Avaya Solution & Interoperability Test Lab

Application Notes for Configuring PAETEC Communications SIP Trunking with the Avaya Communication Server 1000 Release 7.5 and Avaya Aura® Session Border Controller Release 6.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of the Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Border Controller Release 6.0 and the PAETEC Communications system. During the interoperability testing, Avaya Communication Server 1000 was able to interoperate with the PAETEC Communications Acme Packet Session Border Controller via SIP trunks. The Avaya Aura® Session Border Controller is used as an IP-IP network border between the enterprise and the service provider.

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

Table of Contents 2
1. Introduction 5
2. General Test Approach and Test Results 5
   2.1. Interoperability Compliance Testing 5
   2.2. Test Results 6
   2.3. Support 7
3. Reference Configuration 8
4. Equipment and Software Validated 9
5. Avaya Communication Server 1000 Configuration 9
   5.1. Log in to Communication Server 1000 System 10
      5.1.1. Log in to Unified Communications Management (UCM) and Element Manager (EM) 10
      5.1.2. Log in to Call Server by using the Overlay Command Line Interface (CLI) 11
   5.2. Administer a Node IP Telephony 12
      5.2.1. Obtain Node IP address 12
      5.2.2. Administer Terminal Proxy Server (TPS) 14
      5.2.3. Administer Quality of Service (QoS) 15
      5.2.4. Synchronize the New Configuration 15
   5.3. Administer Voice Codec 16
      5.3.1. Enable Voice Codec G.729, G.711, Node IP Telephony 16
      5.3.2. Enable Voice Codec on Media Gateways 17
   5.4. Zones and Bandwidth Management 18
      5.4.1. Create a zone for IP phones (zone 10) 18
      5.4.2. Create a zone for virtual SIP trunk (zone 255) 19
   5.5. Administer SIP Trunk Gateway 20
      5.5.1. Integrated Services Digital Network (ISDN) 20
      5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Border Controller 21
      5.5.3. Administer Virtual D-Channel 23
      5.5.4. Administer Virtual Super-Loop 26
      5.5.5. Administer Virtual SIP Routes 27
      5.5.6. Administer Virtual Trunks 30
      5.5.7. Administer Calling Line Identification Entries 32
      5.5.8. Enable External Trunk to Trunk Transferring 33
   5.6. Administer Dialing Plans 34
      5.6.1. Define ESN Access Codes and Parameters (ESN) 34
      5.6.2. Associate NPA and SPN call to ESN Access Code 2 35

5.6.3. Digit Manipulation Block (DMI) ... 36
5.6.4. Digit Manipulation Block (DMI) for Outbound Call ... 36
5.6.5. Route List Block (RLB) (RLB 14) ... 37
5.6.6. Route List Block (RLB) (RLB 15) ... 39
5.6.7. Inbound Call – Incoming Digit Translation Configuration ... 39
5.6.8. Outbound Call - Special Number Configuration ... 41
5.6.9. Outbound Call - Numbering Plan Area (NPA) ... 42
5.7. Administer Phone ... 42
5.7.1. Phone creation ... 42
5.7.2. Enable Privacy for Phone ... 44
5.7.3. Enable Call Forward for Phone ... 44
5.7.4. Enable Call Waiting for Phone ... 47
6. Configure Avaya Aura® Session Border Controller ... 48
6.1. Service Provider Pre-installation Wizard ... 48
6.2. DevSBC5 Installation ... 55
6.3. Administer Enterprise Servers ... 55
6.3.1. Configuration of “server Paetec” ... 55
6.3.2. Configuration of “server PBX” ... 56
6.4. Administer Heartbeat ... 57
6.5. Administer dial-plan ... 58
6.5.1. The entry “source-route FromPBX” ... 58
6.5.2. The entry “source-route FromPaetec” ... 60
6.6. Administer session-config-pool “entry ToPaetec” ... 61
6.6.1. Administer sip-settings ... 61
6.6.2. Manipulate From, To, Request-URI, and P-Asserted-Identity headers. ... 64
6.6.3. Administer media ... 66
6.6.4. Administer sip-session-timers-setting ... 67
6.6.5. Enable third-party-call-control ... 68
6.7. Administer session-config-pool “entry ToPBX” ... 68
6.7.1. Manipulate To, Request-URI headers ... 68
6.7.2. Administer media ... 70
6.8. Convert History-Info to Diversion header for Call Forward All Call Scenario ... 70
6.8.1. Create entry session-config-pool “Moved Temp” ... 70
6.8.2. Create entry dial-plan source-route “Moved Temp” ... 73
6.9. Convert History-Info to Diversion header for Call Forward Busy Scenario ... 78
6.9.1. Create entry session-config-pool “Busy-Here” ... 78
6.9.2. Create entry source-route dial-plan “Busy-Here” ... 78

6.10. Convert History-Info to Diversion header for Call Forward No Answer Scenario.... 79
6.10.1. Create entry session-config-pool "Temp Unavailable" 79
6.10.2. Create entry source-route dial-plan "Temp Unavailable"................................... 80
6.11. Convert 183 with SDP to 180 without SDP for Ring-Back-Tone in Call Blind Transfer Scenario 81
6.11.1. Create an entry to convert SIP 183 with SDP to SIP 180 with SDP.................. 81
6.11.2. Enable third party-call-control and "*forking-early-media-inhibit*" 82
7. Verification Steps.. 83
7.1. General 83
7.2. Verification of an Active Call on Call Server 83
7.3. Protocol Trace 85
8. Conclusion 86
9. Appendix.. 87
10. Additional References 88

1. Introduction

This document provides a typical network configuration deployment of the Avaya Communication Server 1000 and the PAETEC Communications SIP Trunking (hereafter referred to as PAETEC Communications system). The Avaya Aura® Session Border Controller is used as IP-IP network border between PAETEC Communications Acme Packet SBC and Avaya Communication Server 1000.

2. General Test Approach and Test Results

The Avaya Communication Server 1000 system was connected to the Avaya Aura® Session Border Controller. Then the Avaya Aura® Session Border Controller was connected to the PAETEC Communications system via SIP. Various call types were made from the Communication Server 1000 to the PAETEC Communications system and vice versa to verify the interoperability.

2.1. Interoperability Compliance Testing

The focus of this testing is to verify that Communication Server 1000 can interoperate with the PAETEC Communications system. The following interoperability areas were covered:

- General call processing between Communication Server 1000 and PAETEC Communications systems including:
  - Codec/ptime (G.729/20ms, 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 is supported only with G.711
- DTMF in both directions
- SIP Transport UDP
- Thru dialing via the Communication Server 1000 Call Pilot
- Voice Mail Server Call Pilot (hosted on Avaya system)
- Static registration.

The following assumptions were made for this lab test configuration:

1. Communication Server 1000 R7.5 software and implementation of latest patches
2. PAETEC Communications 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 was 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 between a Communication Server 1000 phone and a PSTN phone with CPND (call party name display) restricted. This is a requirement from PAETEC Communications.
2. PAETEC Communications system cannot translate the originating CLID to the wrong number (e.g.: 111-111-1111) for the outbound calls.
3. If the Communication Server 1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed. This is a Communication Server 1000 known issue.
4. PSTN1 phone calls to Communication Server 1000 phone, then phone does blind transfer to PSTN2 phone. PSTN1 phone could not hear ring-back-tone from PSTN2 phone when Communication Server 1000 phone completed blind transfer. In this particular scenario, the UPDATE support is required on the CS1000 for the ring-back-tone, but the PSTN-to-SIP gateway that PAETEC uses for this Interop testing does not support the UPDATE. In order to fix this ring-back-tone issue, we make sure to enable plug-in 501 on CS1000 to allow blind transfer to work without the UPDATE method and configure Avaya Aura Session Border Controller to translate the SIP 183 with SDP to SIP 180 without SDP so that PSTN1 can hear the local ring-back-tone. If we do this translation on Avaya Aura Session Border Controller, the early media is not supported in this testing.

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

2.3. Support

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

For technical support on PAETEC Commnucations system, please contact PAETEC Communications technical support at:

- Toll Free: 1-800-967.2233
- http://www.paetec.com/customer-care/

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between the Communication Server 1000 and PAETEC Communications systems.
For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

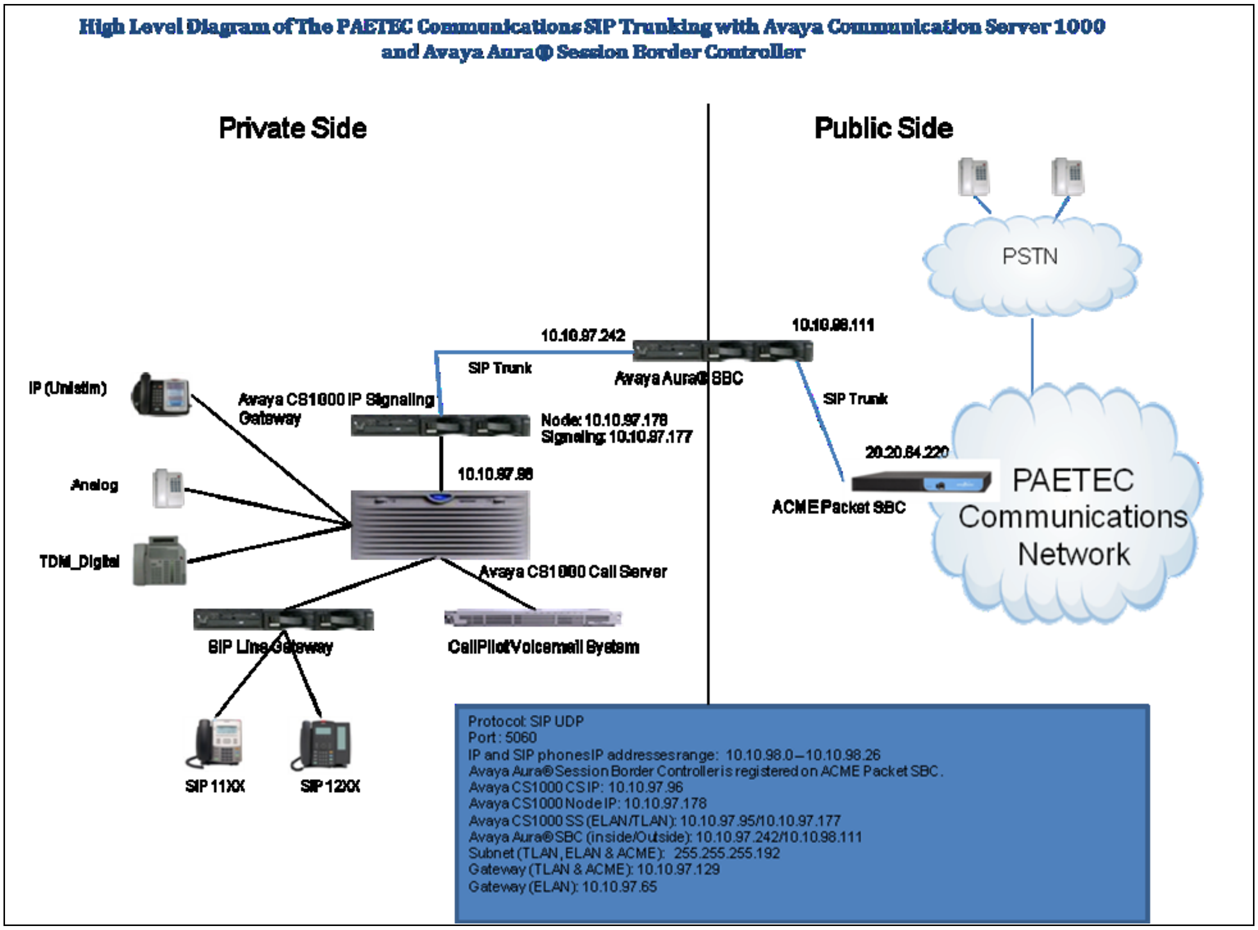


Figure 1- Network diagram for Avaya and PAETEC Communications Systems

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 (CPPM)	• Call Server: 750 Q+ GA • Signaling Server: 7.50.17 GA • SIP Line Server: 7.50.17 GA
Avaya Aura® Session Border Controller	• SBCT 6.0.2.0.3 (sbc E362P4)
Avaya phones	• 2002 p2: 0604DCN (Unistim) • 1140: 0625C8D (Unistim) • 1120: 0624C8D (Unistim) • 2007: 0621C8D (Unistim) • 1120: 4 1 13 0 (SIPLine) • 12xx: 4 1 13 0 (SIPLine)

PAETEC Communications system:

System	Software/Loadware version
Acme Packet Net-Net 4250 Session Border Controller	• Firmware SC6.2.0 Patch 3 (Build 497) Build Date=02/12/10
Broadsoft	• Version 14.sp9
LCS Gateway	• Version 3.14.4.7

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

Call Server: 7.50 Q+ GA plus latest DEPLIST – Deplists_CPL_X21_07_50Q.zip
SSG Server: 7.50.17 GA plus latest DEPLIST – Service_Pack_Linux_7.50_17_20111101.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 PAETEC Communications 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 the references in **Section 10.**

The below procedures describe the configuration details of Communication Server 1000 with a SIP trunk to the PAETEC Communications system.

5.1. Log in to Communication Server 1000 System

5.1.1. Log in 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**.

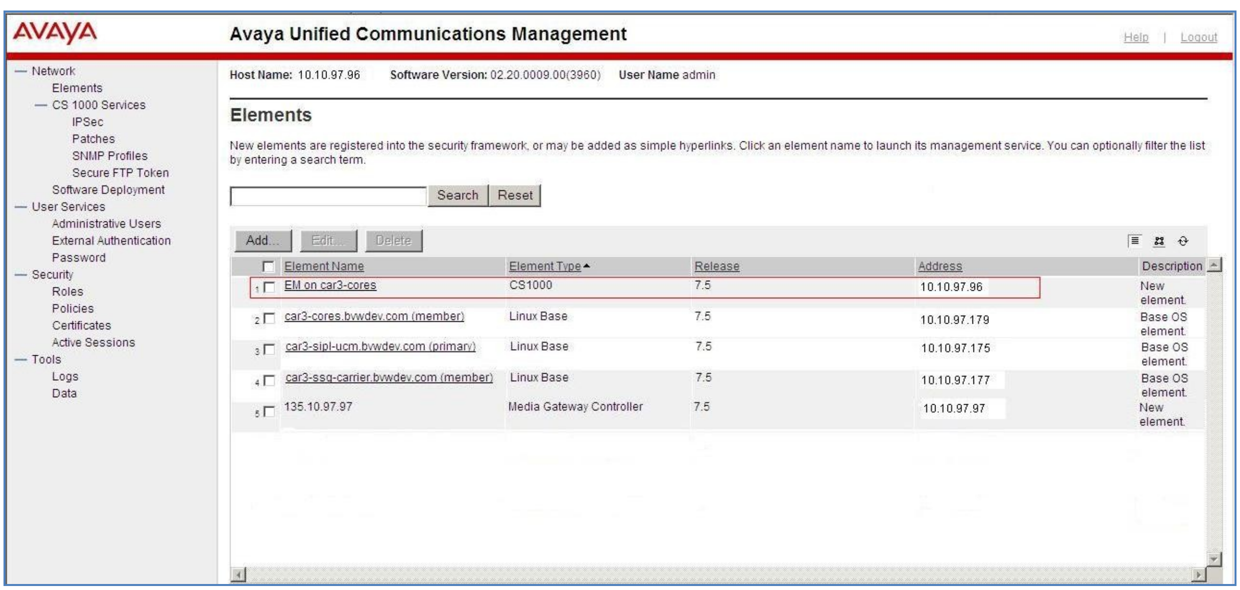


Figure 3 – Unified Communications Management

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: 7.50 Q+

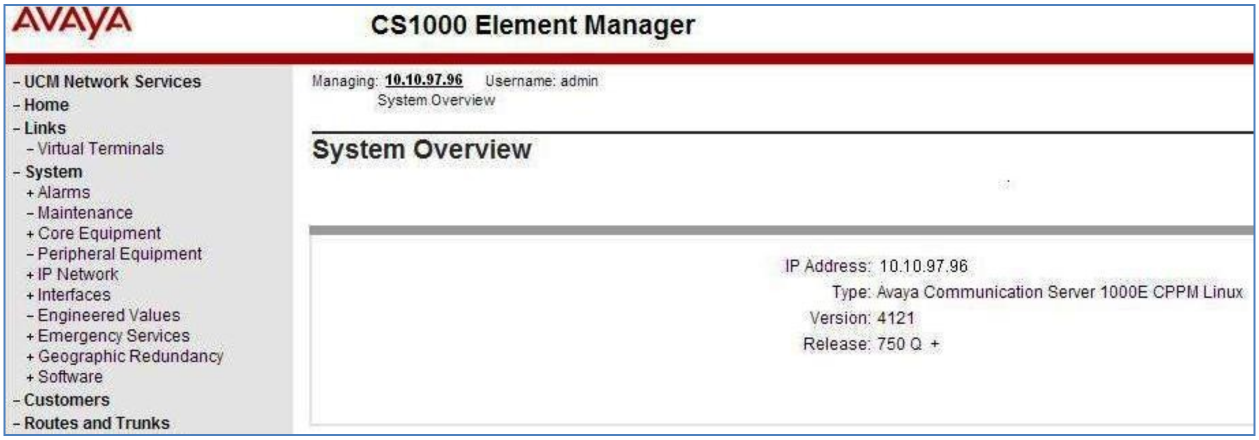


Figure 4 – Element Manager System Overview

5.1.2. Log in 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 log in with the appropriate admin account and password.
c) Here are the logs.

```
login as: admin

          Nortel Networks Linux Base 7.50
The software and data stored on this system are the property of, or licensed to, Nortel Networks
and are lawfully available only to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and punishable under appropriate
laws. If you are not an authorized user then do not try to login. This system may be monitored
for operational purposes at any time.

admin@10.10.97.177's password: <----enter your password
Last login: Tue Nov 01 10:20:05 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 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.
 ADMIN 12:56  01/11/2011
>
```

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 PAETEC Communications system. For further information on Avaya Communications Server 1000, please consult the references in **Section 10**.

