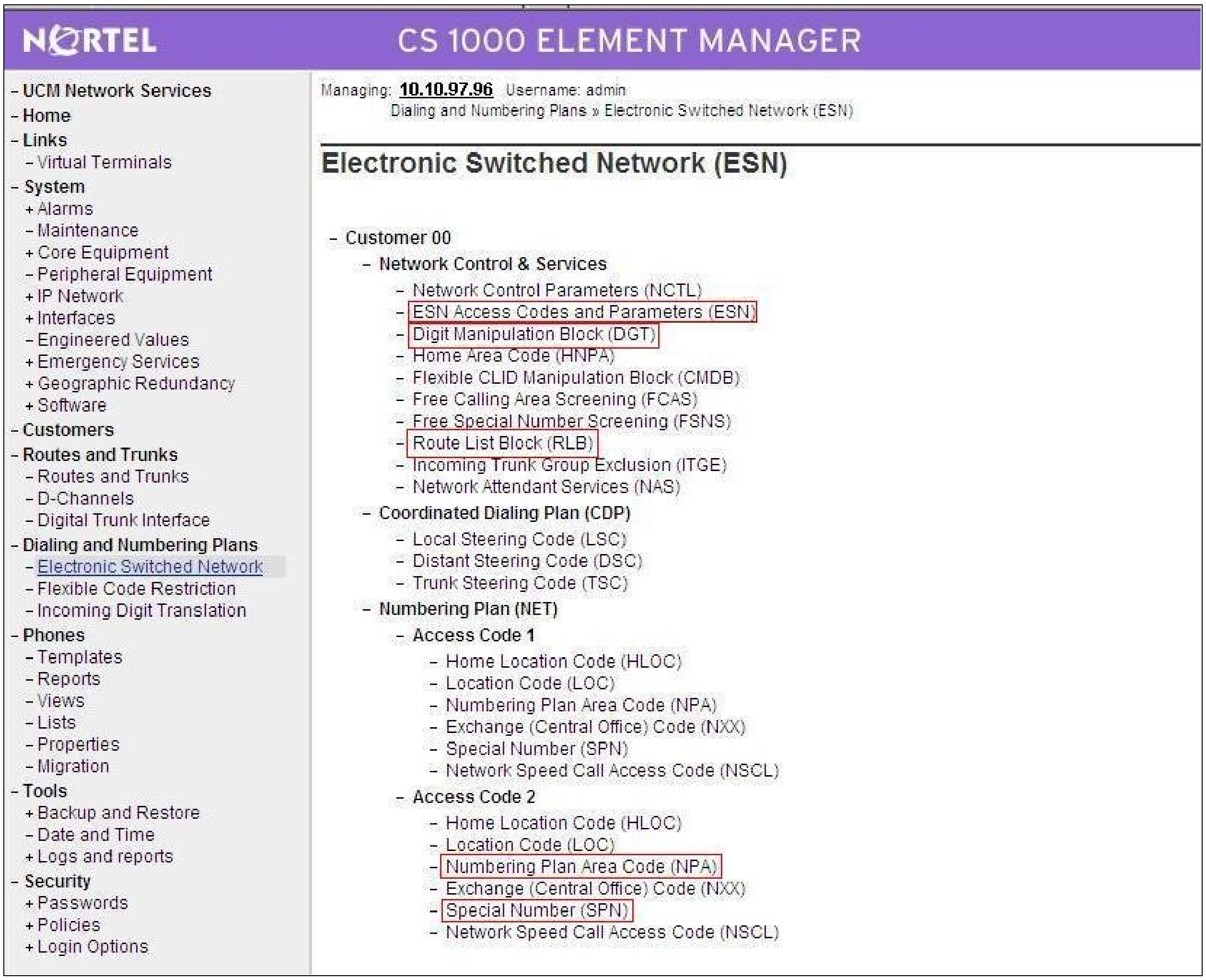

Figure 34 –ESN Configuration Details

b) In the **ESN Access Codes and Basic Parameters** page, define **NARS Access Code 2** as shown in **Figure 35**.
c) Click Submit button (not shown).

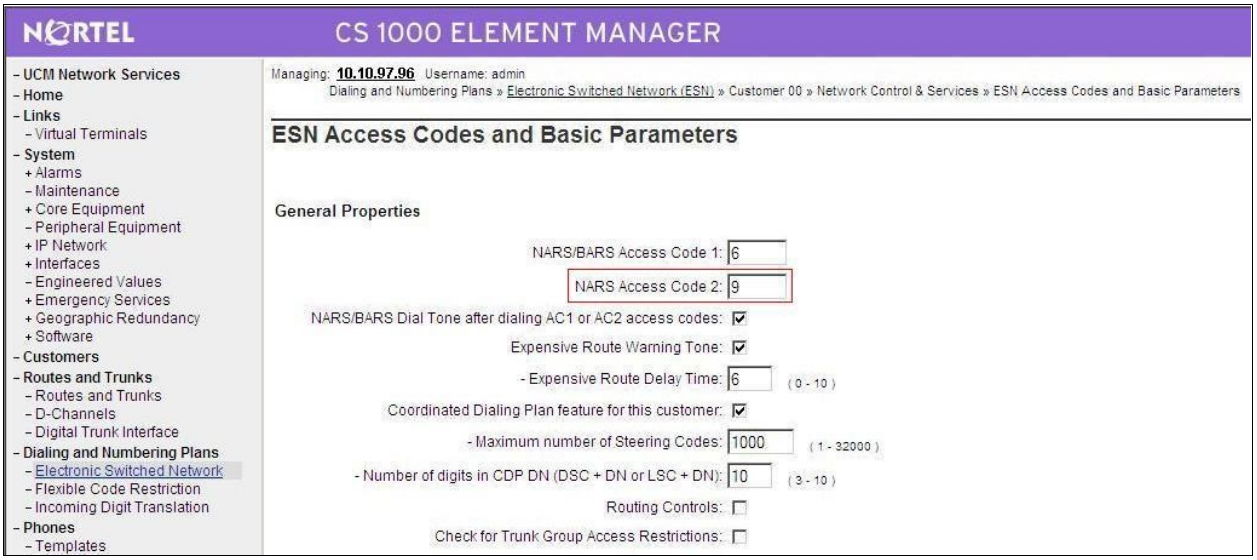

Figure 35 – ESN Access Codes and Basic Parameters

5.6.2. Associate NPA and SPN call to ESN Access Code 2

a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail), 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
AC1xNPAxSPN    ------ > (Set NPA, SPN not to associate to ESN Access Code 1)
FNP
CLID
…
```

b) 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
AC2INTL NPA SPN NXX LOC ------ > (NPA, SPN are associated to ESN Access Code 2)
FNP YES
…
```

5.6.3. Digit Manipulation Block (DMI)

a) Select **Dialing and Numbering Plans** ->**Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Digit Manipulation Block** (DGT) as shown in **Figure 34**.
b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click **to Add**as shown in **Figure 36**.
c) Enter the **Number of leading digits to be Deleted** (Del) field and select the **Call Type to be used by the manipulated digits** (CTYP) and then click **Submit** (see **Section 5.6.4**).

5.6.4. Digit Manipulation Block (DMI) for Outbound Call

In the following steps show how to add DMI for the outbound call, there are 4 indexes, which were added to the Digit Manipulation Block List (14 and 15).
a) Select **Dialing and Numbering Plans** --->**Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Digit Manipulation Block** (DGT) as above.
b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click on**to Add**button as shown in **Figure 36**.

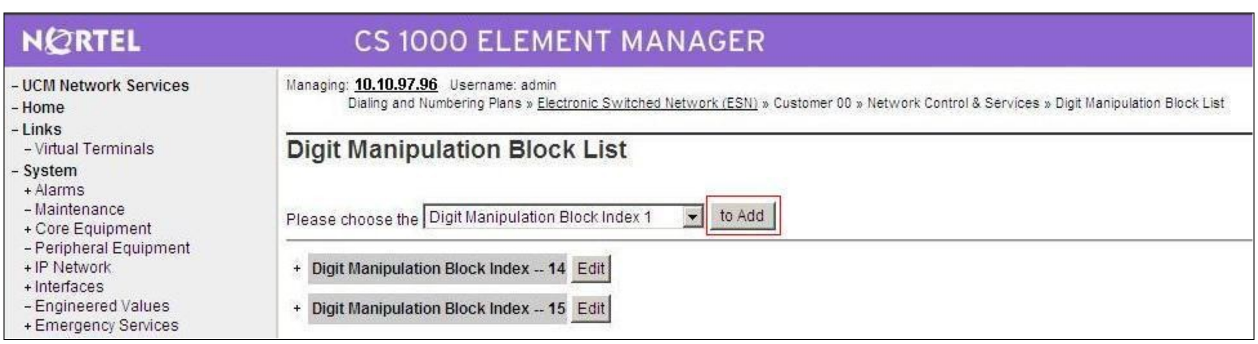

Figure 36 – Add a DMI

c) Add DMI_14: Enter 0 for the **Number of leading digits to be Deleted** (Del) field and select **NPA**for the **Call Type to be used by the manipulated digits** (CTYP) and then click on **Submit**button as shown in **Figure 37a**

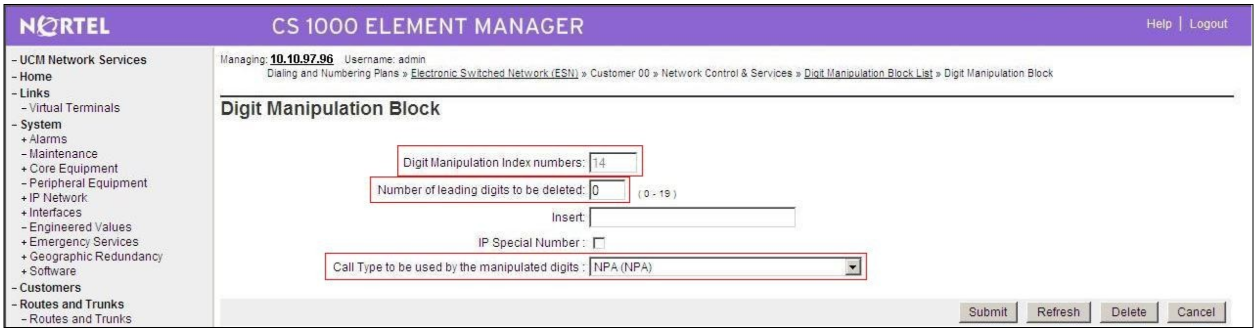

Figure 37a – DMI_14ConfigurationDetails

d) Add DMI_15: Enter 1 for the **Number of leading digits to be Deleted** (Del) field and select **NPA** for the **Call Type to be used by the manipulated digits** (CTYP) and then click on **Submit**button as shown in **Figure 37b**

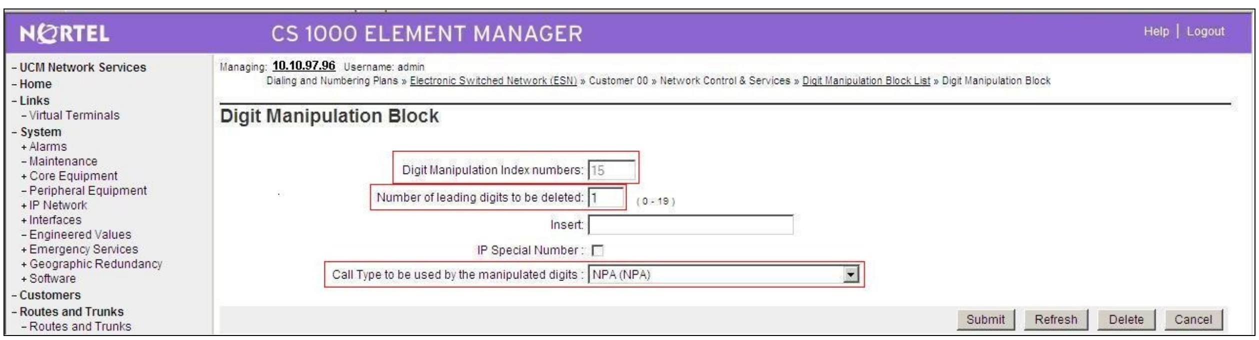

Figure 37b – DMI_15ConfigurationDetails

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

This session shows how to add a RLB associated with the DMI created in **Section 5.6.4**.
a) Select **Dialing and Numbering Plans ->Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Route List Block** (RLB) as shown in **Figure 34**.

b) Select an available value in the textbox for the **route list index** (in this case is 14) and click on**to Add**buttonas shown in **Figure 38**.