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

Figure 5 – IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 6, Figure 7** 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 IP Address** to communicate with other components to process the SIP call.

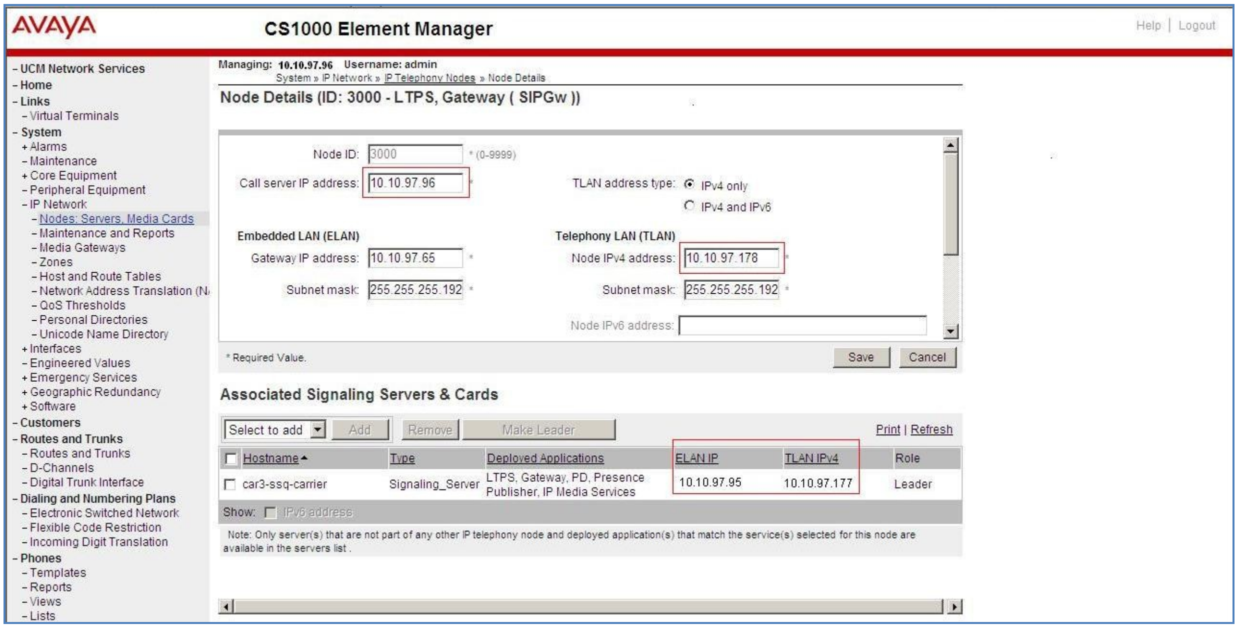


Figure 6 –Node Details

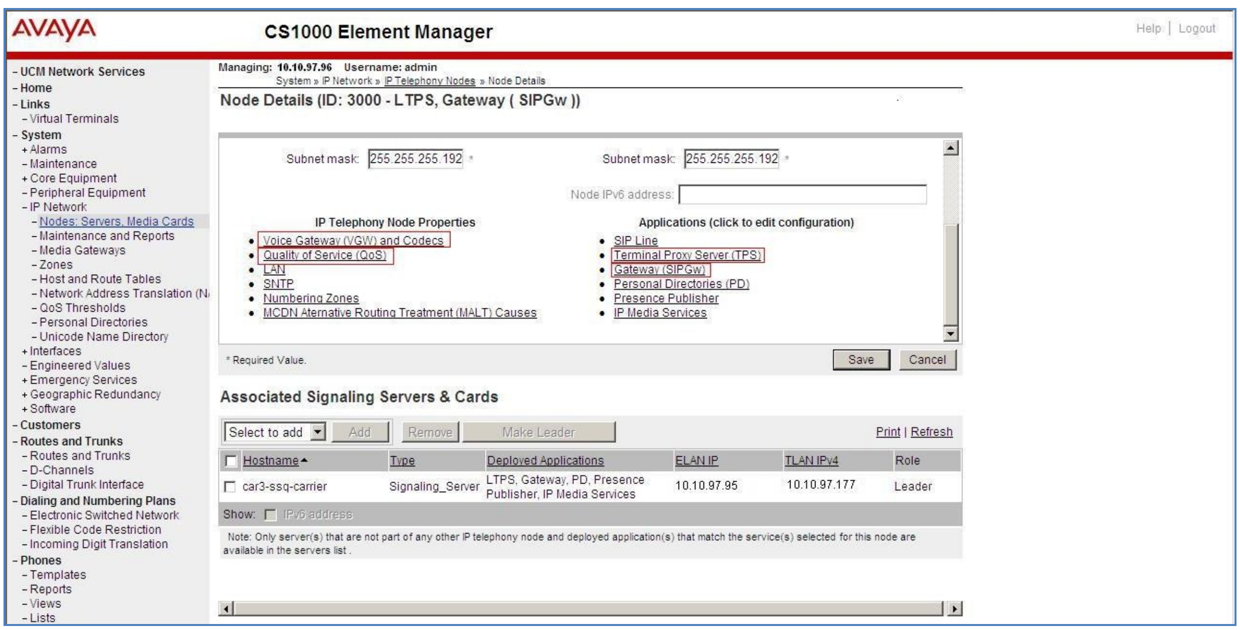


Figure 7 –Node Details

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 7**.

d) Check the **UNIStim Line Terminal Proxy Server** check box and then click the **Save** button as shown in **Figure 8**.

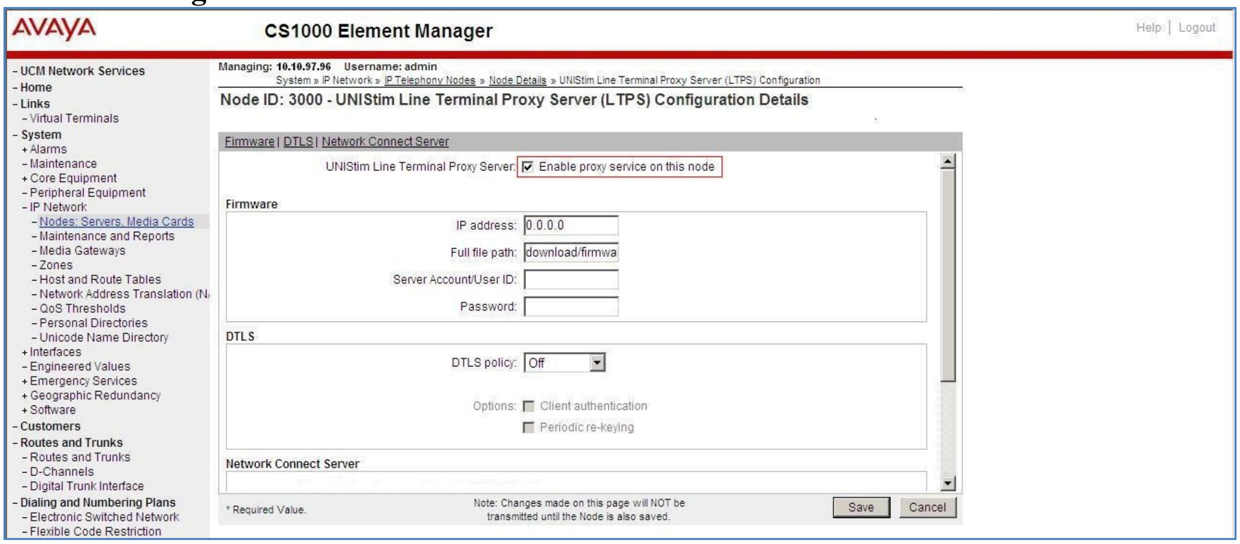


Figure 8 – TPS Configuration Details

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 7**.
f) The default Diffserv values are as shown in **Figure 9**. Click on the **Save** button.

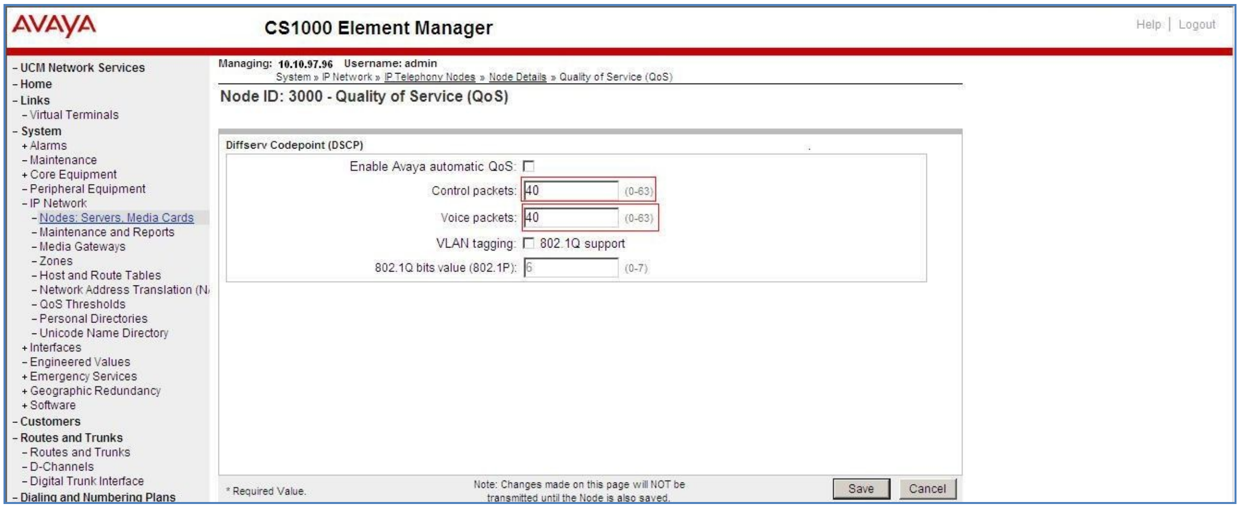


Figure 9 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

g) Continue from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button.
h) The **Node Saved** screen is displayed. Click on the **Transfer Now** (not shown).
i) The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box and click on the **Start Sync** (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 G.729, G.711, Node IP Telephony.

a) Select **IP Network** -> **Nodes: Servers, Media Cards** 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. (See **Section 5.2.1** for more detail).

b) On the **Node Details** page as shown in **Figure 7**, click on **Voice Gateway (VGW) and Codec.**

c) The PAETEC Communications system supports **G.729/ptime 20ms** and **G.711/ptime 20ms with VAD disabled**. Then click on the **Save** button.

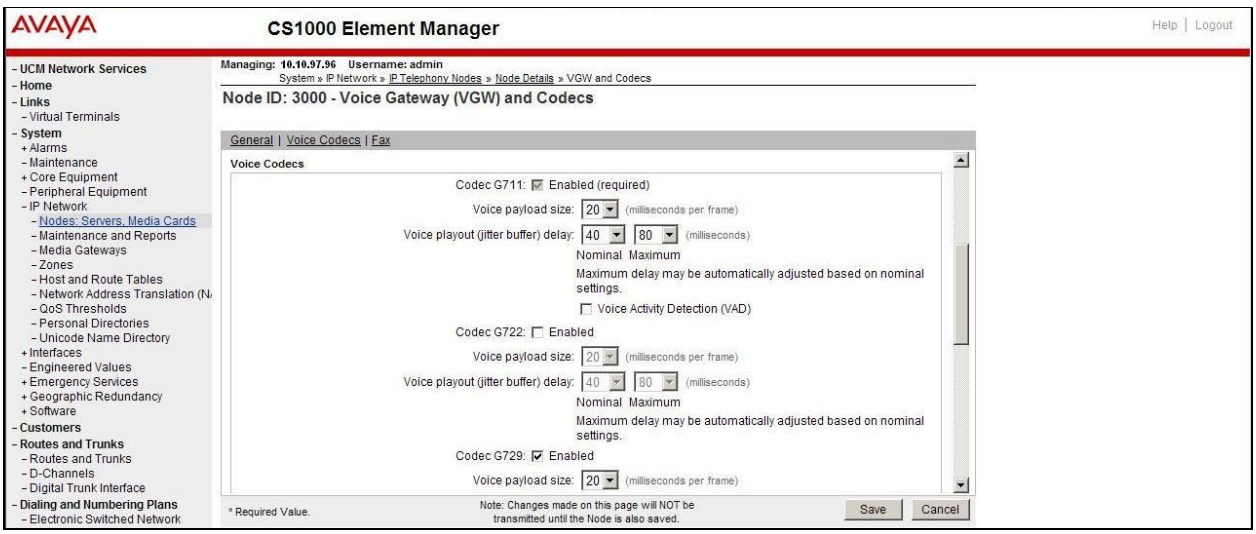


Figure 10 – Voice Gateway and Codec Configuration Details

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

5.3.2. Enable Voice Codec on Media Gateways.

a) From the left menu of the Element Manager page in **Figure 10**, select **IP Network** -> **Media Gateways** menu 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 G.729 and G.711** and uncheck **VAD** as shown in **Figure 11**.

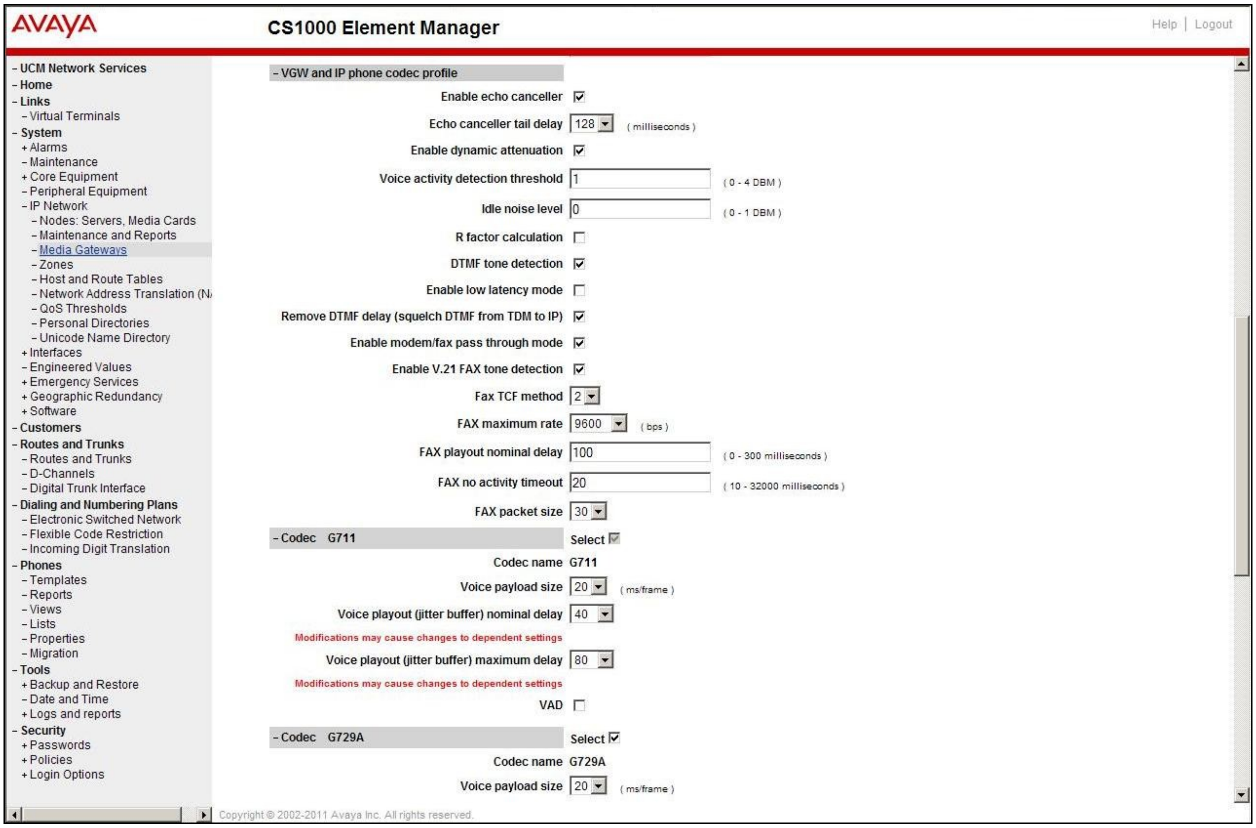


Figure 11 – Media Gateways Configuration Details

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 12**.

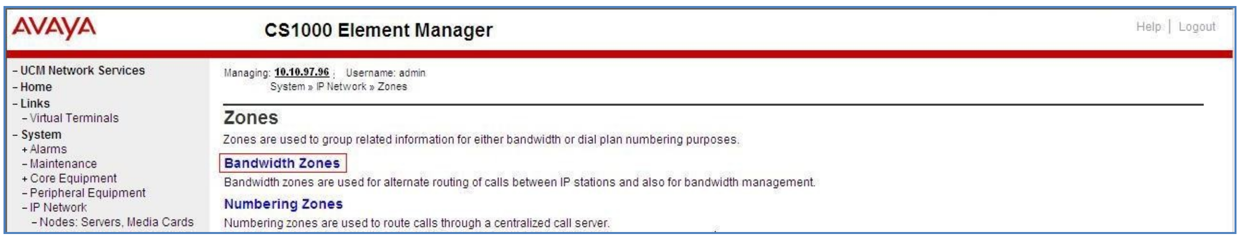


Figure 12 – Zones Page

b) The **Bandwidth Zones** screen is displayed as shown in **Figure 13**. Click **ADD** to create new zone for IP Phones.

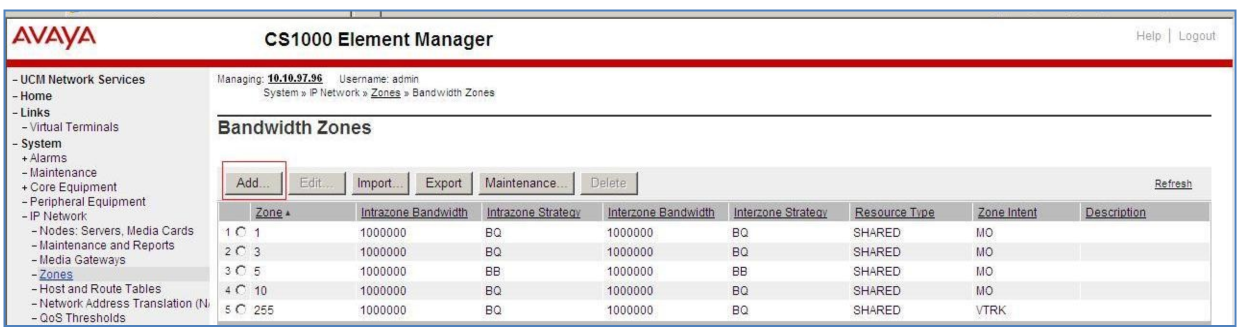


Figure 13 – Bandwidth Zones

c) Select the values as shown (in red box) in **Figure 14** 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.

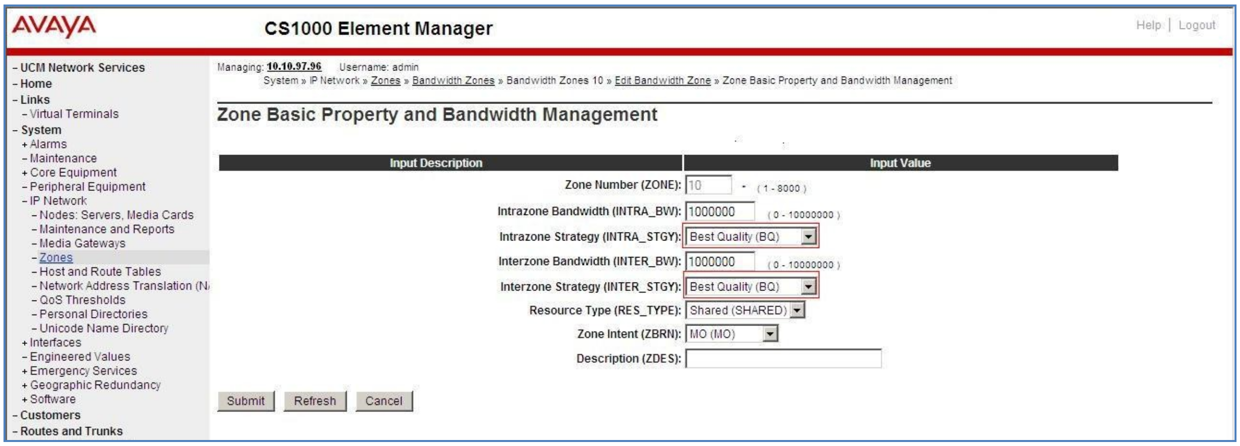


Figure 14 –Bandwidth Management Configuration Details – IP phone

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 15** and then click on the **Submit** button.

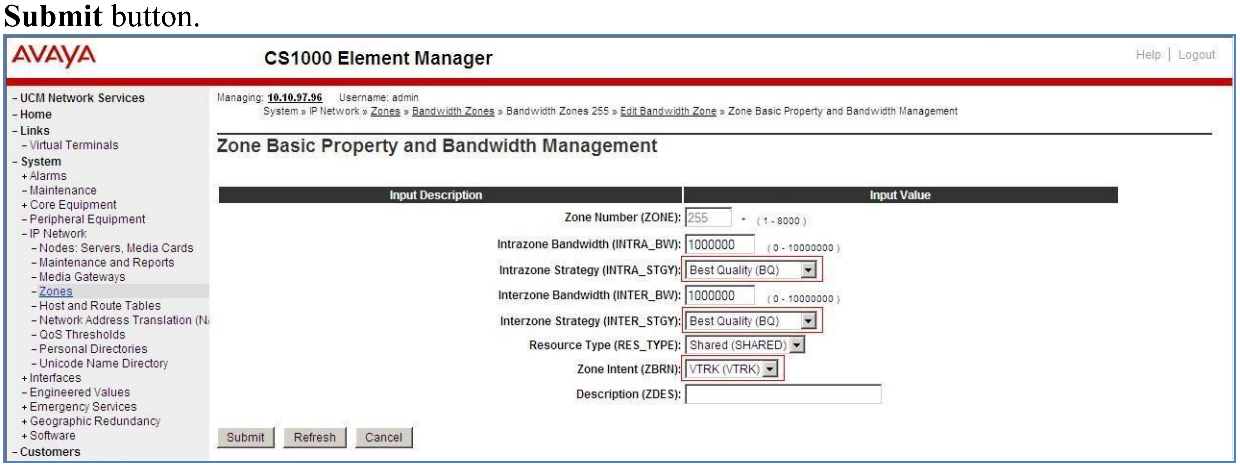


Figure 15 –Bandwidth Management Configuration Details –virtual SIP trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between SIP Signaling Gateway (SSG) to Avaya Aura® Session Border Controller.

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 00 Edit** 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 16** 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).

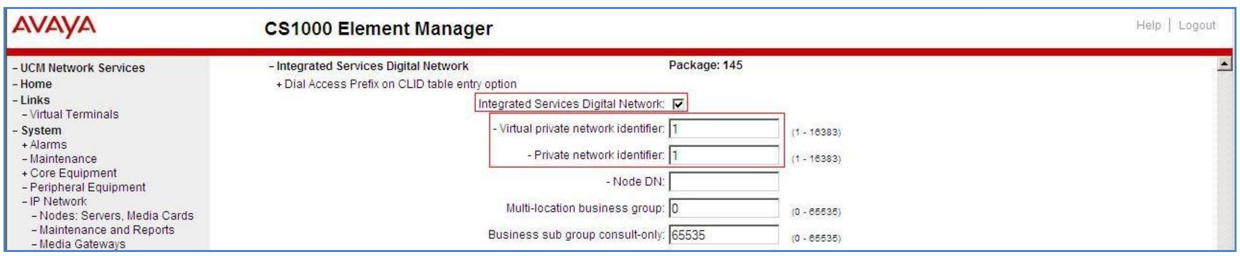


Figure 16 –Customer – ISDN Configuration

5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Border Controller

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 7**, **Section 5.2.1.**

b) On the **Node Details** screen, select **SIP 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 17**. The parameters (highlighted in red boxes) are filled in. The **SIP domain name** and **Local SIP port** should be matched in Avaya Aura® Session Border Controller configuration.

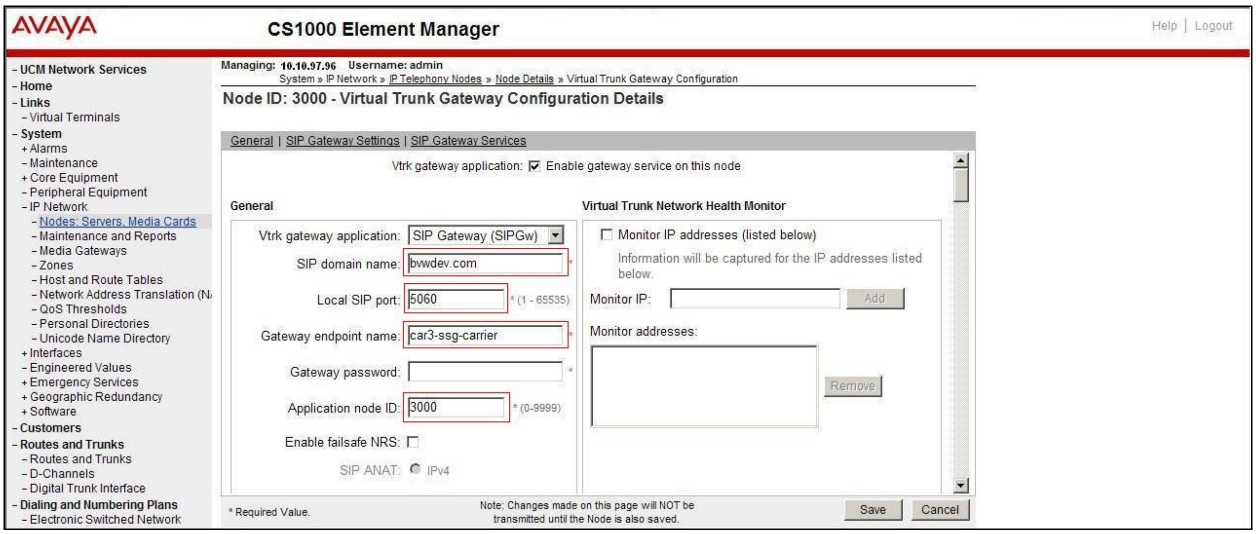


Figure 17 – Virtual Trunk Gateway Configuration Details

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 18**. Enter **Primary TLAN IP address** as the IP address of Avaya Aura® Session Border Controller Inside interface.

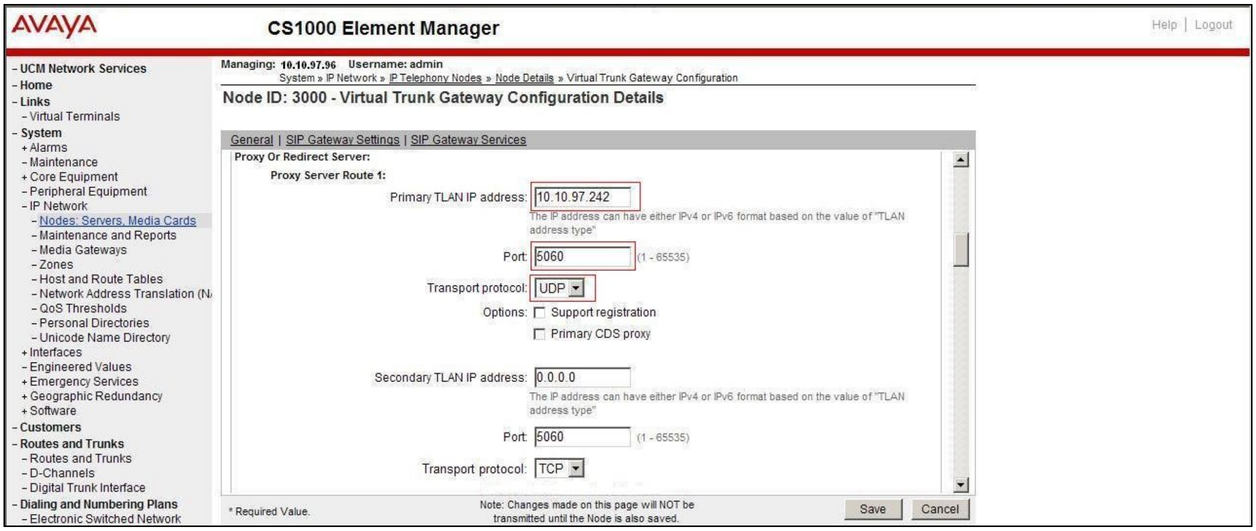


Figure 18 – Virtual Trunk Gateway Configuration Details

e) On the same page as shown in **Figure 18**, scroll down 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 19**. Then click on the **Save** button.