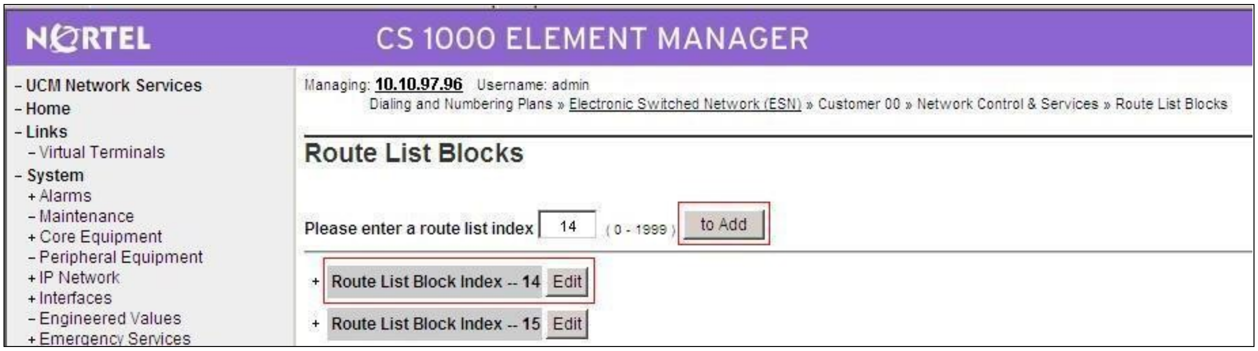

Figure 38 – Add a Route List Block.

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 39a**).Scroll down to the bottom of the screen, and click on the**Submit**button.

- **Route number** (ROUT): 100 (created in **Section 5.5.5**)
- **Digit Manipulation Index** (DMI): 14 (created in **Section 5.6.4**)
- **Incoming CLID Table**: 0 (created in **Section 5.5.7**)

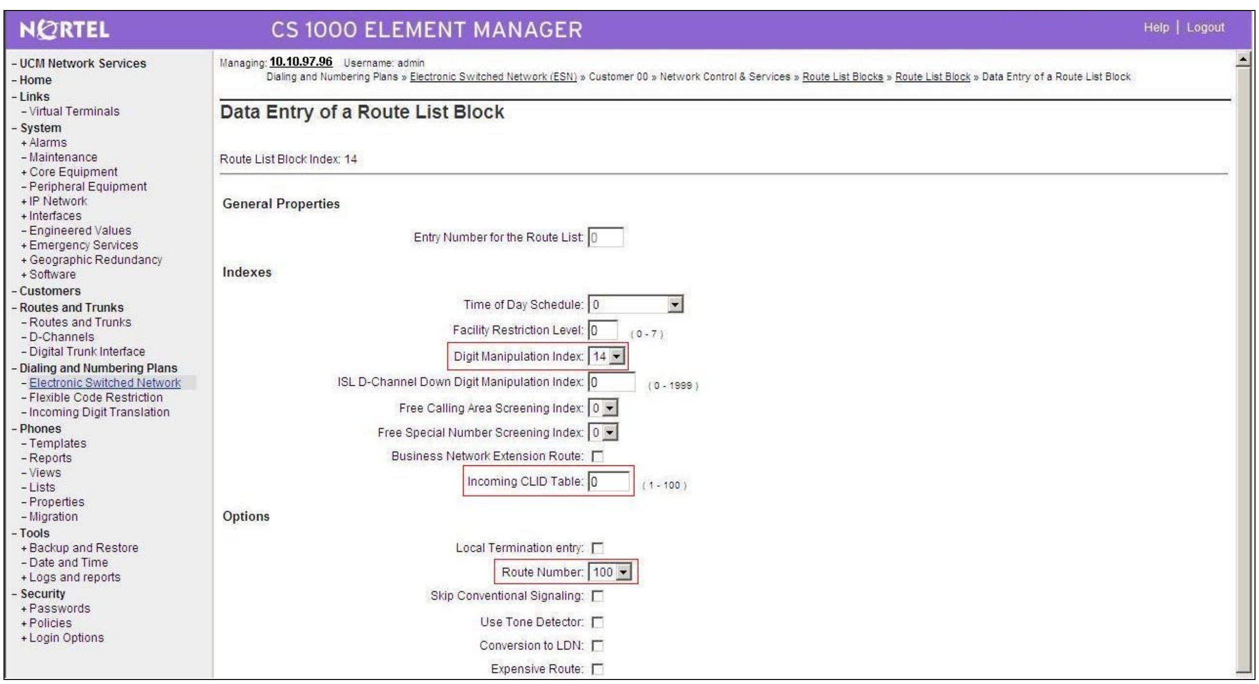

Figure 39a – RLB_14 Route List BlockConfigurationDetails

5.6.6. Route List Block (RLB) (RLB 15)

a) Select **Dialing and Numbering Plans** ->**Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Route List Block** (RLB) as shown in**Figure 34**.

b) Select an available value in the textbox for the **route list block index** (in this case is 15) and click on the**“to Add”**buttonas shown in **Figure 38**.

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 39b**).Scroll down to the bottom of the screen, and click on the**Submit** button.

- **Route number** (ROUT) : 100 (created in **Section 5.5.5**)
- **Digit Manipulation Index** (DMI): 15 (created in **Section 5.6.4**)
- **Incoming CLID Table**: 0 (created in **Section 5.5.7**)

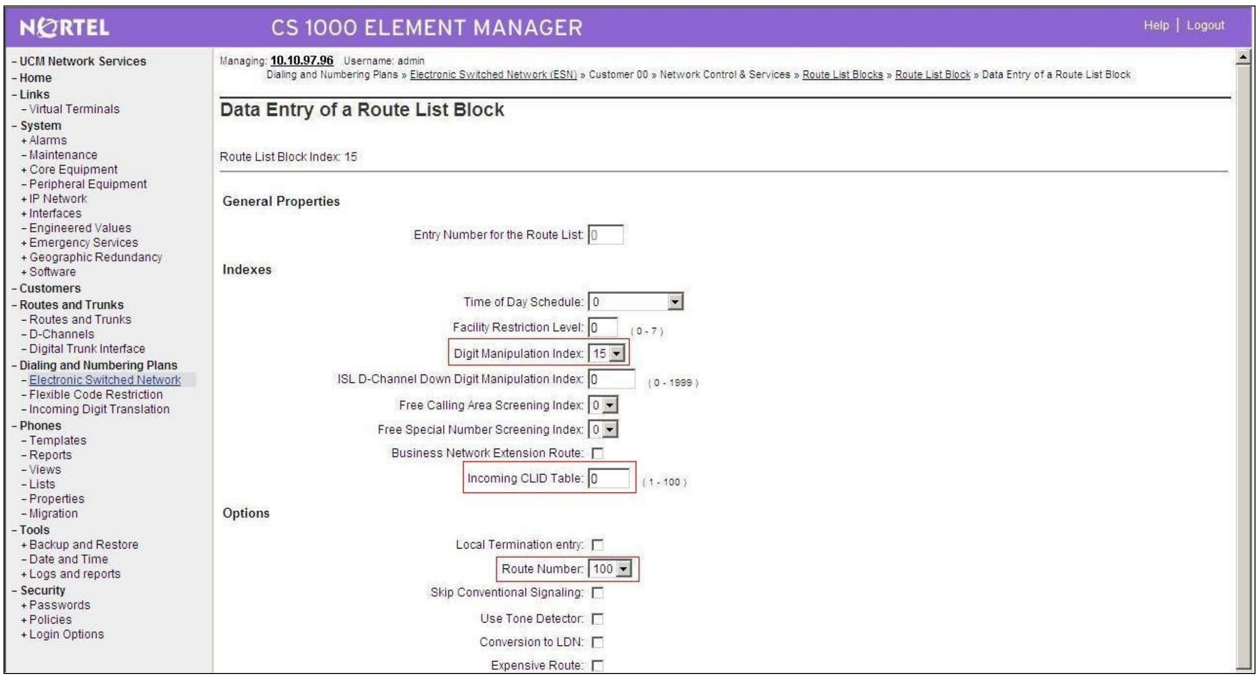

Figure 39b – RLB_15 Route List BlockConfigurationDetails

5.6.7. Inbound Call – Incoming Digit Translation Configuration

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

a) 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 40**.

Figure 40 – Incoming Digit Translation

b) Click on the **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number 1 has been created as shown in **Figure 41**.

Figure 41 – Incoming Digit Conversion Property

c) Detail configuration of the Digit Conversion TreeConfiguration is shown in **Figure 42**. The**Incoming Digits** can be added to map to the Converted Digits which would be the Communication Server 1000 system phones DN. This **DCN0** has been assigned to route 100 as shown in **Figure 26** and **27**.
In the following configuration, the incoming call from PSTN with the prefix 501287xxxx will be translated to DN xxxx. The DID number 5012871072 is translated to 1700 for Voicemail accessing purpose.