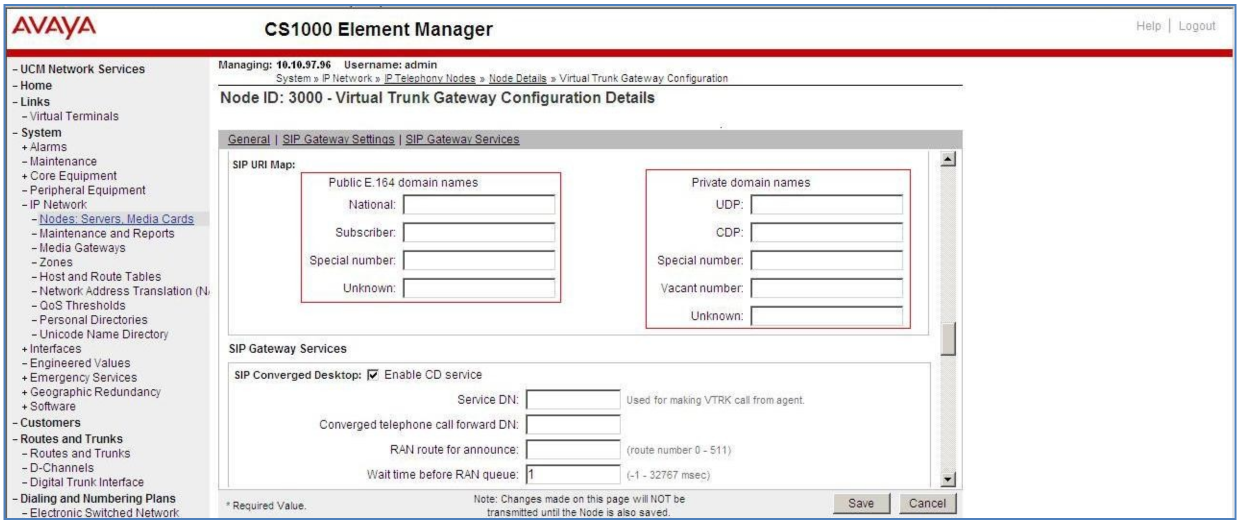


Figure 19 – Virtual Trunk Gateway Configuration Details

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

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 the **to Add** button.

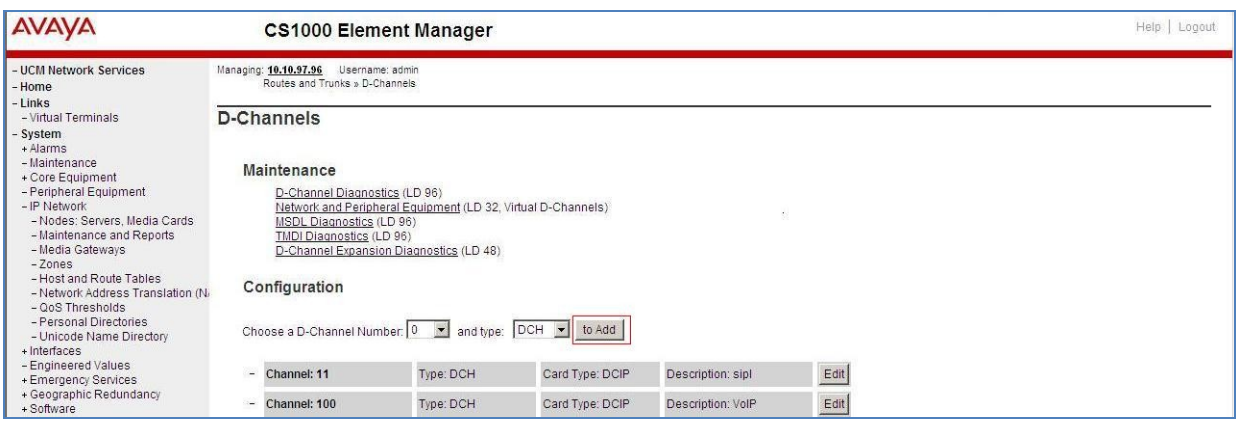


Figure 20 – D-Channels

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

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.

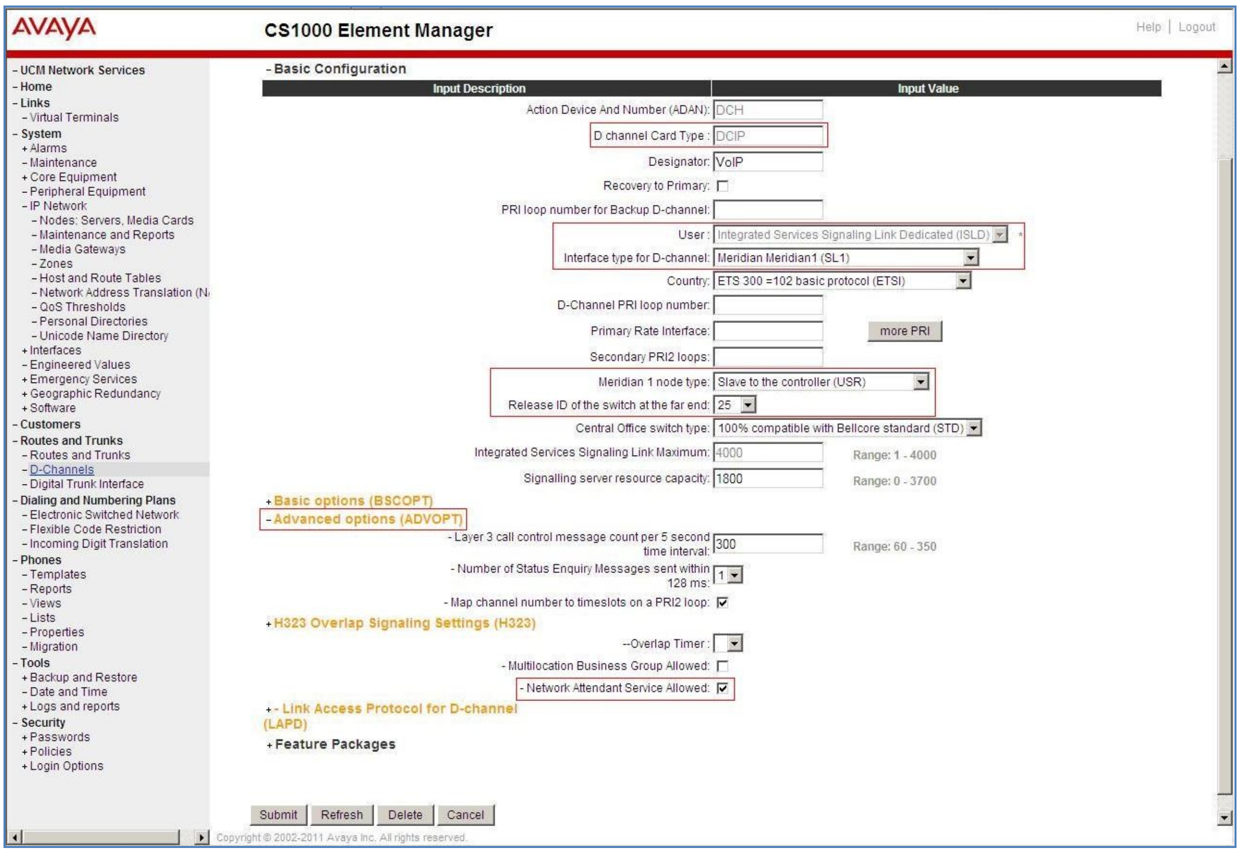


Figure 21 – D-Channels Configuration Details

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**.

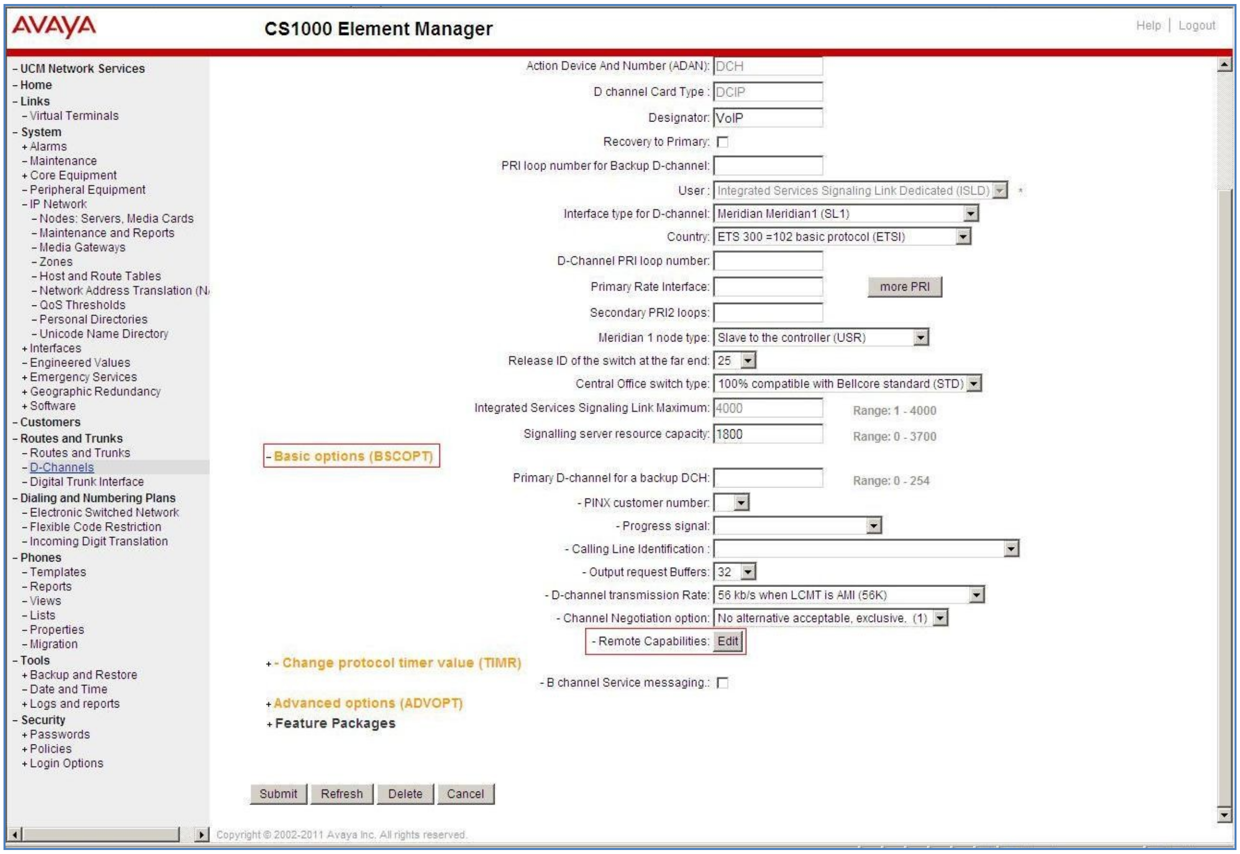


Figure 22 – D-Channel Configuration Details

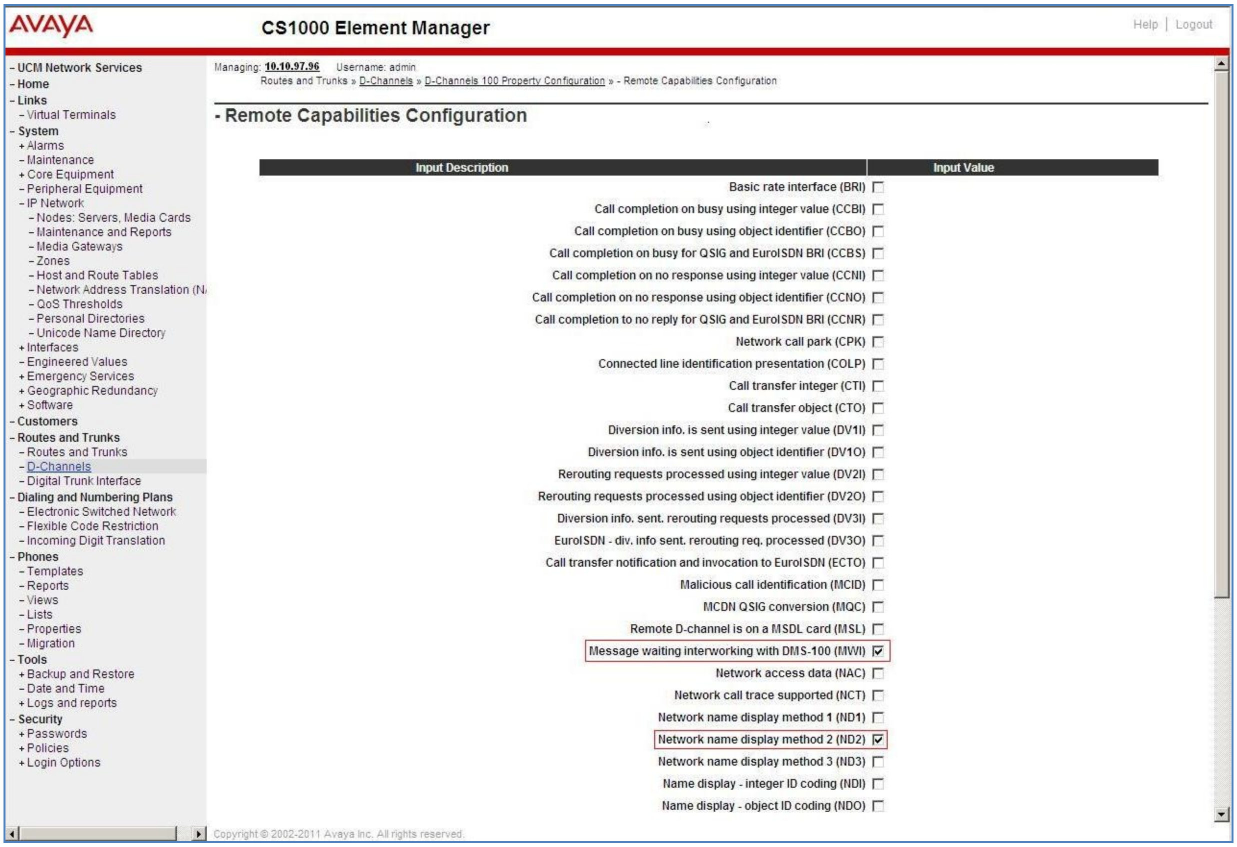


Figure 23 – Remote Capabilities Configuration Details

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 the "**Add**" button to create a new one as shown in **Figure 24**. In this example, superloop 4, 96, 100 and 124 have been added and are being used.

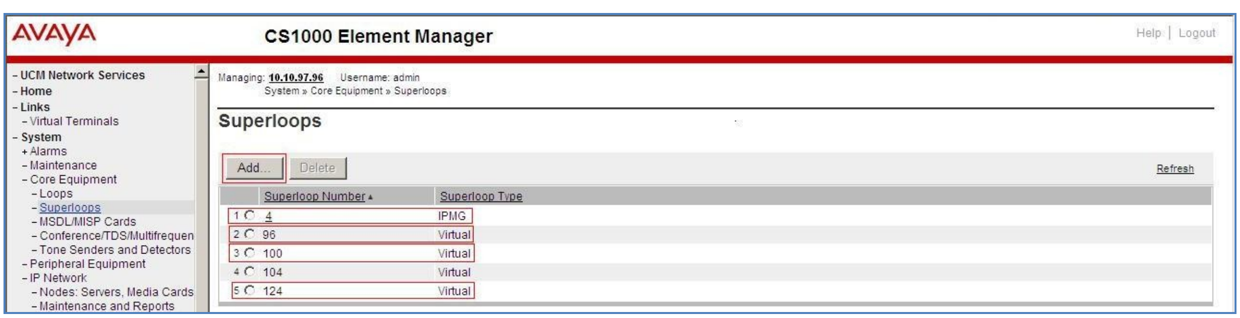


Figure 24 – Administer Virtual Super-Loop Page

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**.

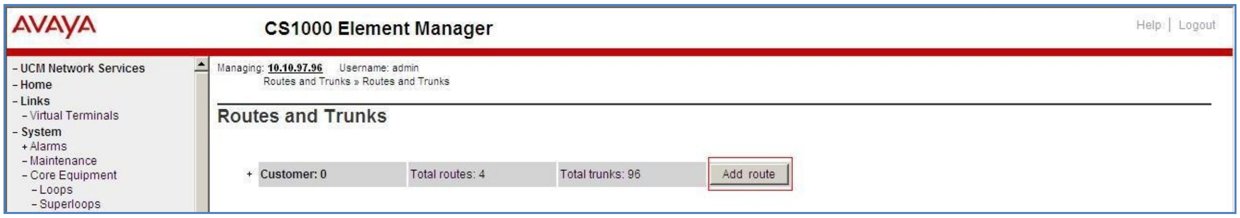


Figure 25 – Add route

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 the specified 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.

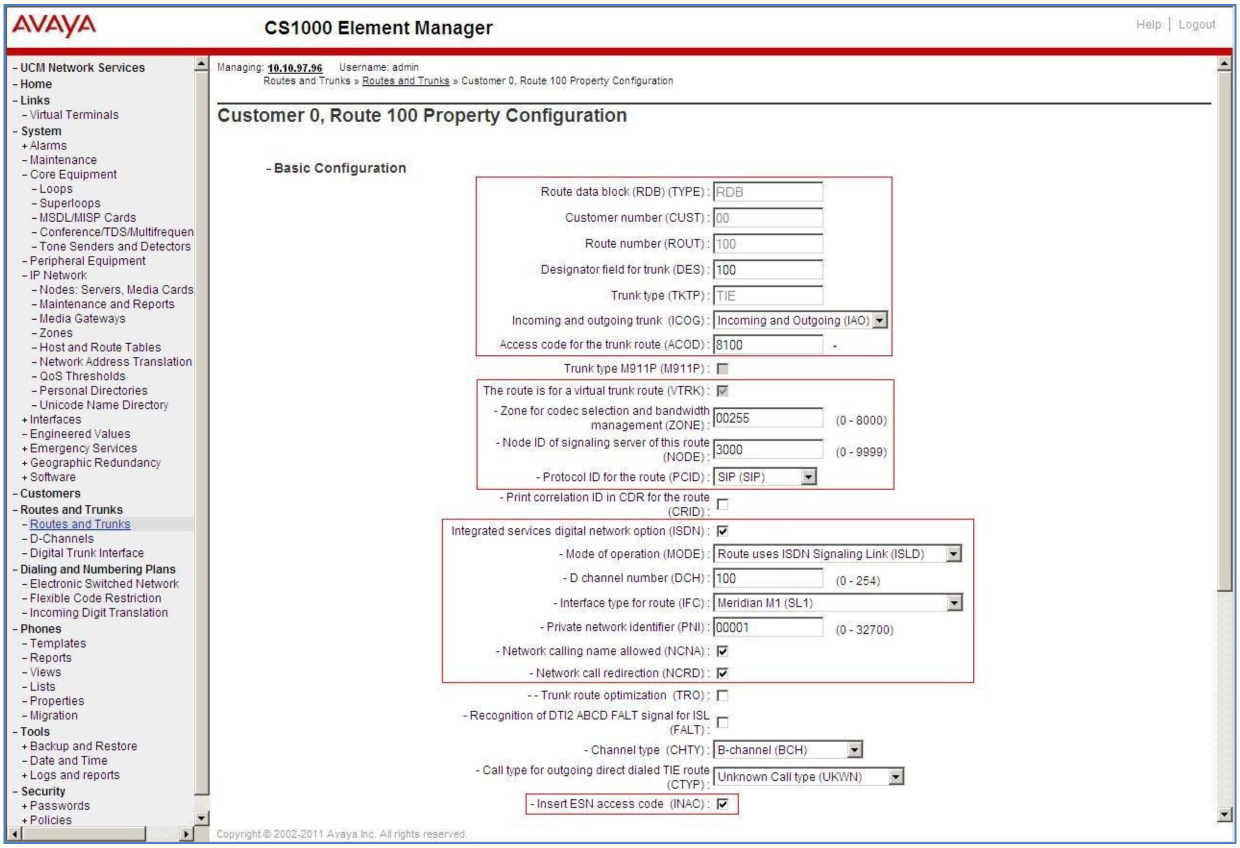


Figure 26 – Route Configuration Details

- 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.**

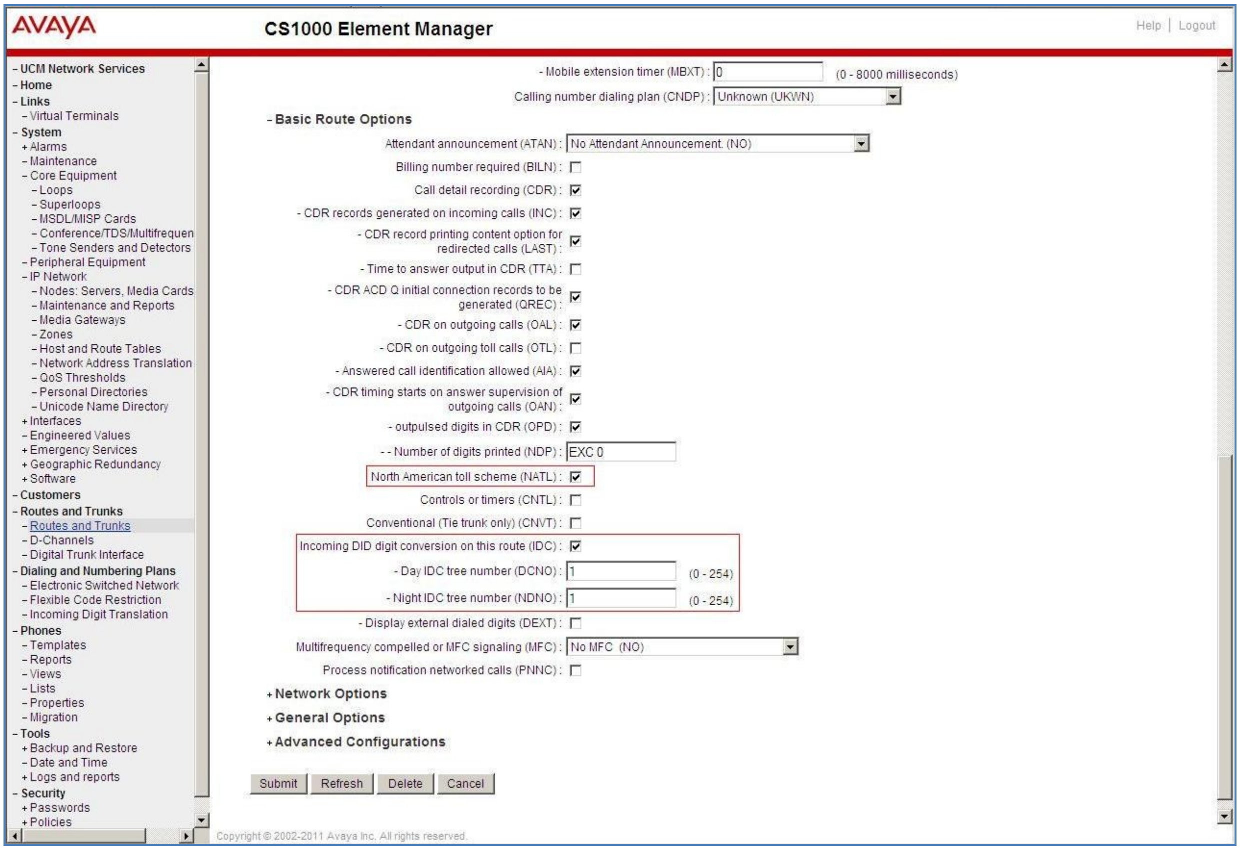


Figure 27 – Route Configuration Details

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**.

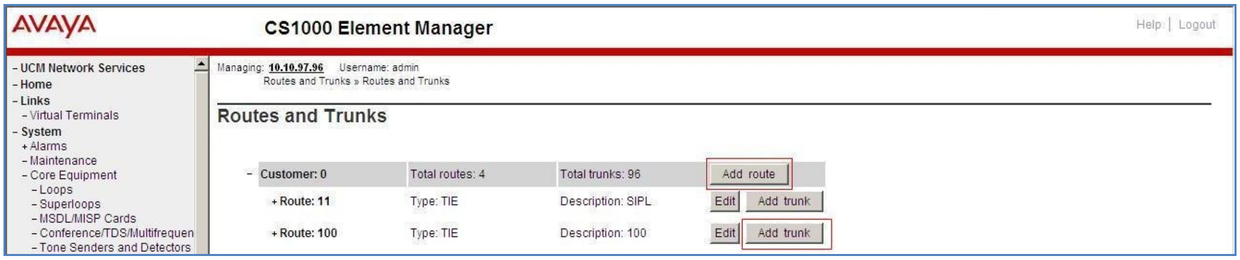


Figure 28 – Route and Trunks Page

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 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 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

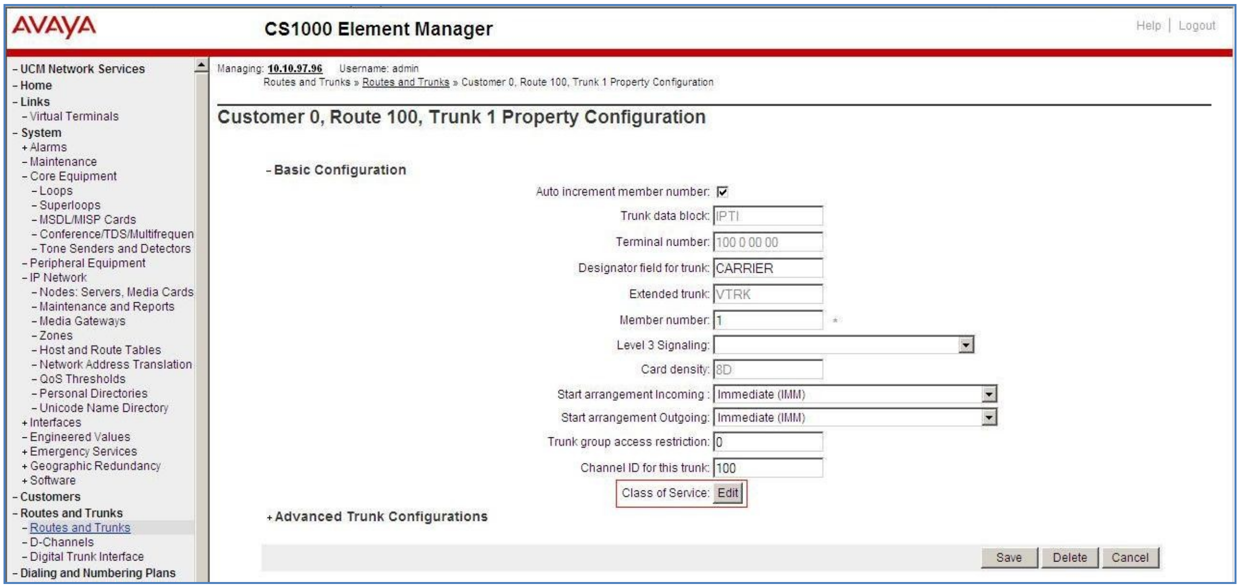


Figure 29 – New Trunk Configuration Details

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)

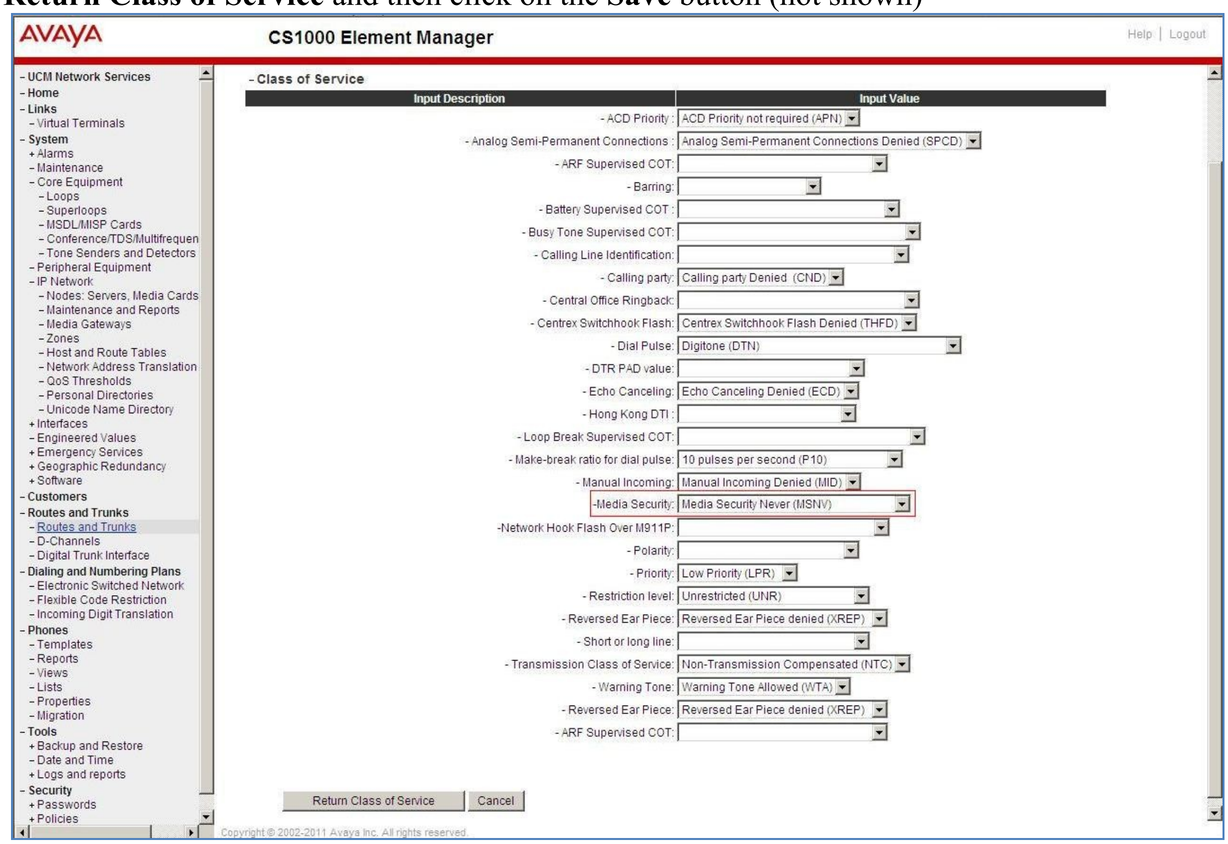


Figure 30 – Class of Service Configuration Details Page

5.5.7. Administer Calling Line Identification Entries

a) Select **Customers** -> **<u>00</u>** -> **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in **Figure 31**.

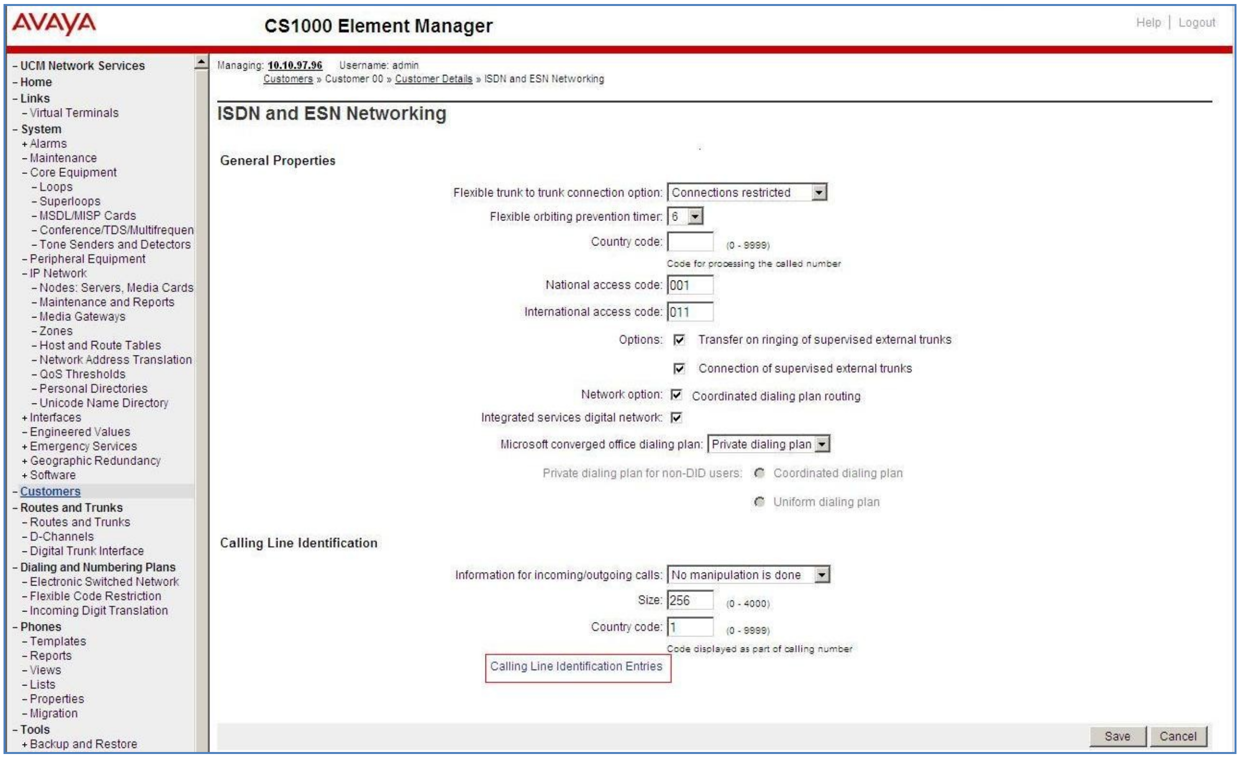


Figure 31 – ISDN and ESN Networking

b) Click on **Add** as shown in **Figure 32**.