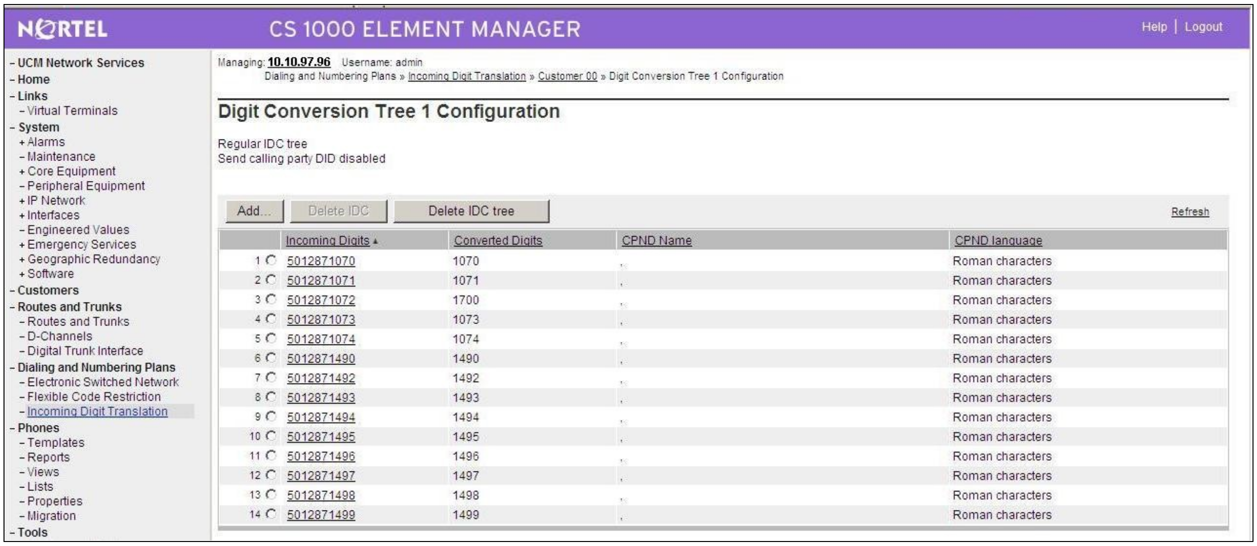

Figure 42 – Digit Conversion Tree

5.6.8. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 011, 1800, 411, 911 and so on.

a) Select **Dialing and Numbering Plans** ->**Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Special Number** (SPN) as shown in **Figure 34**.

b) Enter SPN number and then click on **to Add** button. **Figure 43**shows all the special number used for this testing.

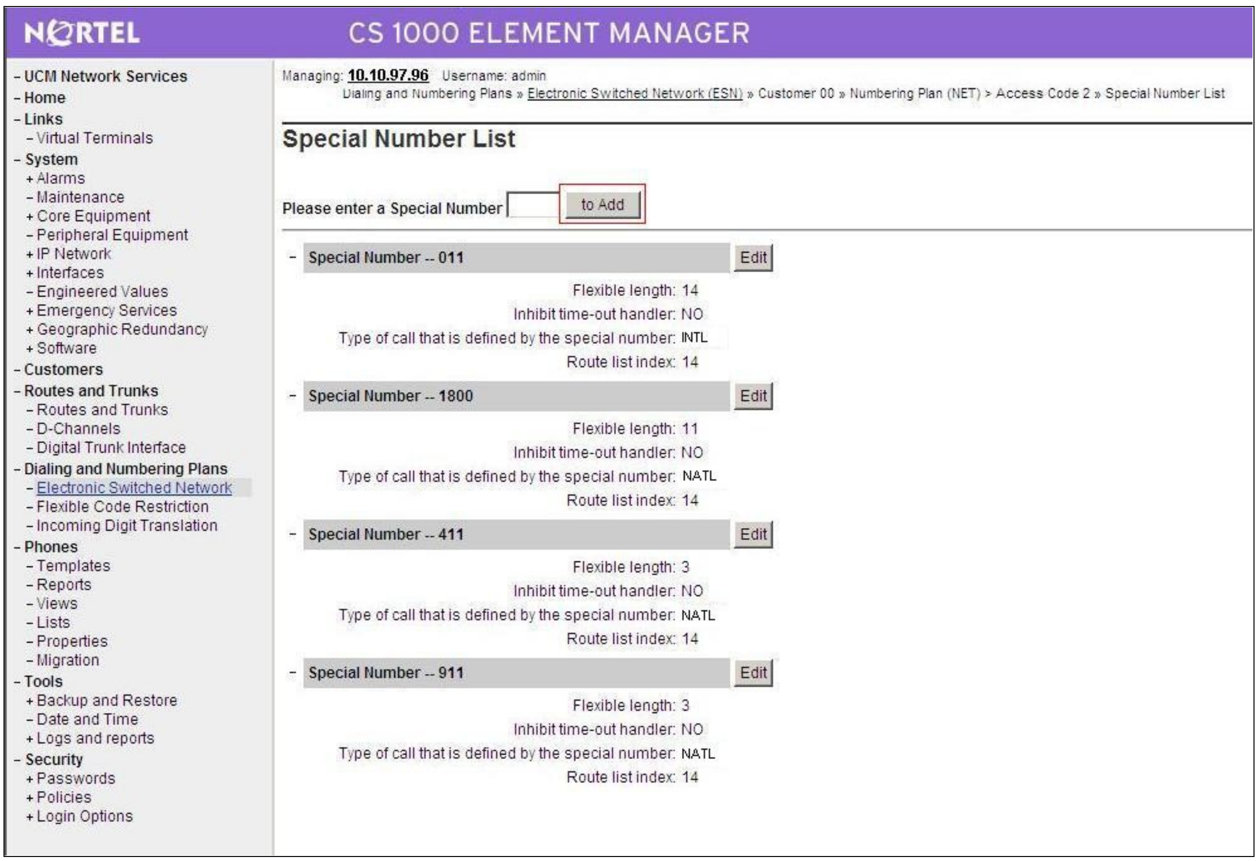

Figure 43 – Add a SPN.

5.6.9. Outbound Call - Numbering Plan Area (NPA)

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

a) Select **Dialing and Numbering Plans** ->**Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Numbering Plan Area Code** (NPA) as shown in **Figure 34**.
b) Enter the area code desired in the text box and click on the **"to Add"** button. The 1501,1613 and 1647 area codes were used in this configuration as shown in **Figure 44**.

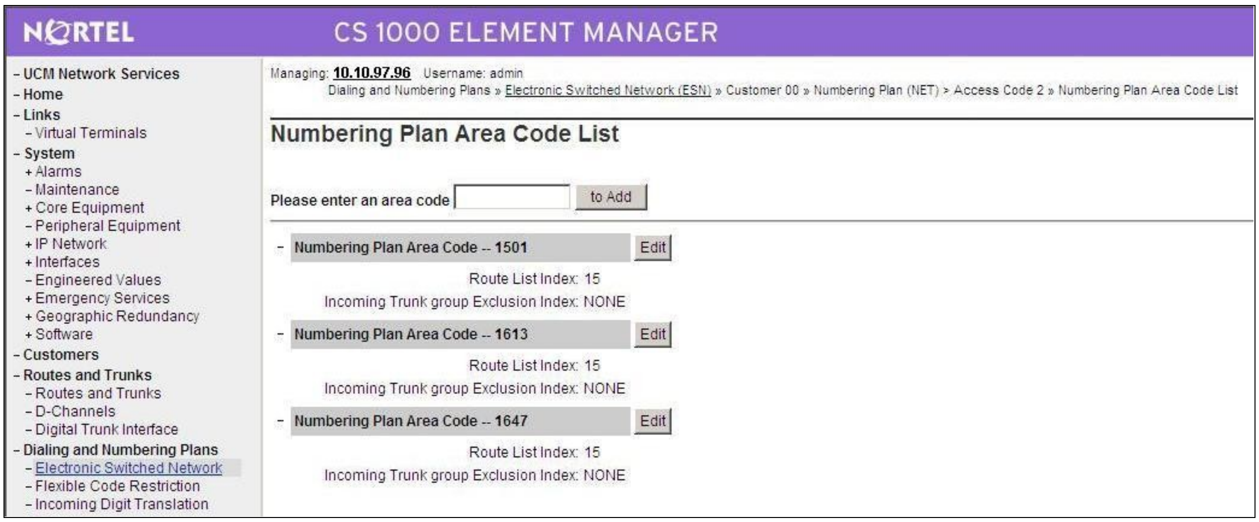

Figure 44 – Numbering Plan Area Code List

5.7. Administer Phone

This section describes the creation of Communication Server 1000 clients used in this configuration.

5.7.1. Phone creation

a) Refer to **Section 5.5.4** to create a virtual super-loop - **96** used for IP phone.
b) Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone.
c) Login Call ServerCommand Line Interface (please refer to **Section 5.1.2** for more detail).
d) Create an IP phone by using **LD 11**.

```
REQ: prt
TYPE: 2002p2
TN   96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  2002P2
TN   96 0 00 02  VIRTUAL
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010
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 FBD WTA LPR MTD FND HTD TDD CRPD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED 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 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 1492 0     MARP
      CPND
        CPND_LANG ROMAN
NAME Carrier1
          XPLN 13
          DISPLAY_FMT FIRST,LAST
    01
    02
<Text removed for brevity>
```

5.7.2. Enable Privacy for Phone

In this section, it shows how to enable Privacy for a phone by changing its class of service (CLS). By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately.

a) To hide the display name, set CLS to **namd**. Communication Server 1000 will include “Privacy:user” in the SIP message header before sending it to the Service Provider.

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

b) To hide the display number, set CLS to **ddgd**. Communication Server 1000 will include “Privacy:id” in the SIP message header before sending it to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN   96 0 0 2
```

```
ECHG yes
ITEM clsddgd
…
```

c) To hide display name and number, set CLS to **namd, ddgd**. Communication Server 1000 will include “Privacy:id, user” in the SIP message header before sendingto the Service Provider.

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

d) To allow display name and number, set CLS to **nama, ddga**. Communication Server 1000 will not send the Privacy header to the Service Provider.

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

5.7.3. Enable Call Forward for Phone

In this section, it shows how to configure the Call Forward feature at the system and phone level.

a) Select **Customer**->**00**->**CallRedirection**. The Call Redirection page is shown in **Figure 45**.

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

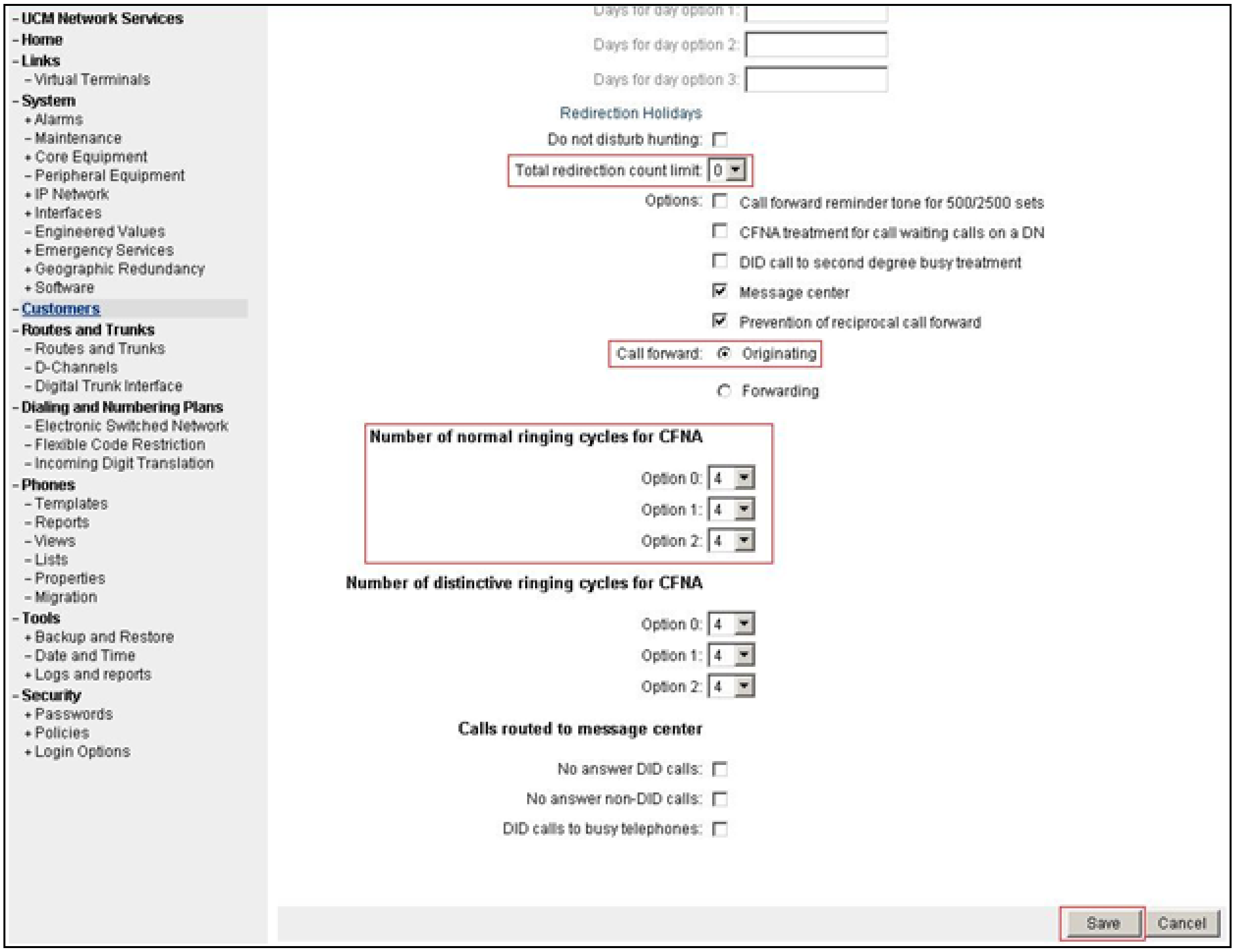

Figure 45 – Call Redirection

b) To enable **Call Forward All Call** (**CFAC**) for a phone over a trunk, use**LD 11**, change its CLS to **CXFA**, **SFA** then program the forward number on the phone set. Following is the configuration of a phone that has **CFAC** enabled with forwarding number 916139675205

```
REQ: prt
TYPE: 2007
TN   96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  2007
TN   96 0 00 04  VIRTUAL
TYPE 2007
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
    ICDA CDMA LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXA ARHD CLTD ASCD
…
    19 CFW 16  916139675205
…
```

d) To enable **Call Forward Busy (CFB)** for phone over trunk by using **LD 11**, change its **CLS** to **FBA, HTA,SFA** then program the forward number as is **HUNT**. Following is the configuration of a phone has **CFB** enabled with forward number is 916139675205

```
REQ: prt
TYPE: 2007
TN   96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  2007
TN   96 0 00 04  VIRTUAL
TYPE 2007
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
…
FDN 916139675205
HUNT916139675205
…
```

c) To enable **Call Forward No Answer (CFNA)** for a phone over a trunk by using **LD 11**, change its **CLS** to **FNA, SFA** then program the forward number as **FDN**. Following is the configuration of a phone that has CFNA enabled with forward number 916139675205

```
REQ: prt
TYPE: 2007
TN   96 0 0 4
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  2007
TN   96 0 00 04  VIRTUAL
TYPE 2007
…
FDN  916139675205
HUNT  916139675205

…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
  …
```

5.7.4. Enable Call Waiting for Phone

In this section, it shows how to configure Call Waiting feature at phone level.
Login Call Server CLI (please refer to **Section 5.1.2** for more detail), configure Call Waiting feature for phone by using **LD 11** to change **CLS** to **HTD**, **SWA** and adding a **CWT** key.