Figure 32 – Calling Line Identification Entries

c) Add entry **0** as shown in **Figure 33:**

- **National Code**: leave as blank
- **Local Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits – 713343. 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 - 713343. 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 - 713343. 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**.

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

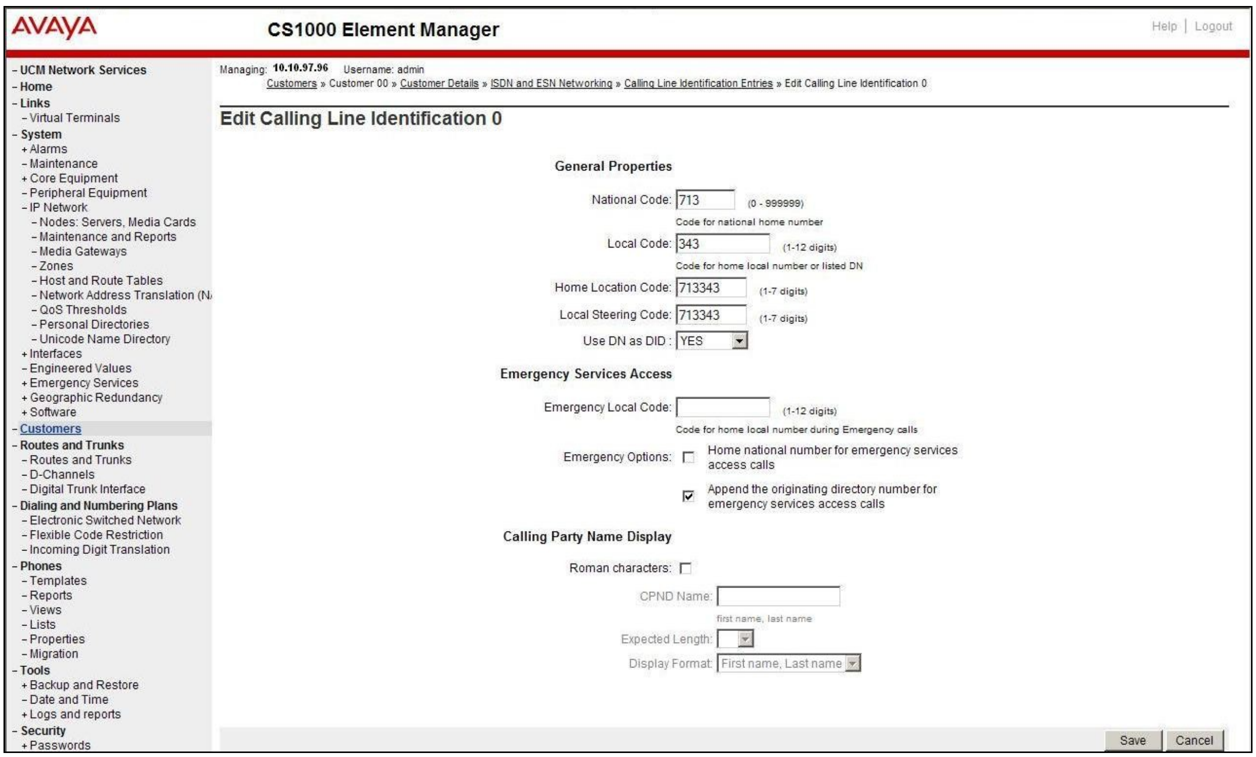


Figure 33 – Edit Calling Line Identification 0

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.**

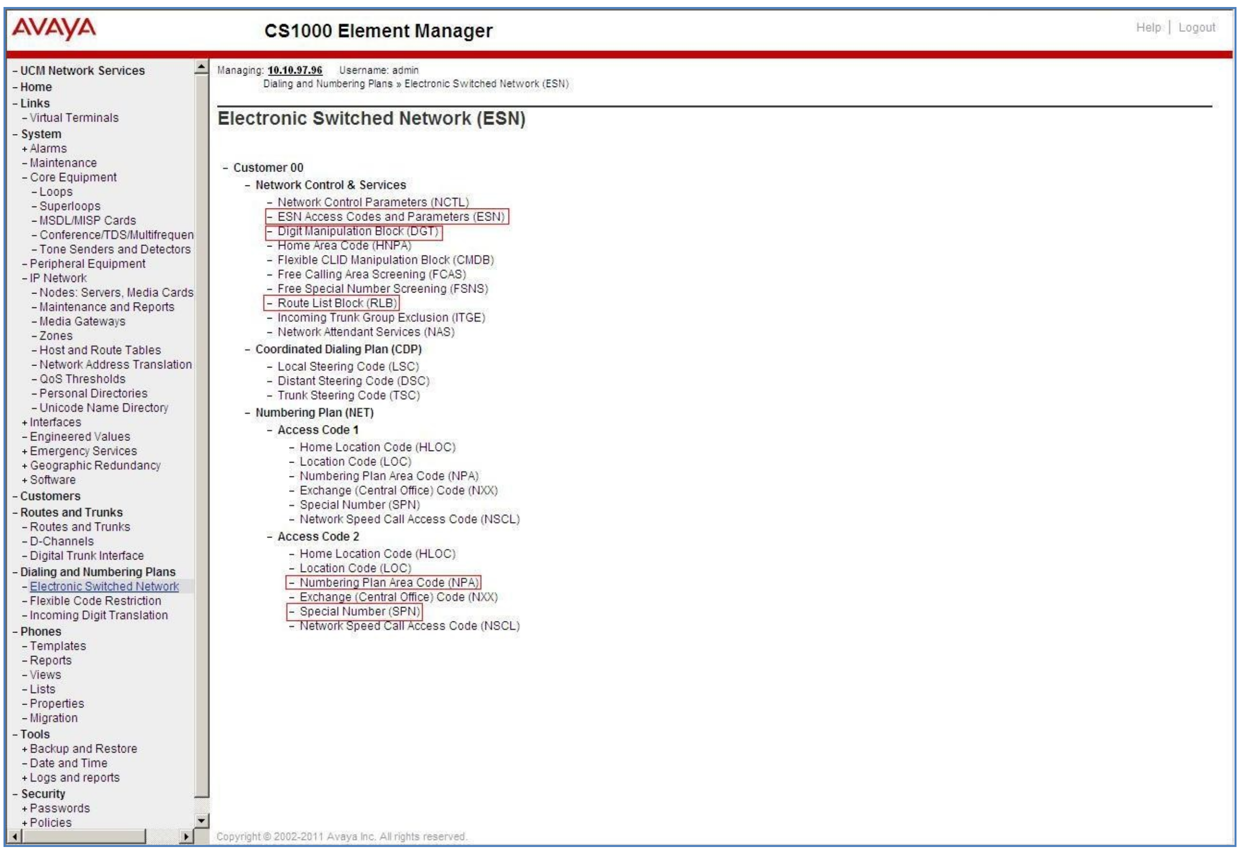


Figure 34 –ESN Configuration Details

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).

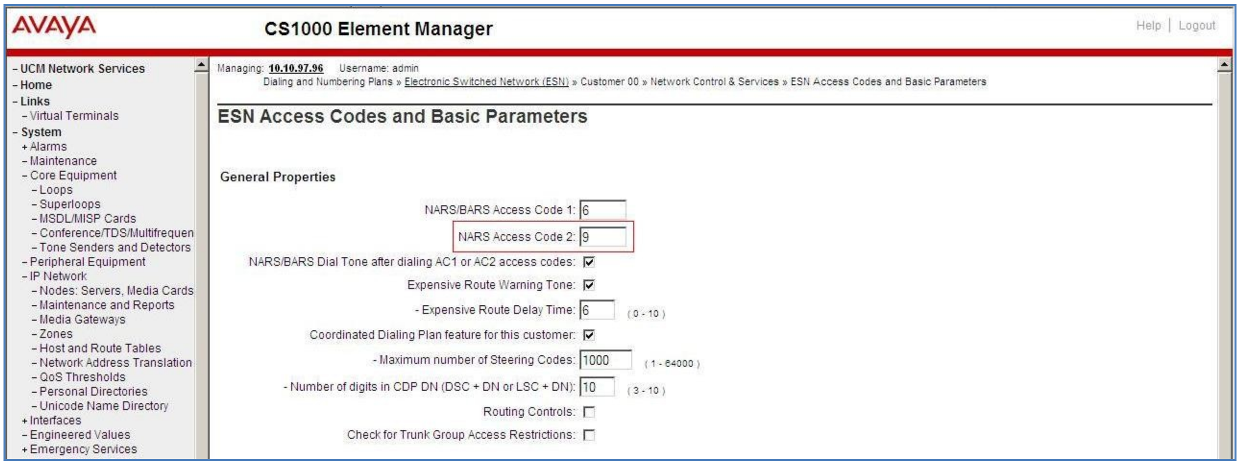


Figure 35 – ESN Access Codes and Basic Parameters

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
AC1 xNPA xSPN     ------  > (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
AC2 INTL 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

The following steps show how to add DMI for the outbound call. There are 2 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**.

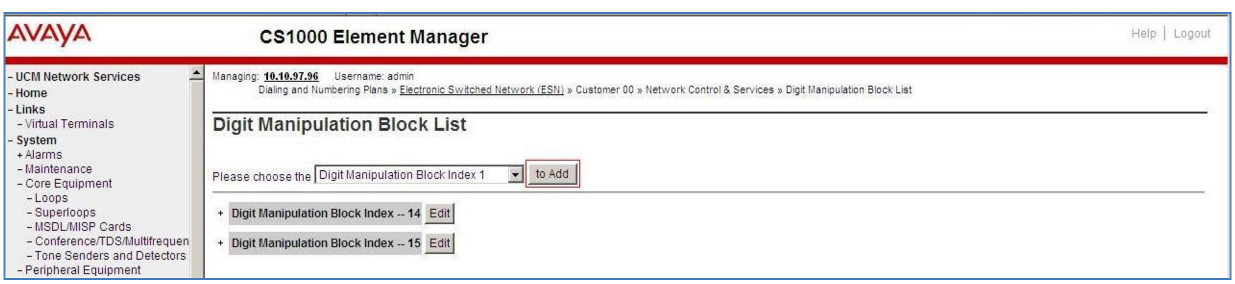


Figure 36 – Add a DMI

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 37**.

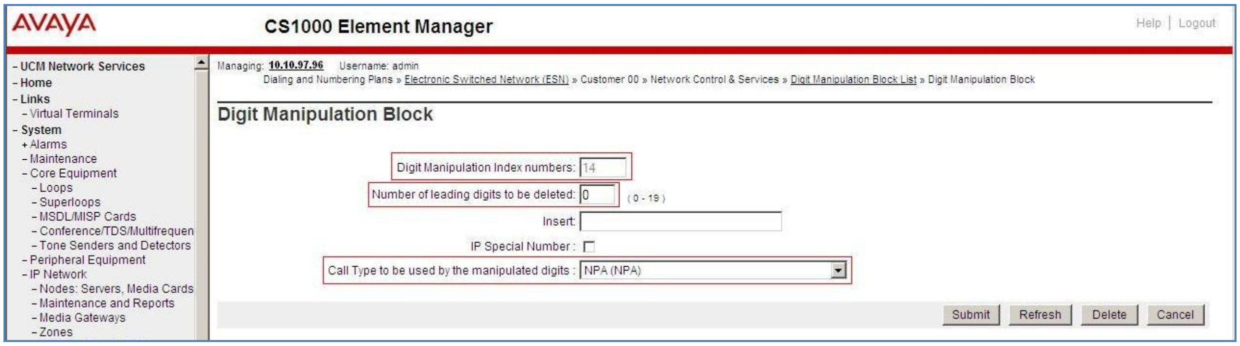


Figure 37 – DMI_14 Configuration Details

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 38**.

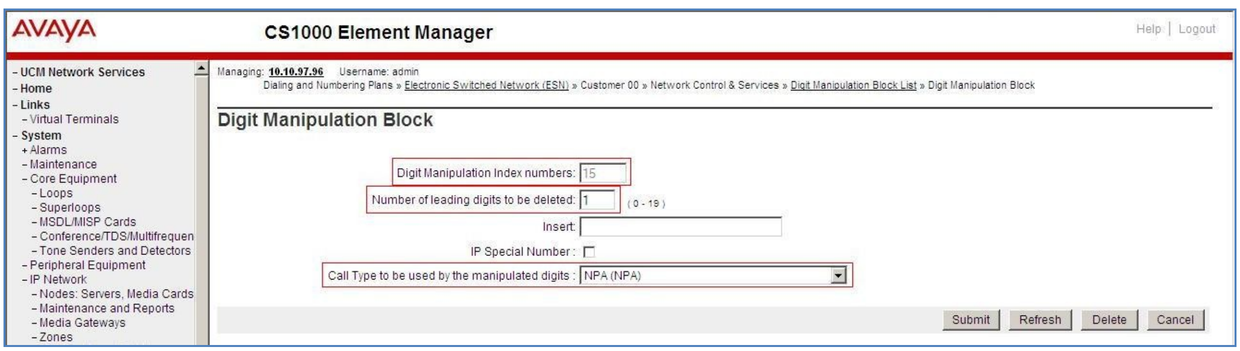


Figure 38 – DMI_15 Configuration Details

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** button as shown in **Figure 39**.

Figure 39 – Add a Route List Block.