```
REQ: prt
TYPE: 2002p2


TN   96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES  2002P2
TN   96 0 00 02  VIRTUAL
TYPE 2002P2
…
CLS  UNR FBD WTA LPR MTD FNA HTD TDD HFD CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWA LNA CNDA
…
KEY  00 SCR 1492 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Carrier1
            XPLN 13
            DISPLAY_FMT FIRST,LAST
     01 CWT
…
```

5.8. NRS/SPS Configuration

In this section, it shows how to configure a NRS/SPS on Communication Server 1000. Follow the steps bellow to setup the NRS/SPS server.It is assumed that the NRS/SPS has been deployed on the Communication Server 1000 UCM environment with all latest Service Pack applied.

5.8.1. Create a New Domain Name on NRS/SPS

In this section, it shows how to create a new domain name for this test configuration.
a) Under the **Element Names**, select the **NRSM on car3-sps**
b) The **Network Routing Service Manager** page will appear, click on the radio button of the **Standby database**. Then select **Numbering Plan ->Domains.** Click on the **Service Domain (1)** tab then click on the **Add** button to add a new domain as shown in **Figure 46**.

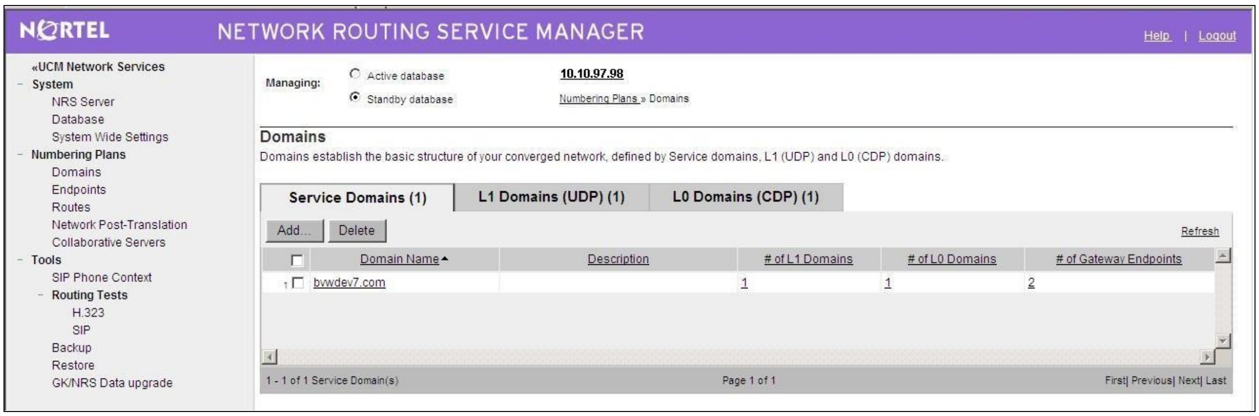

Figure 46 – Add Domain Name

c) Enter the domain name to be added; in this case it is bvwdev7.com. Then click on the**Save** button.
d) Select the **L1 Domains (UDP) (1),** from the **Filter by Domain**, select the newly created domain **bvwdev7.com**. Click on the **Add** button and enter **udp** as L1 Domain name. Then click on the**Save**button (not shown).
e) Select the **L0 Domains (CDP) (1),** from the **Filter by Domain**, select the newly created domain **bvwdev7.com**. Click on the **All L1 Domain** pull down menu to choose the **udp**. Click on the **Add** button and enter **cdp** as L0 Domain name. Then click on the**Save**button (not shown).
f) From the left menu column, select **System ->Database.** Then click on the **Cut Over** button to transfer the configured data of the domain name to save it to the **Active Database.** Click on the **Commit** button (not shown).

5.8.2. Configure NRS/SPS to create Gateway Endpoints for the SIP Signaling Gateway

This section shows how to add the SIP Signaling Gateway as a dynamic gateway endpoint on the NRS/SPS.

a) Click on the radio button of the **Standby database**, select the **Numbering Plan** ->**Endpoints**. Enter the endpoint name and choose the values which are highlighted in red boxes as shown in **Figure 47**. Click on the **Add** button to create new gateway endpoint.

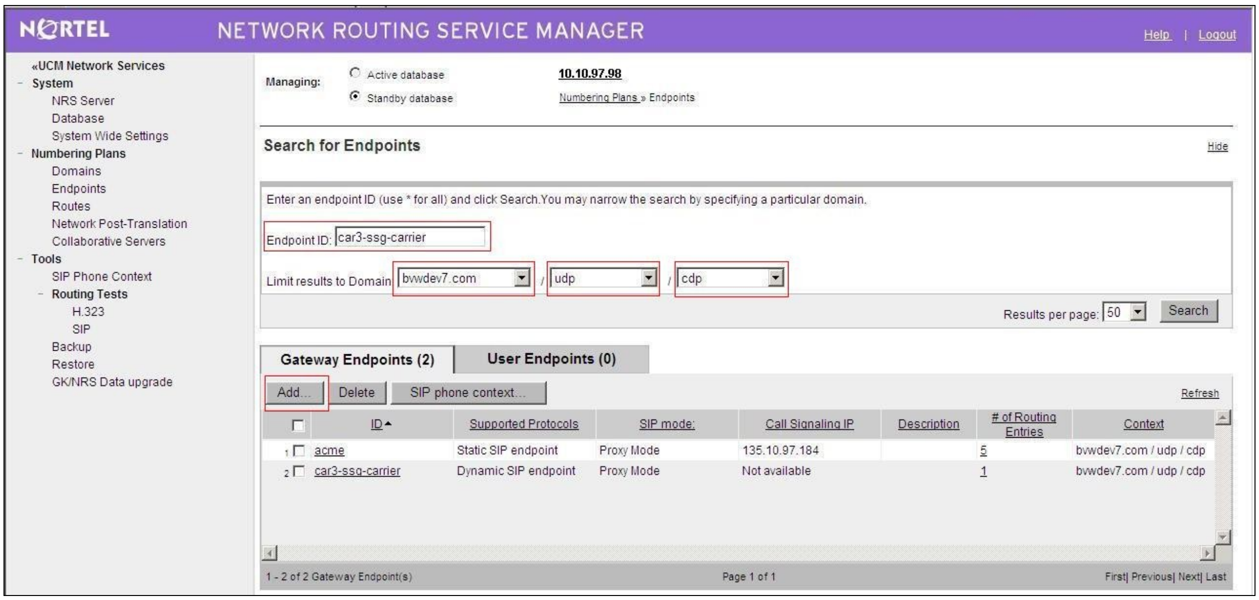

Figure 47 – Adding New Gateway Endpoints

b) The detail gateway endpoint configuration page will appear. Using the values for the highlighted attributes in red boxes as shown in **Figures 48** and **49** and click on the**Save**button.

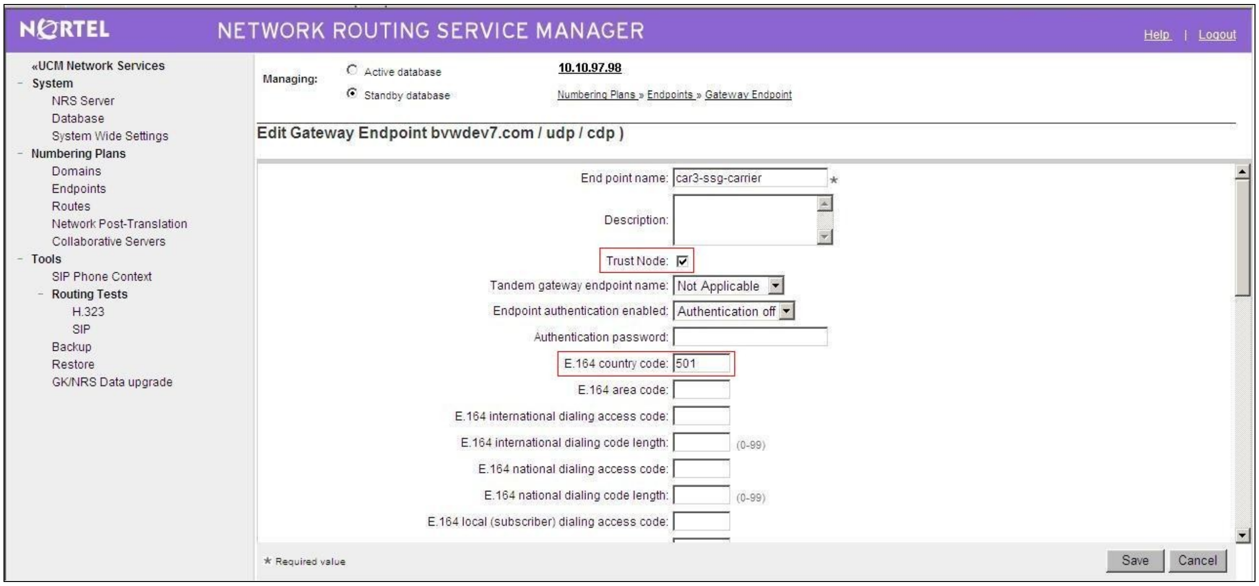

Figure 48 – SSG Gateway Endpoint Details Configuration

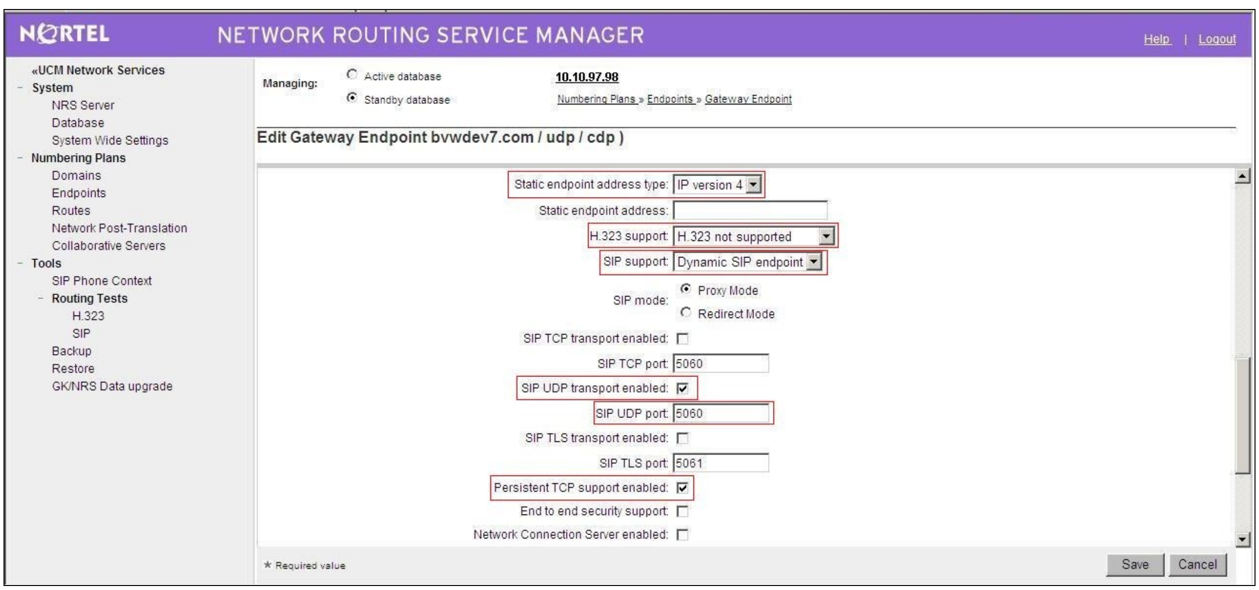

Figure 49 – SSG Gateway Endpoint Details Configuration

c) From the left menu column, select **System** ->**Database.** Then click on the **Cut Over** button to transfer the configured data of the domain name to save in to the **Active Database.** Click on the **Commit** button (not shown).

5.8.3. Create a Static Gateway Endpoint for the ACME Session Border Controller

This section shows how to add the Session Border Controller as a static gateway endpoint on the NRS/SPS.

a) Click on the radio button of the **Standby database**, select the **Numbering Plan** ->**Endpoints**. Enter the endpoint name for the ACME session border controller as **acme** and choose the values "Limit results Domain: **bwvdev7.com/udp/cdp**". Click on the **Add** button.

b) The detail gateway endpoint configuration page will appear. For the Static Endpoint IP Address, enter the ACME internal (private side) IP address and use the values for the highlighted attributes in red boxes as shown in **Figure 51**, **Figure52**. Click on the**Save** button.

c) From the left menu column, select **System** ->**Database.** Then click on the **Cut Over** button to transfer the configured data of the domain name to save it to the **Active Database.** Click on the **Commit** button (not shown).

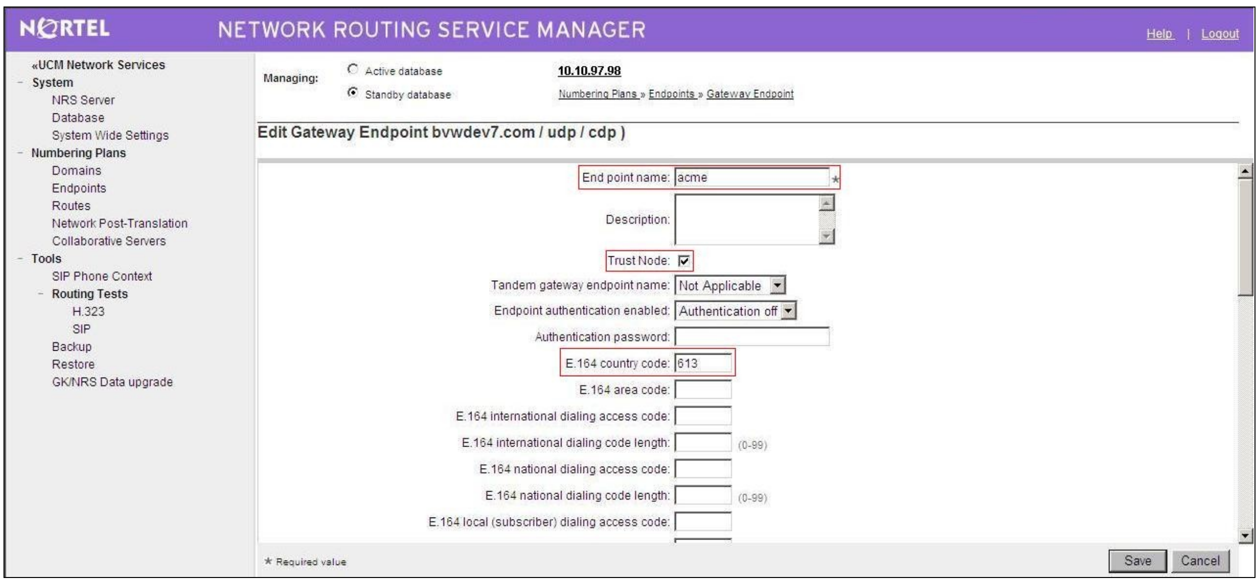

Figure 50 – ACME Gateway Endpoint Details Configuration

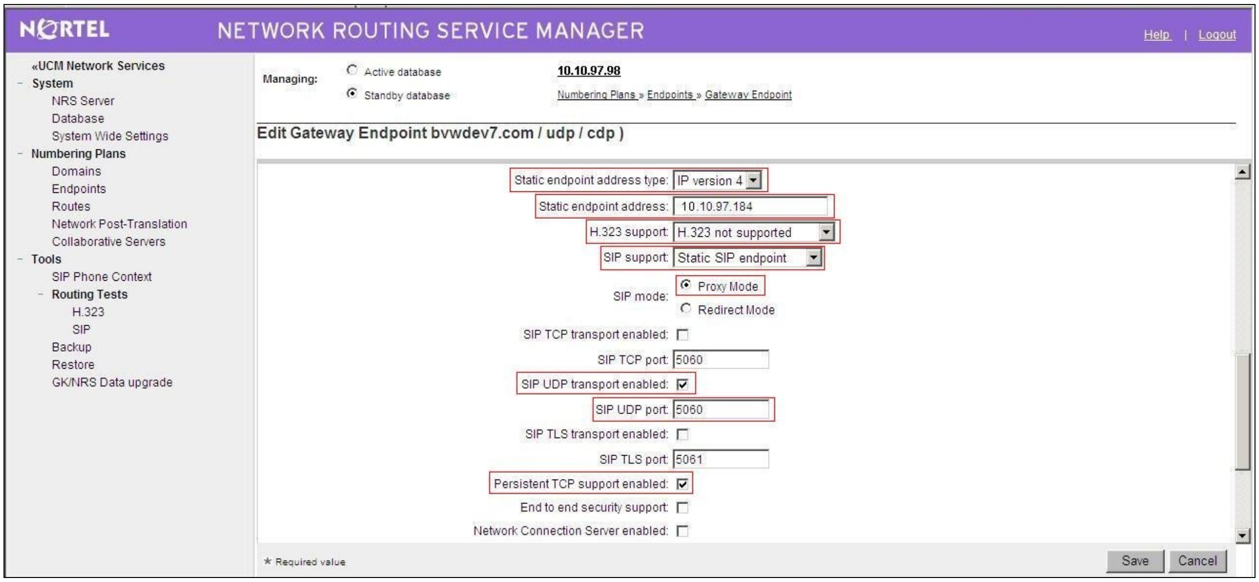

Figure 51 – ACME Gateway Endpoint Details Configuration

Note: After adding the SIP Signaling Gateway (SSG) and the ACME session border controller to the NRS/SPS, Active database shows IP addresses of the gateways(highlighted redbox) and both SSG and **acme** gatewaysare successfully registered to NRS/SPS (as shown in **Figure 52**)

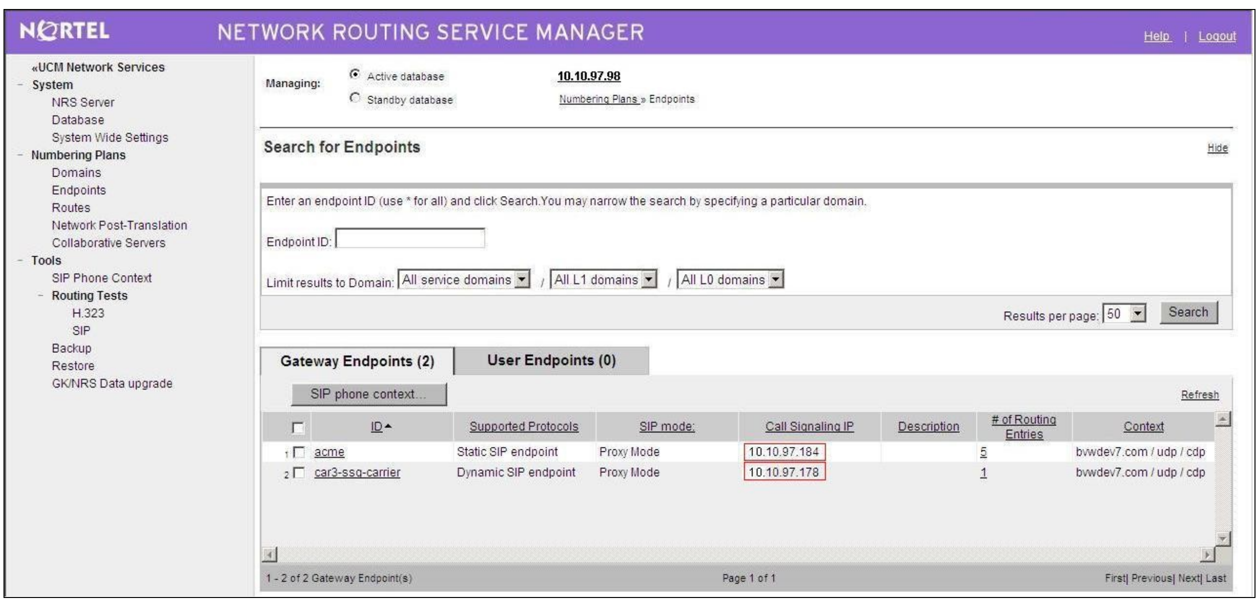

Figure 52 – SSG and ACME successfully register to NRS/SPS

5.8.4. Creating Routing Entry for the SSG on the NRS/SPS