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 40**). 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**)

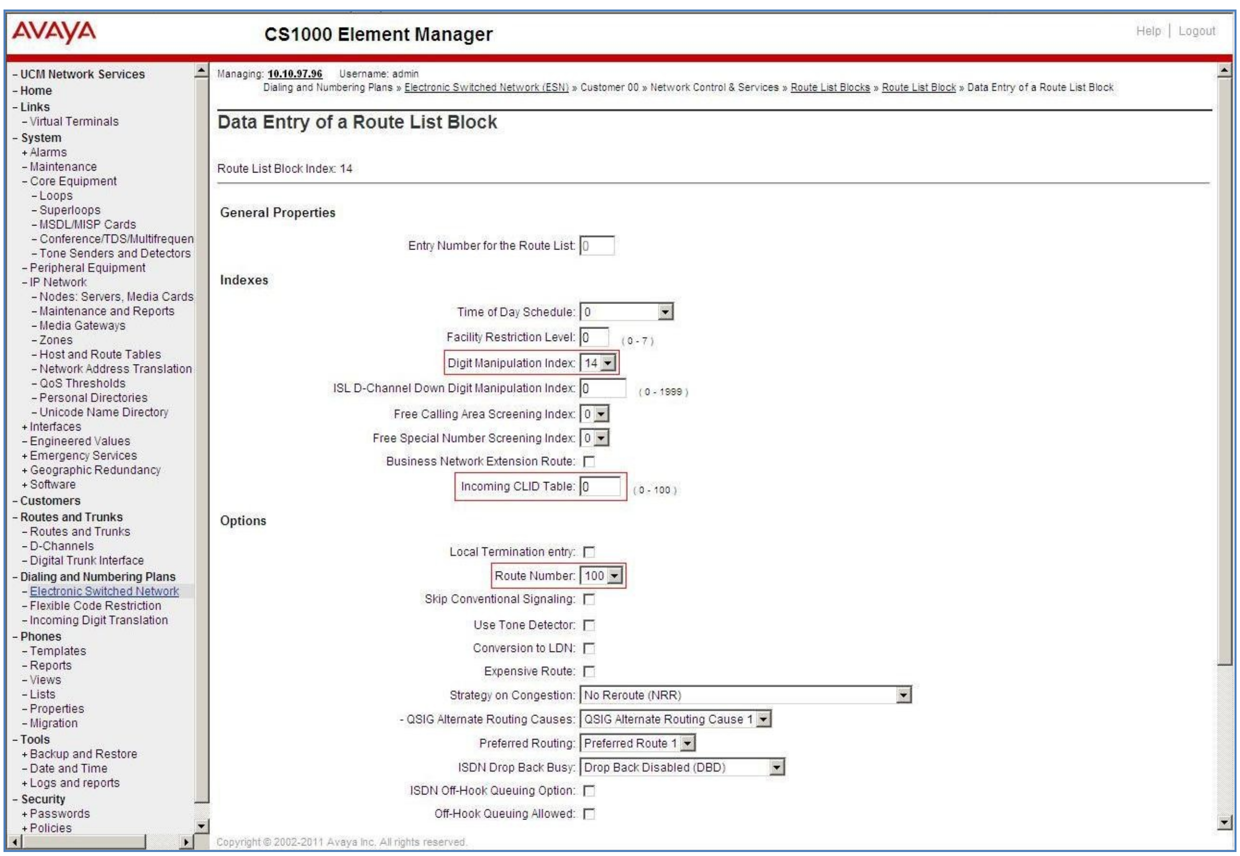


Figure 40 – RLB_14 Route List Block Configuration Details

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 15) and click on the **"to Add"** button as shown in **Figure 39**.
c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 41**). 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**)

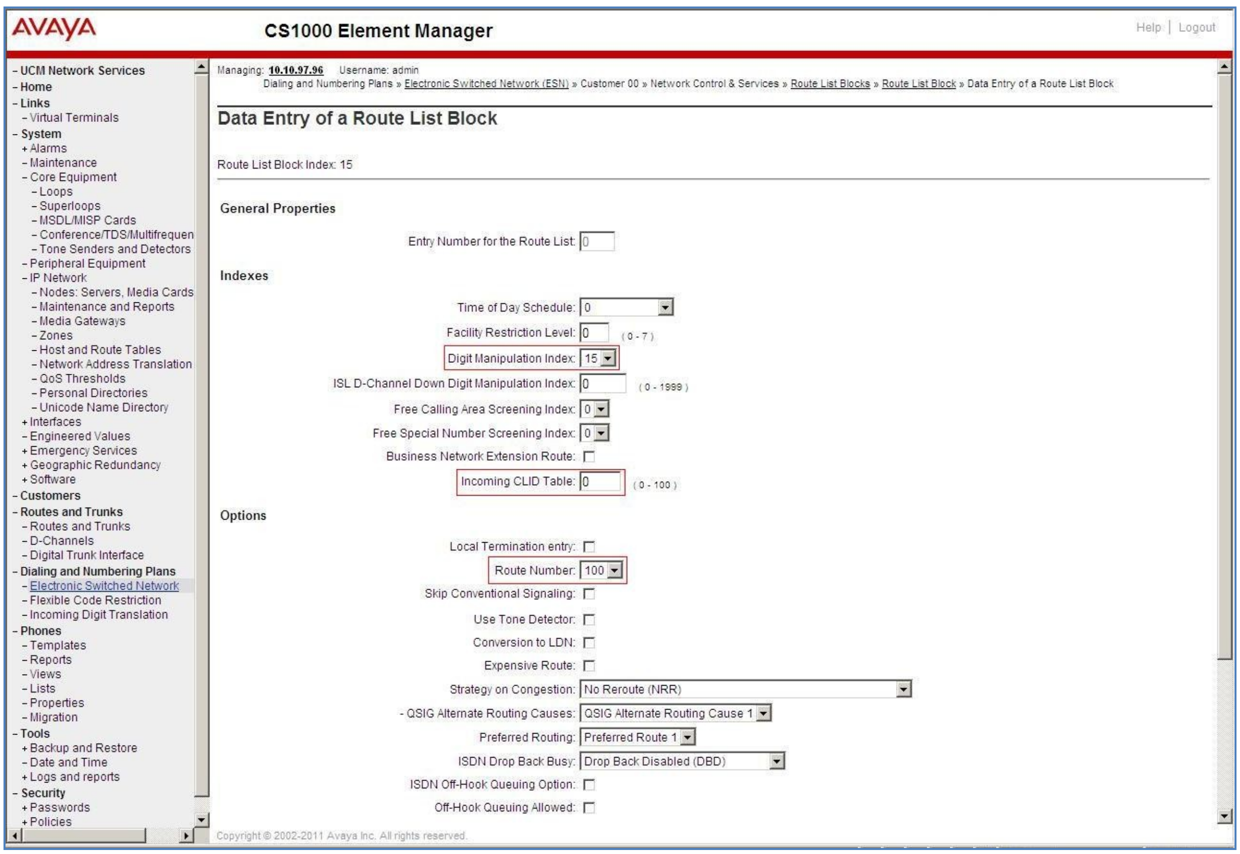


Figure 41 – RLB_15 Route List Block Configuration Details

5.6.7. Inbound Call – Incoming Digit Translation Configuration

This section describes the steps for receiving the calls from PSTN via the PAETEC Communications 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 42**.

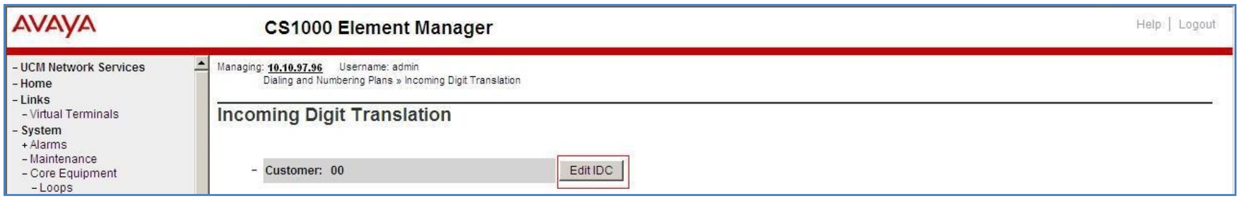


Figure 42 – Incoming Digit Translation

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 43**.

Figure 43 – Incoming Digit Conversion Property

c) Detail configuration of the Digit Conversion Tree Configuration is shown in **Figure 44**. 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 713-343xxxx will be translated to DN xxxx. The DID number 2814022045 is translated to 1700 for Voicemail accessing purpose.

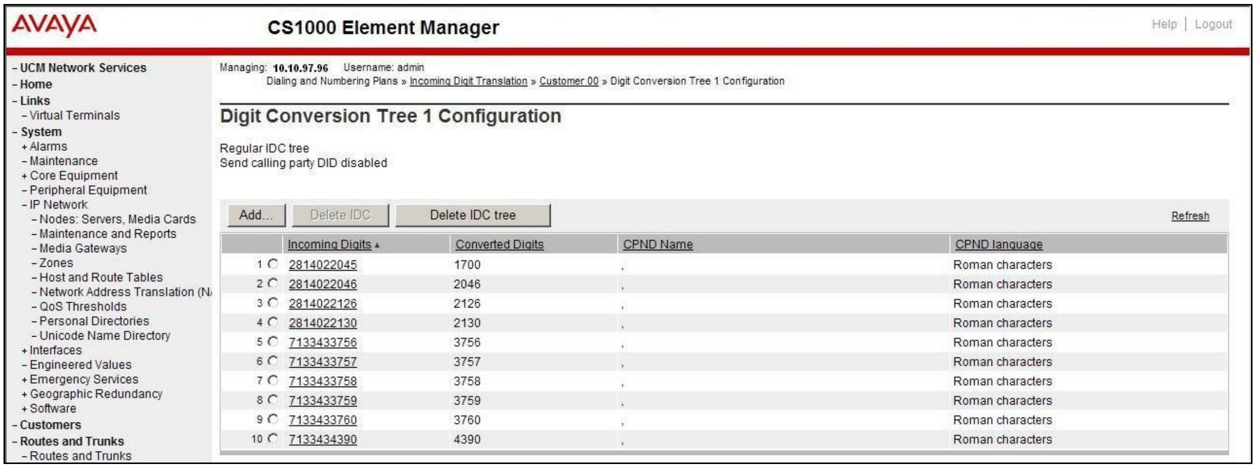


Figure 44 – Digit Conversion Tree

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 45** shows all the special number used for this testing.

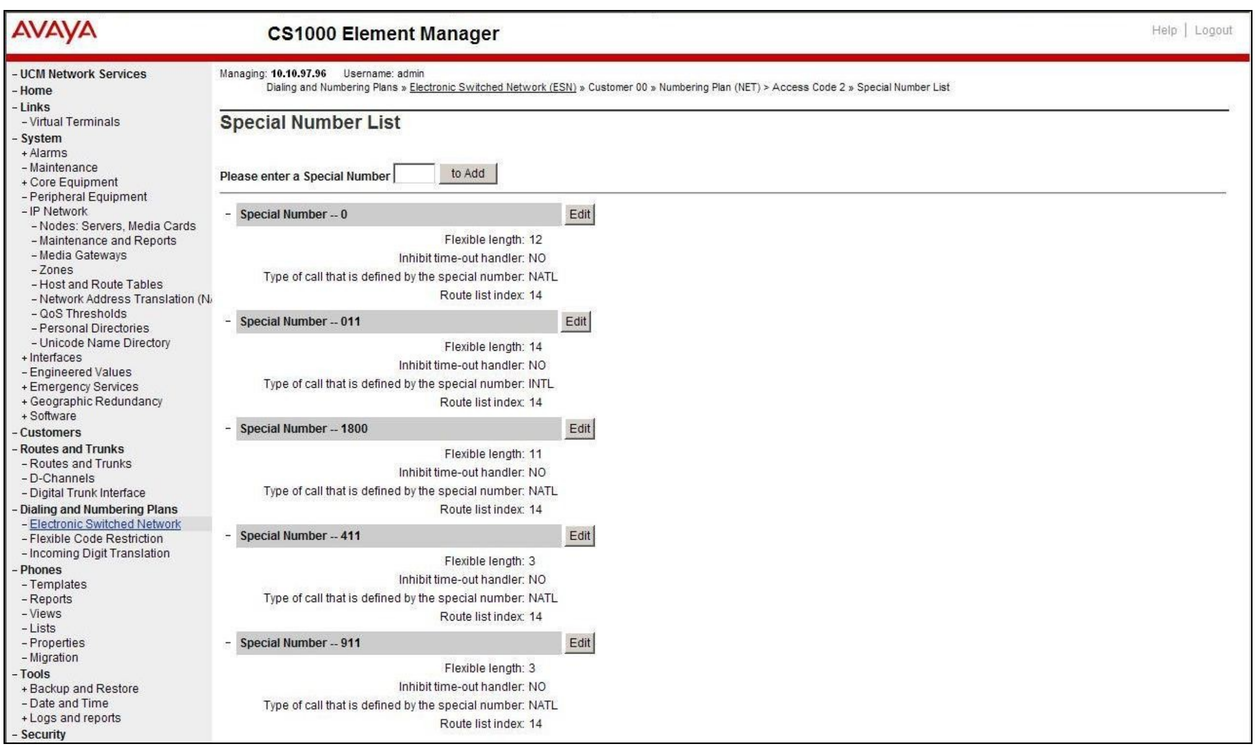


Figure 45 – Add a SPN.

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 textbox and click on the **"to Add"** button. The 1713, 1613, 1647 and 1281 area codes were used in this configuration as shown in **Figure 46**.

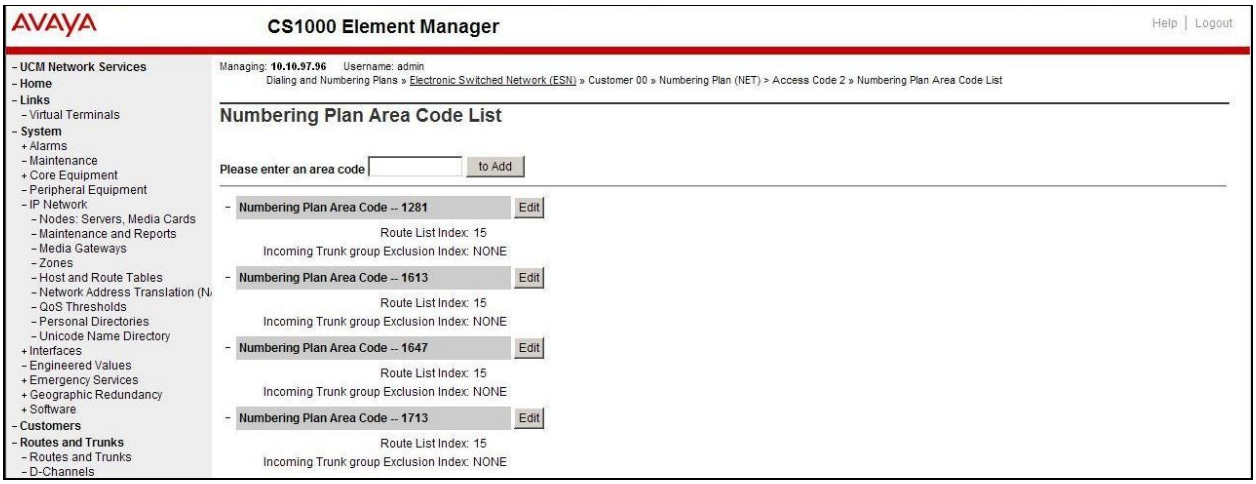


Figure 46 – Numbering Plan Area Code List

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) Log in to the Call Server Command 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 3758 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 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 cls ddgd
…
```

b) To allow display number, set CLS to **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 cls ddga
…
```

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** -> **Call Redirection**. The Call Redirection page is shown in **Figure 47**.