In this section, it describes how to create the routing entry on the NRS/SPS to route the inbound calls. In the test configuration, we have used the routing entry 501 which is sent from Windstream as the first 3 digits of the DIDs range, 501 - XXX – XXXX.

a) Click on radio button **Standby database**, then on the Network Routing Service Manager page as shown in **Figure 46**, on the left menu column, select **Numbering Plan** ->**Routes**. On the Routing Entries page, choose and change the attributes highlighted in red boxes to the values as shown in **Figure 53**. Click the **Add** button.

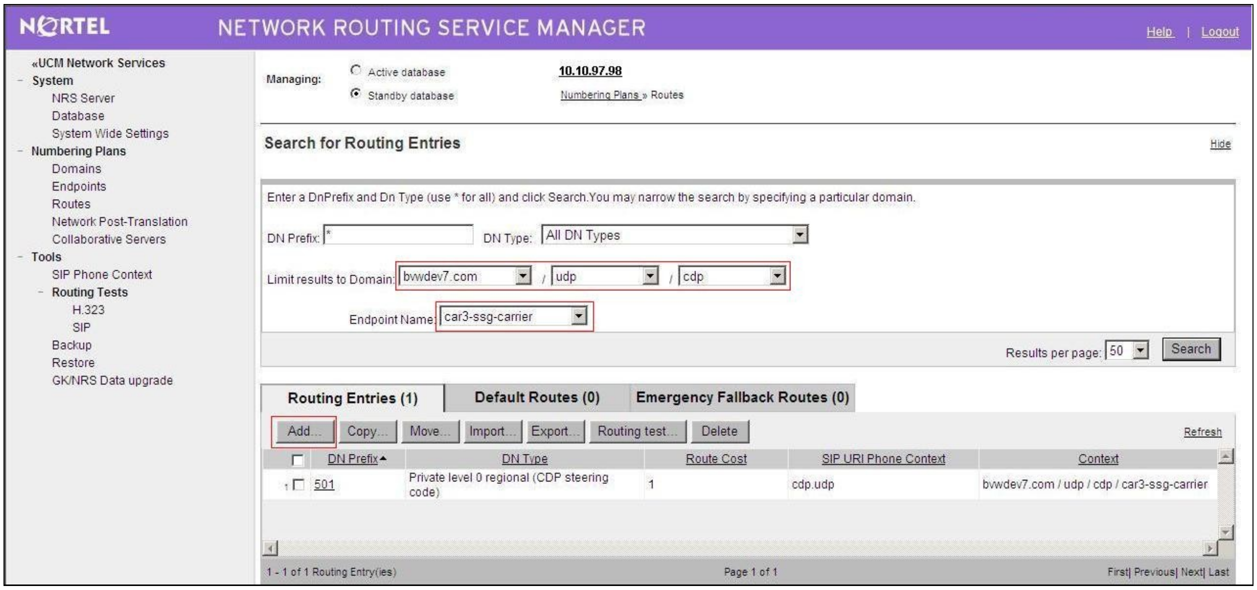

Figure 53 – Routing Entries Page

b) The Routing Entries page will appear as shown in **Figure 54**. Fill in the textboxes with the values highlighted in red boxes. Then click on the **Save** button.
- DN Type: **Private level 0 regional (CDP steering code)**
- DN Prefix: **501**
- Route cost: **1**

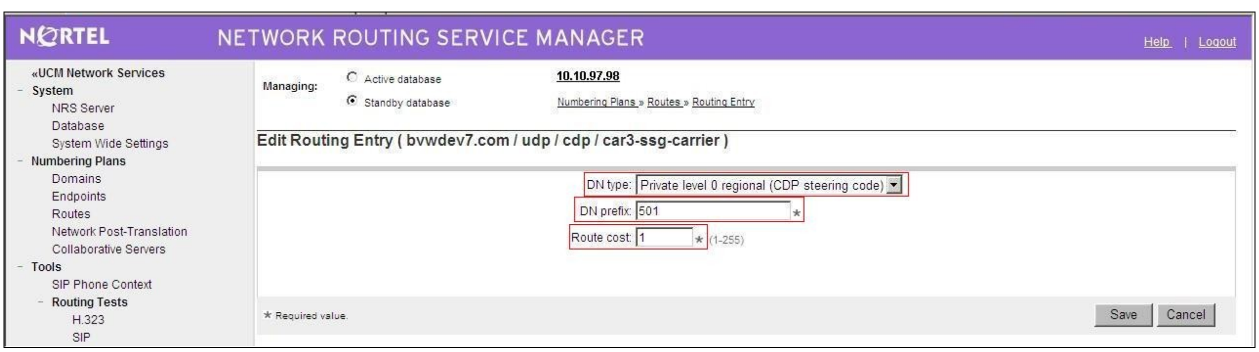

Figure 54 – Routing Entries Configuration Details Page

c) From the left menu column, select **System ->Database.** Then click on the **Cut Over** button to transfer the configured data of the domain name to save in to the **Active Database.** Click on the **Commit** button (not shown).

5.8.5. Creating Routing Entry for the ACME on the NRS/SPS

This section describes how to create the routing entry on the NRS/SPS to route the call from NRS/SPS to the ACME session border controller. In the test configuration, we have used the routing entries 011, 411, 911, 1800, 613, 647, 1613 and 501. In the following example, it shows only one entry 613. Others entries can be done the same way.

a) Click on radio button **Standby database**, then on the Network Routing Service Manager page as shown in **Figure 46**, select **Numbering Plan ->Routes**. On the Routing Entries page, choose and change the attributes highlighted in red boxes to the values as shown in **Figure 55**. Click the **Add** button.

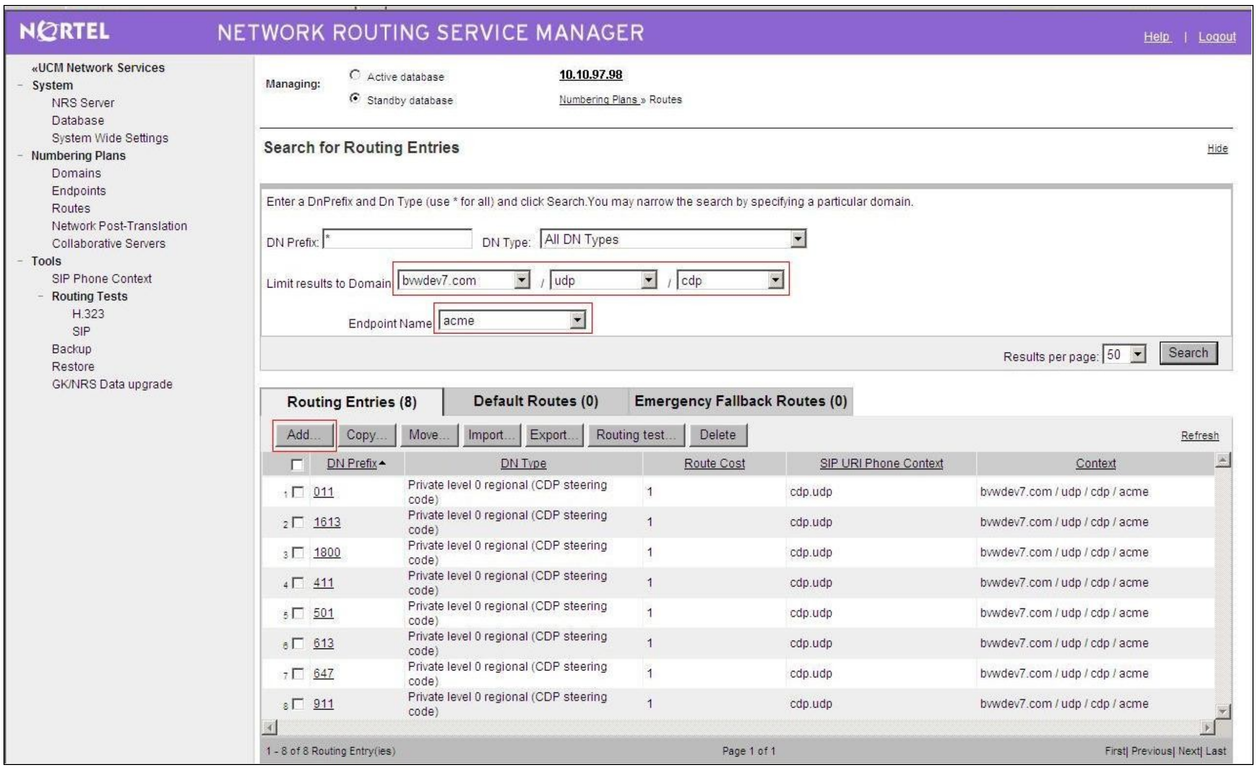

Figure 55 – Add a Routing Entry for ACME

b) The Routing Entries page will appear as shown in **Figure 56**. Fill in the textboxes with the values highlighted in red boxes. Then click on the **Save** button.

DN Type:Private level 0 regional (CDP steering code)

- **DN Prefix:**613
- **Route cost:**1

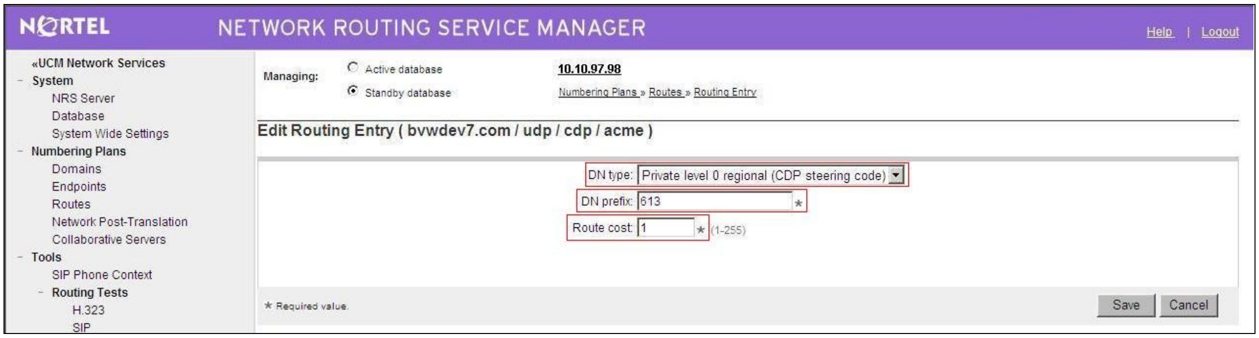

Figure 56 – Routing Entry Configuration Details for ACME

c) From the left menu column, select **System ->Database.** Then click on the **Cut Over** button to transfer the configured data of the domain name to save in to the **Active Database.** Click on the **Commit** button (not shown).

6. Configure Acme Packet Net-Net 3800

This section describes the configuration of the Acme Packet Net-Net 3800 necessary for interoperability with the Communication Server 1000 and Windstream systems. The Net-Net 3800 was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet products.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to Communication Server 1000. The remaining fields are generally the default/standard value used by the Net-Net 3800 for that field.

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

6.1. Acme Packet Command Line Interface Summary

The Net-Net 3800 is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Net-Net 3800 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Net-Net 3800 server for cable connection). Use the following settings for the serial port on the PC.
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
2. Log in to the Net-Net 3800 with the user password.
3. Enable the Super-user mode by entering the **enable** command and then the superuser password. The command prompt will change to include a "#" instead of a ">" while in Superuser mode. This level of system access (i.e. at the "acmesystem#" prompt) will be

referred to as the ***main*** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific ***elements*** and specific ***parameters*** of those elements.

4. In Super-user mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the ***configuration*** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface).**
7. Enter the name of an element parameter followed by its value (e.g., **name INSIDE**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

Note – Net-Net 3800 provisioning applicable to the reference configuration is shown in **bold**text. Other parameters and setting are shown for informational purposes.

6.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet slot 0/port 0 was connected to the internal corporate LAN. The Ethernet interface slot 1/port 0 was connected to the external un-trusted network. A network interface was defined for each physical interface to assign it a routable IP address.

The physical interface below defines the ports on theinterface connected to the network on which the Avaya elements reside.

```
phy-interface
name                    INSIDE
operation-type          Media
port                    0
    slot                    0
    virtual-mac
    admin-state             enabled
    auto-negotiation        enabled
    duplex-mode             FULL
    speed                   100
    overload-protection     disabled
    last-modified-by        admin@console
    last-modified-date      2011-06-07 10:11:20
```

The physical interface below defines the ports on theinterface connected to the network on which the Windstream elements reside.

```
phy-interface
name         OUTSIDE
    operation-type          Media
    port                    0
    slot                    1
    virtual-mac
    admin-state             enabled
    auto-negotiation        enabled
    duplex-mode             FULL
    speed                   100
    overload-protection     disabled
    last-modified-by        admin@console
    last-modified-date      2011-06-07 10:11:30
```

The network interface below defines the IP addresses on theinterface connected to the network on which the Avaya elements reside.

```
network-interface
name                    INSIDE
    sub-port-id         0
    description
    hostname
ip-address              10.10.97.184
pri-utility-addr
    sec-utility-addr
netmask         255.255.255.192
gateway                 10.10.97.129
    sec-gateway
gw-heartbeat
        state                   disabled
        heartbeat               0
        retry-count             0
        retry-timeout           1
        health-score            0
dns-ip-primary
    dns-ip-backup1
    dns-ip-backup2
dns-domain
dns-timeout             11
hip-ip-list             10.10.97.184
    ftp-address
icmp-address        10.10.97.184
snmp-address
    telnet-address
ssh-address
    last-modified-by        admin@console
    last-modified-date      2011-06-07 10:20:11
```

The network interface below defines the IP addresses on theinterface connected to the network on which the Windstream elements reside.

network-interface	
name	**OUTSIDE**
sub-port-id	0
description	
hostname	
ip-address	**10.10.98.98**
pri-utility-addr	
sec-utility-addr	
netmask	**255.255.255.224**
gateway	**10.10.98.97**
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	**10.10.98.98**
ftp-address	
icmp-address	**10.10.98.98**
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@console
last-modified-date	2011-06-07 15:22:28

6.3. Realm

A realm represents a group of related Net-Net 3800 components. Two realms were defined for the compliance test.
The realm configuration “INSIDE” below represents the internal network on which the Avayaelements reside.

```
realm-config
identifier                    INSIDE
    description
addr-prefix                   0.0.0.0
network-interfaces
      INSIDE:0
    mm-in-realm               disabled

      <Text removed for brevity>
```

The realm configuration “OUTSIDE” below represents the externalnetwork on which the Windstream system resides.

```
realm-config
identifier                    OUTSIDE
    description
addr-prefix                   0.0.0.0
network-interfaces
                   OUTSIDE:0
    mm-in-realm               disabled

      <Text removed for brevity>
```

6.4. Session Agent

A session agent defines the characteristics of a signaling peer to the Net-Net 3800.
The **session agent** below represents the Windstream border element. The Acme will attempt to send calls to the border element. The **in-manipulationid** and **out-manipulationid** define the SIP header manipulation applying to the OUTSIDE realm.

```
session-agent
hostname                          20.20.242.26
ip-address                        20.20.242.26
    port                          5060
    state                         enabled
app-protocol                SIP
    app-type
transport-method            UDP
    realm-id                      OUTSIDE
    egress-realm-id
description                       Windstream_CS1K 7.0
    carriers
    allow-next-hop-lp       enabled
    constraints                   disabled

      <Text removed for brevity>

    ping-interval                 0
ping-send-mode               keep-alive

      <Text removed for brevity>

    ping-from-user-part
    li-trust-me                   disabled
in-manipulationid    WS_TO_CS1K7_NAT_IP
    out-manipulationid      CS1K7_TO_WS_NAT_IP
    manipulation-string
```

The **session agent** below represents the configuration for inside interface to connect to NRS mentioned in **Section 5.8**

```
session-agent
hostname                        10.10.97.183
ip-address                      10.10.97.183
    port                        5060
    state                       enabled
app-protocol                SIP
    app-type
transport-method            UDP
realm-id                        INSIDE
    egress-realm-id
description                     Windstream_CS1K7.0
    carriers
    allow-next-hop-lp       enabled
    constraints                 disabled
      <Text removed for brevity>
```

6.5. SIP Configuration

The SIP configuration (***sip-config***) defines the global system-wide SIP parameters.
The key SIP configuration (***sip-config***) field is:

- **home-realm-id**: The name of the realm on the private side of the Net-Net 3800.
- **egress-realm-id**: Thename of the realm on the private side of the Net-Net 3800.

```
sip-config
    state                       enabled
    operation-mode              dialog
    dialog-transparency         enabled
home-realm-id               INSIDE
    egress-realm-id             INSIDE
nat-mode                        None

      <Text removed for brevity>
```

6.6. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on the Net-Net 3800. Two SIP interfaces were defined; one for each realm.

The SIP interface below is used tocommunicate with the Communication Server 1000 system.

```
sip-interface
      state                             enabled
realm-id                                INSIDE
      description
      sip-port
address                                 10.10.97.184
            port                                 5060
            transport-protocol                   UDP
tls-profile
            allow-anonymous                      all

         <Text removed for brevity>
```

The SIP interface below is used tocommunicate with the Windstream system.

```
sip-interface
      state                             enabled
realm-id                                OUTSIDE
      description
      sip-port
address                                 10.10.98.98
            port                                 5060
            transport-protocol                   UDP
tls-profile
            allow-anonymous                      all

         <Text removed for brevity>
```

6.7. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. The following sip-manipulation **CS1K7_TO_WS_NAT_IP** is applied to **OUTSIDE** realm***out-manipulationid***. These rules perform the following:

- The header rule**manipRURI**changes Avaya Domain Name/IP address to 20.20.242.26(Windstream border element) in the Request URI headers sent to Windstream.
- The header rule**manipTo**performs address translation and topology hiding for SIP messages between the Windstream system and the Avaya elements.

```
sip-manipulation
name            CS1K7_TO_WS_NAT_IP
    description
    split-headers
    join-headers
    header-rule
name                              manipRURI
        header-name                       request-uri
        action                            manipulate
        comparison-type                   case-sensitive
msg-type                          any
        methods                           INVITE
        match-value
        new-value
        element-rule
name                              modRURI
            parameter-name
type                              uri-host
            action                                replace
            match-val-type                        any
            comparison-type                       case-sensitive
            match-value
new-value                         20.20.242.26
    header-rule
name                              manipTo
        header-name                       To
        action                            manipulate
        comparison-type                   case-sensitive
msg-type                          any
        methods
        match-value
        new-value
        element-rule
```

name	**To**
parameter-name	
type	**uri-host**
action	**replace**
match-val-type	**any**
comparison-type	**case-sensitive**
match-value	
new-value	**$REMOTE_IP**
header-rule	
name	**HistRegex**
header-name	**History-Info**
action	**store**
comparison-type	**pattern-rule**
msg-type	**request**
methods	**INVITE**
match-value	**()**
new-value	
element-rule	
name	**GetUser**
parameter-name	
type	**uri-user**
action	**store**
match-val-type	**any**
comparison-type	**pattern-rule**
match-value	
new-value	
element-rule	
name	**GetHost**
parameter-name	
type	**uri-host**
action	**store**
match-val-type	**any**
comparison-type	**pattern-rule**
match-value	
new-value	
element-rule	
name	**GetUserReason1**
parameter-name	
type	**header-value**
action	**store**
match-val-type	**any**
comparison-type	**pattern-rule**
match-value	**(.*)(Moved)(.*)**
new-value	
element-rule	

```
name                            GetUserReason2
            parameter-name
type                            header-value
            action                          store
            match-val-type                  any
            comparison-type                 pattern-rule
            match-value                     (.*)(Busy)(.*)
            new-value
        element-rule
name                            GetUserReason3
            parameter-name
type                            header-value
            action                          store
            match-val-type                  any
comparison-type                 pattern-rule
            match-value                     (.*)(Unavailable)(.*)
            new-value
    header-rule
name                            AddDiversion1
        header-name                     Diversion
        action                          add
        comparison-type                 boolean
msg-type                        request
        methods                         INVITE
        match-value                     $HistRegex[0].$GetUserReason1
        new-value                       <sip:+$HistRegex[0].$GetUser.$0+@+
                                        $HistRegex[0].$GetHost.$0+>;privacy=off;
                                        reason=unconditional;screen=no
    header-rule
name                            AddDiversion2
        header-name                     Diversion
        action                          add
        comparison-type                 boolean
msg-type                        request
        methods                         INVITE
        match-value                     $HistRegex[0].$GetUserReason2
        new-value

                                            <sip:+$HistRegex[0].$GetUser.$0+@+$Hi
                                        stRegex[0].$GetHost.$0+>;privacy=off;
                                        reason=user\-busy;screen=no
    header-rule
name                            AddDiversion3
        header-name                     Diversion
        action                          add
        comparison-type                 boolean
```

```
msg-type                        request
          methods                      INVITE
          match-value                  $HistRegex[0].$GetUserReason3
          new-value                    <sip:+$HistRegex[0].$GetUser.$0+@+
$HistRegex[0].$GetHost.$0+>;privacy=off;
reason=no\-answer;screen=no
     header-rule
name                            delHistInfo
          header-name                  History-Info
          action                       delete
          comparison-type              case-sensitive
msg-type                        any
          methods                      INVITE
          match-value
          new-value
     header-rule
name                            manipFrom
          header-name                  From
          action                       manipulate
          comparison-type              case-sensitive
msg-type                        any
          methods
          match-value
          new-value
          element-rule
name                            From
               parameter-name
type                            uri-host
               action                       replace
               match-val-type               any
               comparison-type              case-sensitive
               match-value
new-value                       10.10.98.98
     last-modified-by           admin@console
     last-modified-date         2011-07-06 21:42:22
```

The following sip-manipulation **WS_TO_CS1K7_NAT_IP,** ***in-manipulationid,*** is applied to **OUTSIDE**realm and translates the SIP header information for Communication Server 1000 to understand. These rules perform the following:

- The header rules**manipRURI**changesIP address to the Avaya Communication Server 1000 Domain Name in the Request URI headers sent to the Communication Server 1000 elements.

```
sip-manipulation
name                            WS_TO_CS1K7_NAT_IP
```

```
      description
      split-headers
      join-headers
      header-rule
name                            manipRURI
          header-name                   request-uri
          action                        manipulate
          comparison-type               case-sensitive
msg-type                        any
          methods                       INVITE
          match-value
          new-value
          element-rule
name                            modRURI
               parameter-name
type                            uri-host
               action                          replace
               match-val-type                  any
               comparison-type                 case-sensitive
               match-value
new-value                       bvwdev7.com
      header-rule
name                            manipTo
header-name                     To
          action                        manipulate
          comparison-type               case-sensitive
msg-type                        any
          methods
          match-value
          new-value
          element-rule
name                            To
               parameter-name
type                            uri-host
               action                          replace
               match-val-type                  any
               comparison-type                 case-sensitive
               match-value
new-value                       bvwdev7.com
      last-modified-by          admin@console
      last-modified-date        2011-06-07 12:52:23
```

6.8. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.
The key steering pool (***steering-pool***) fields are:

- **ip-address:** The address of the interface on the Net-Net 3800.
- **start-port:** An even number of the port that begins the range.
- **end-port:** An odd number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

```
steering-pool
ip-address                    10.10.98.98
start-port                    20000
end-port                      40000
realm-id                      OUTSIDE
        network-interface
        last-modified-by      admin@console
        last-modified-date    2011-06-07 22:20:07
steering-pool
ip-address                    10.10.97.184
start-port                    20000
end-port                      40000
        realm-id              INSIDE
        network-interface
        last-modified-by      admin@console
        last-modified-date    2011-06-07 22:20:22
```

6.9. Local Policy

The local policies below govern the routing of SIP messages from elements on the network on which the Avaya elements, reside to the Windstream system and vice versa.

```
local-policy
        from-address
            20.20.242.26
        to-address
                            5012871070
            5012871071
            5012871072
            5012871073
                            5012871074
            5012871490
            5012871491
            5012871492
```

```
         5012871493
         5012871494
         5012871495
         5012871496
         5012871497
         5012871498
         5012871499
      source-realm
         OUTSIDE
      description          WS_TO_CS1K7
      activate-time                 N/A
      deactivate-time               N/A
      state                         enabled
      policy-priority               none
      last-modified-by              admin@console
      last-modified-date            2011-06-07 14:44:50
      policy-attribute
            next-hop                        10.10.97.183
            realm                           INSIDE
            action                          none
            terminate-recursion             disabled
            carrier
            start-time                      0000
            end-time                        2400
            days-of-week                    U-S
            cost                            0
            app-protocol                    SIP
            state                           enabled
            methods
            media-profiles
            lookup                          single
            next-key
eloc-str-lkup    disabled
eloc-str-match
```

```
local-policy
      from-address
         anonymous.invalid
         bvwdev7.com
      to-address
         *
      source-realm
         INSIDE
      description                   CS1K_TO_WS
```

```
    activate-time           N/A
    deactivate-time         N/A
    state                   enabled
    policy-priority         none
    last-modified-by        admin@console
    last-modified-date      2011-06-07 20:25:30
    policy-attribute
        next-hop                20.20.242.26
        realm                   OUTSIDE
        action                  none
        terminate-recursion     disabled
        carrier
        start-time              0000
        end-time                2400
        days-of-week            U-S
        cost                    0
        app-protocol            SIP
        state                   enabled
        methods
        media-profiles
        lookup                  single
        next-key
eloc-str-lkup   disabled
eloc-str-match
```

7. Verification Steps

The following steps may be used to verify the configuration.

7.1. 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 thatthe call remains stable for several minutes and disconnects properly.

7.2. Verification an Active Call on Call Server

a) Active Call Trace (LD 80)

The following is an example of one of the commands available on the Communication Server 1000 to trace the DN which the call is in progress and or idle.The call scenario involved PSTN phone number 6139675205 calling 5012871492.

- Login on to Signaling Server 10.10.97.177 with admin account and password.
- Issue a command “cslogin”call to login on to the Call Server.
- Login to the Overlay command prompt, issue the command**LD80** and then **trace 0 1492**.
- After the call is released, issue command **trac 0 1492** again to see if the DN is released back to idle state.

Bellow is the actual output of the Call Server Command Line mode when the 1492 is in call state:

```
USERID? admin
PASS?....
.
TTY #09 LOGGED IN admin 16:22  08/6/2011
.
>ld 80
.trac 0 1492

ACTIVE  VTN 96 0 00 02

ORIG   VTN 100 0 00 00   VTRK IPTI  RMBR  100 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 10.10.97.184
  FAR-END MEDIA ENDPOINT IP: 10.10.97.184  PORT: 21638
  FAR-END VendorID: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.00.20
TERM   VTN 96 0 00 02KEY 0  SCR MARP  CUST 0  DN 1492  TYPE 2002P2
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.10.98.36  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1492
MAIN_PM  ESTD
TALKSLOT  ORIG  17   TERM  81
QUEU  NONE
CALL ID 501 84

----  ISDN ISL CALL (ORIG) ----
CALL REF # =  484
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =    NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  5012871492  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call on 1492 is finished.

```
.trac 0 1492
IDLE VTN 96 0 00 02   MARP
```

b) SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675205) to an internal device (5012871492). Then check the SIP trunk status by using LD 32, one trunk is BUSY

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

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

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

7.3. Protocol Trace

Below is a wireshark trace of the same call scenario described in **Section 7.2**. It is shown in text format bellow. Note that only detail of the INVITE message is being shown here.

No. Time Source Destination Protocol Info
41 36.977060 20.20.242.26 10.10.98.98 SIP/SDP Request: INVITE sip:5012871492@10.10.98.98:5060, with session description

Frame 41: 841 bytes on wire (6728 bits), 841 bytes captured (6728 bits)
Ethernet II, Src: Nortel_01:b4:49 (00:17:65:01:b4:49), Dst: AcmePack_a1:8c:a5 (00:08:25:a1:8c:a5)
Internet Protocol, Src: 20.20.242.26 (20.20.242.26), Dst: 10.10.98.98 (10.10.98.98)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Request-Line: INVITE sip:5012871492@10.10.98.98:5060 SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 20.20.242.26:5060;branch=z9hG4bK1n34a920dgnhces1o081.1
    Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info
    Max-Forwards: 69
    Call-ID: E3F6469F@75.89.98.228
From: "Anonymous" <sip:6139675205@20.20.242.26:5060;transport=udp>;tag=75.89.98.228+1+23db11+c56cdbdc;isup-oli=00
    To: <sip:5012871492@10.10.98.98>
CSeq: 1006829771 INVITE
    Expires: 180
    Organization:
    Supported: 100rel
    Content-Length: 170
    Content-Type: application/sdp
    Contact: "Anonymous" <sip:61396715205@20.20.242.26:5060;transport=udp>;isup-oli=00
    Privacy: id
  Message Body

No. Time Source Destination Protocol Info
42 36.978738 10.10.98.98 20.20.242.26 SIP Status: 100 Trying

No. Time Source Destination Protocol Info
43 37.026764 10.10.98.98 20.20.242.26 SIP Status: 180 Ringing

No. Time Source Destination Protocol Info
44 37.096280 20.20.242.26 10.10.98.98 SIP Request: PRACK
sip:5012871491@10.10.98.98:5060;user=phone;transport=udp

No. Time Source Destination Protocol Info
45 37.105426 10.10.98.98 20.20.242.26 SIP Status: 200 OK

No. Time Source Destination Protocol Info
51 40.692824 10.10.98.98 20.20.242.26 SIP/SDP Status: 200 OK, with session description

No. Time Source Destination Protocol Info
70 41.191712 10.10.98.98 20.20.242.26 SIP/SDP Status: 200 OK, with session description

No. Time Source Destination Protocol Info
121 42.192600 10.10.98.98 20.20.242.26 SIP/SDP Status: 200 OK, with session description

No. Time Source Destination Protocol Info
126 42.265984 20.20.242.26 10.10.98.98 SIP Request: ACK
sip:5012871491@10.10.98.98:5060;user=phone;transport=udp

No. Time Source Destination Protocol Info
2444 65.105429 10.10.98.98 20.20.242.26 SIP Request: BYE
sip:anonymous@20.20.242.26:5060;transport=udp

No. Time Source Destination Protocol Info
2452 65.175428 20.20.242.26 10.10.98.98 SIP Status: 200 OK

8. Conclusion

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test result met the objectives outlined in **Section2.1**. The Winstream system is considered **compliant** with the Avaya Communication Server 1000 Release 7.0.

9. Additional References

Product documentation for ACME packet and Avaya products may be found at:
http://www.acmepacket.com/support.htm
http://support.avaya.com/css/appmanager/public/support

[1]*Communication Server 1000 Network Routing Service Fundamentals, Release 7.0, Revision 02.01, June 2010, Document Number NN43001-130*

[2]*IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.0, Revision: 04.01, June 2010, Document Number NN43001-313*

[3] *Communication Server 1000E Overview Release 7.0, Revision 04.02, April 2011, Document Number NN43041-110*

[4]*Communication Server 1000 Unified Communications Management Common Services Fundamentals, Revision 04.01, June 2010, Document Number NN43001-116*

[5]*Communication Server 1000 Dialing Plans Reference, Release 7.0, Revision 04.01, June 2010, Document Number NN43001-283*

[6]*Product Compatibility Reference, Avaya Communication Server 1000, Release 7.0,Revision 04.01, June 2010,Document Number NN43001-256*

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.