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

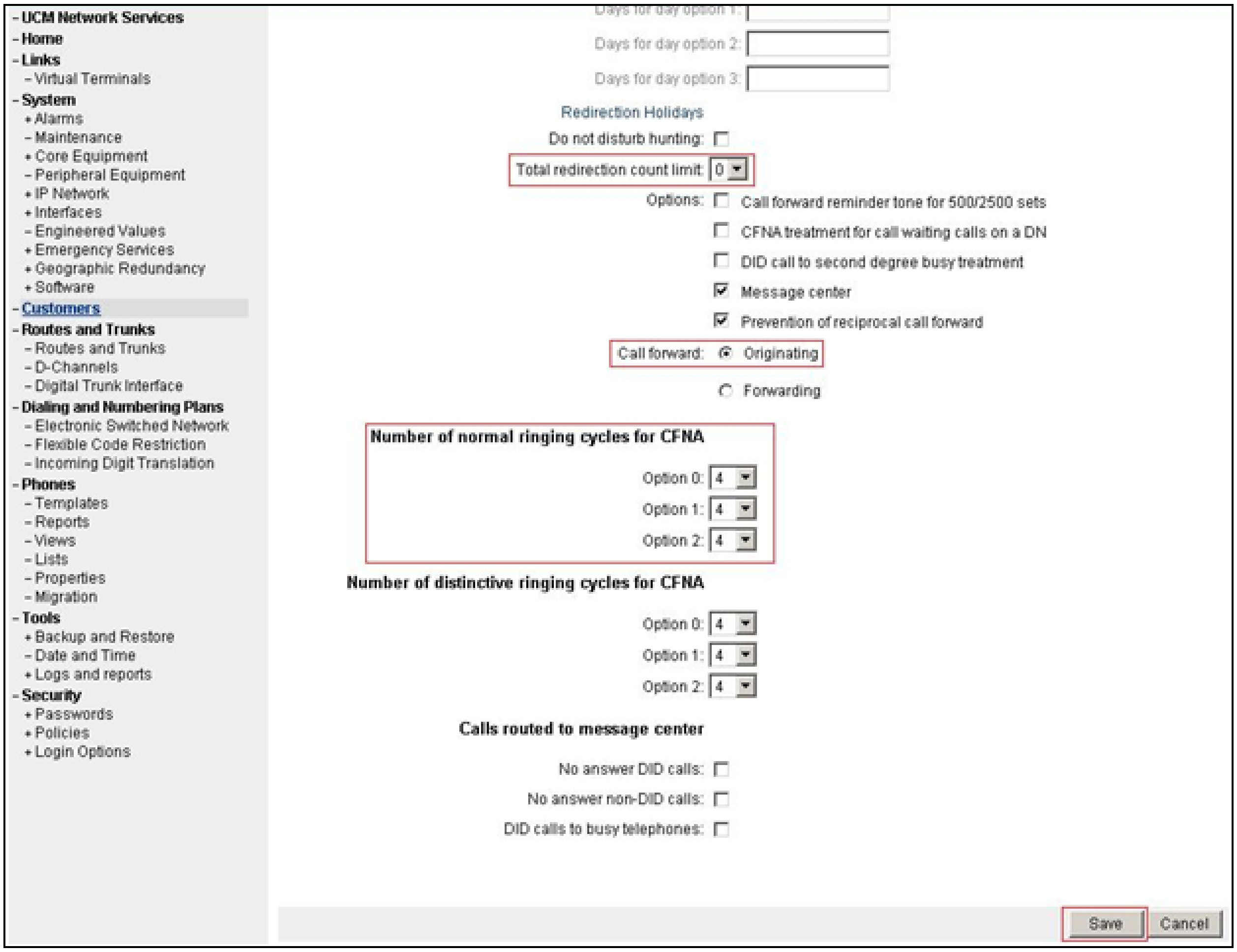


Figure 47 – Call Redirection

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
HUNT 916139675205
…
```

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.
Log in to the 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 3758 0     MARP
       CPND
         CPND_LANG ROMAN
           NAME Carrier1
           XPLN 13
           DISPLAY_FMT FIRST,LAST
    01 CWT
…
```

6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controllers necessary for interoperability with the CS1000 and PAETEC Communications systems.

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 CS1000. The remaining fields are generally the default/standard value used by the DEVSBC5 for that field.

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

6.1. Service Provider Pre-installation Wizard

Service Provider Pre-installation Wizard is a tool distributed along with SBC Release 6.0 installation packages. This wizard collects network configuration information relevant to PAETEC Communications system, and generates template file with extension EPW. Later on, EPW file is uploaded to the wizard during SBC installation.

Run **SP_Pre-Installation_Wizard_5273.exe** to the install the **Service Provider Pre-installation Wizard** on a Window based PC. After the installation is complete, invoke the wizard from **Start > All Programs > SP Pre-installation Wizard > Run SP Pre-installation Wizard.**

a) The **SP Pre-installation Wizard** will be run in a web browser. Under **Select a template**, select **SBCT** from the drop down list, and then click **Next Step** as shown in **Figure 48.**

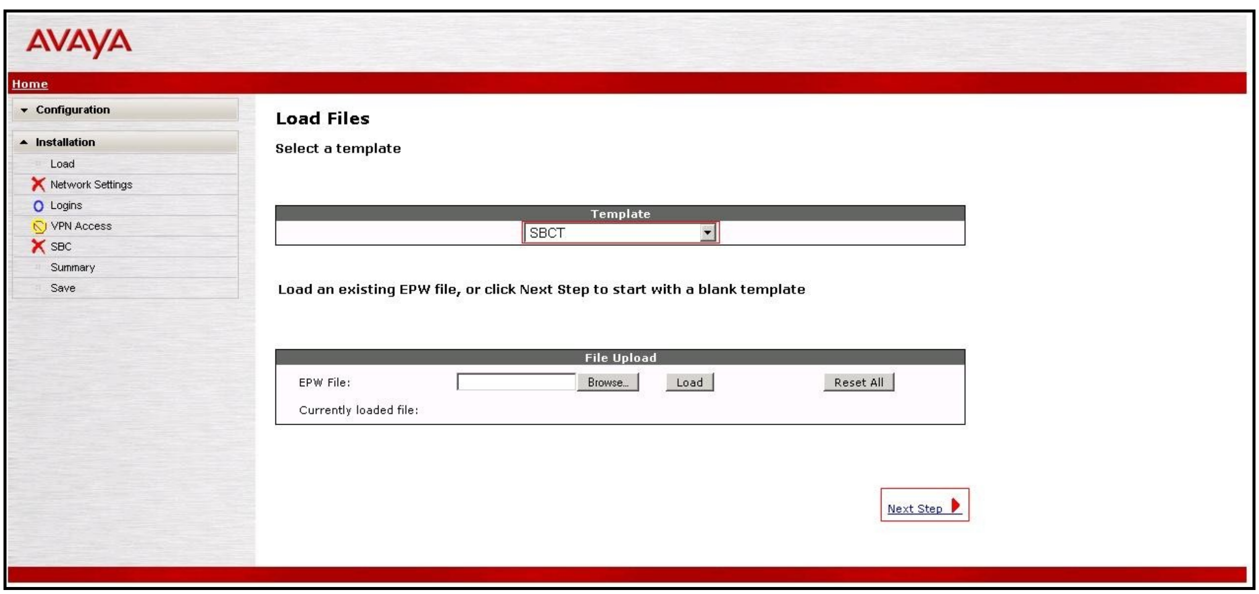


Figure 48: SP Pre-installation Wizard; Select a template

b) Next step, **Network Settings** is to configure internal interface of the DEVSBC5 to connect to enterprise CS1000 network as shown in **Figure 49**.

- **Domain0 IP Address**: IP address of System Platform system domain 0, e.g. 10.10.97.240
- **CDom IP Address**: IP address of System Platform console domain, e.g 10.10.97.241
- **Gateway IP Address**: 10.10.97.193
- **Network Mask**: 255.255.255.192
- **SBC**: IP address of SBC internal interface, e.g. 10.10.97.242
- **Hostname**: DevSBC5
- **Domain**: bvwdev.com

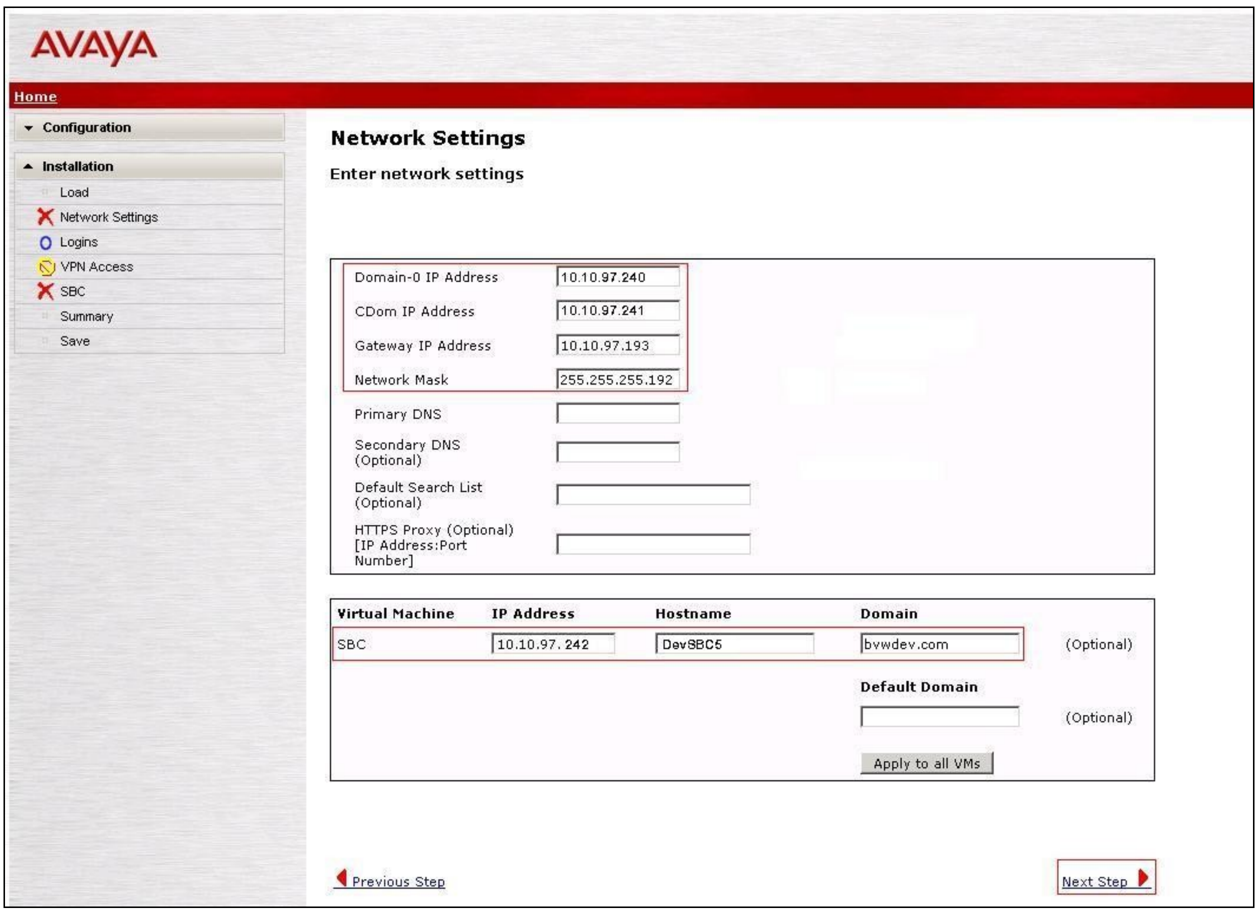


Figure 49: SP Pre-installation Wizard; Network Settings

c) Next step, the **Service logins for SBC (optional)** is to define password for account **craft**, **init** and **dadmin** as shown in **Figure 50**.

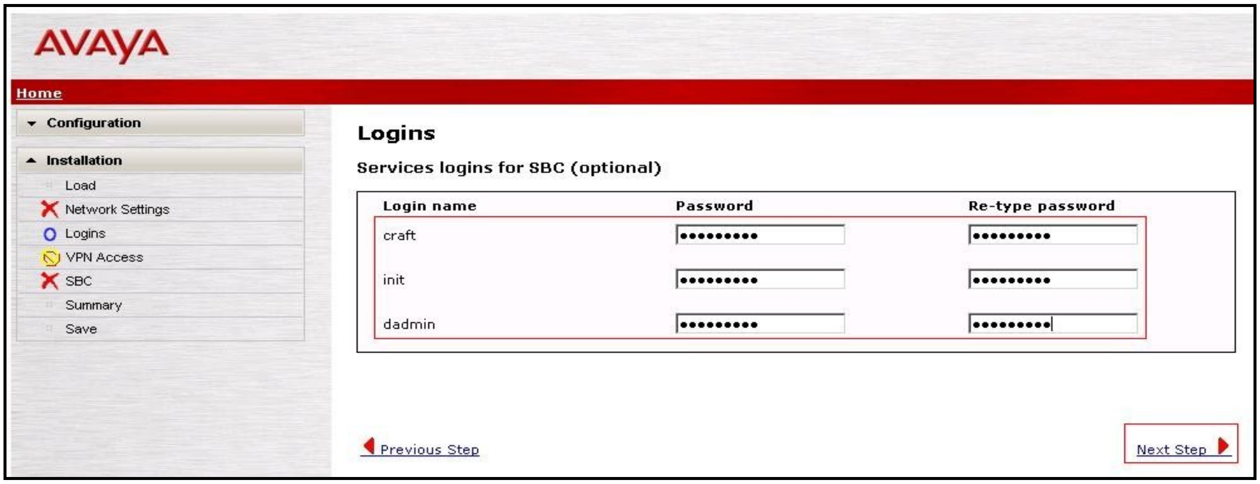


Figure 50: SP Pre-installation Wizard; Services logins for SBC (optional)

d) Next step, the **VPN Access**. The SIP Trunk connect to PAETEC Communications is not behind the VPN, so select **No** (VPN mode is disabled) then click **Next Step**.

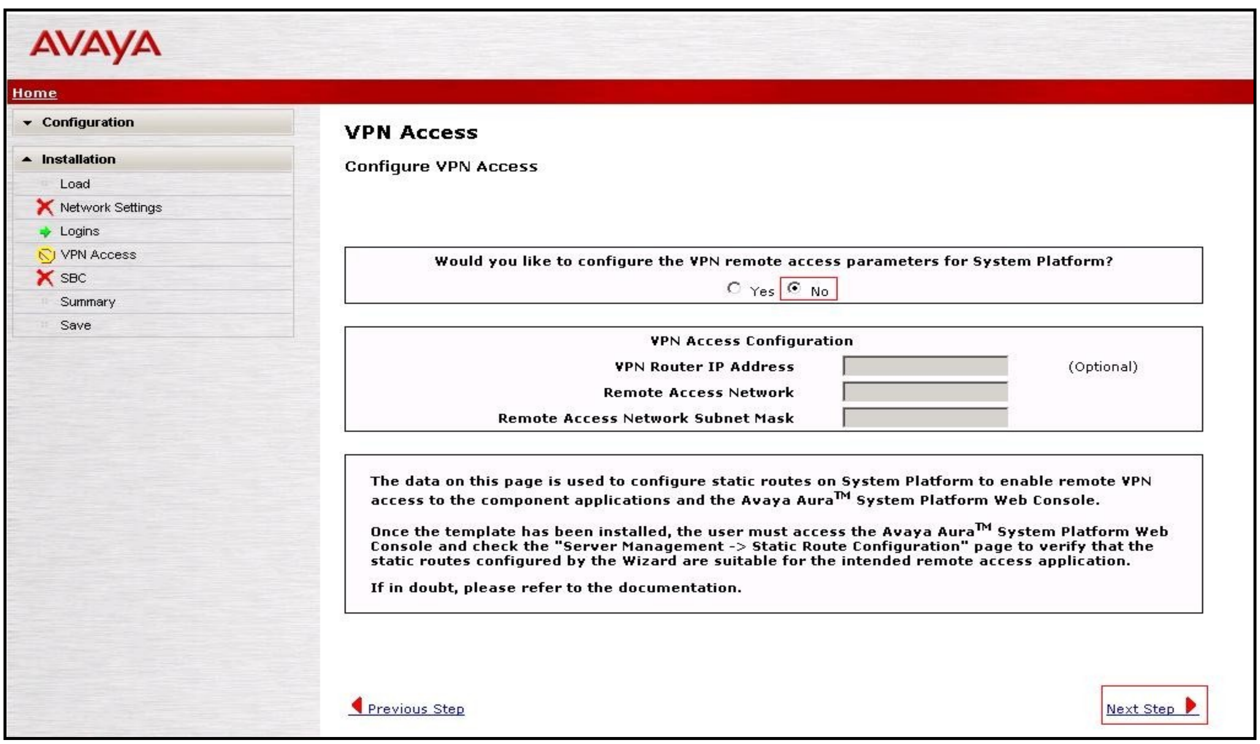


Figure 51: SP Pre-installation Wizard; VPN Access

e) Next step, **Session Border Controller Data** is to define IP address of PAETEC Communications SBC used for SIP signaling and for RTP as shown in **Figure 52**.

SIP Service Provider Data:
- **Service Provider**: Generic
- **Port**: 5060
- **IP Address1**: IP address of PAETEC Communications SBC used for SIP signaling, e.g. 20.20.64.220

SBC Network Data:
- **Public**: IP address of DevSBC5 to connect to PAETEC Communications system, e.g. 10.10.98.111
- **Net Mask**: 255.255.255.224
- **Gateway**: 10.10.98.97

Enterprise SIP Server:
- **SIP Domain**: bvwdev.com
- **IP Address1**: the IP address of Node IP of CS1000 Server (please refer to **Section 5.2.1**), e.g. 10.10.97.178
- **Transport1**: UDP

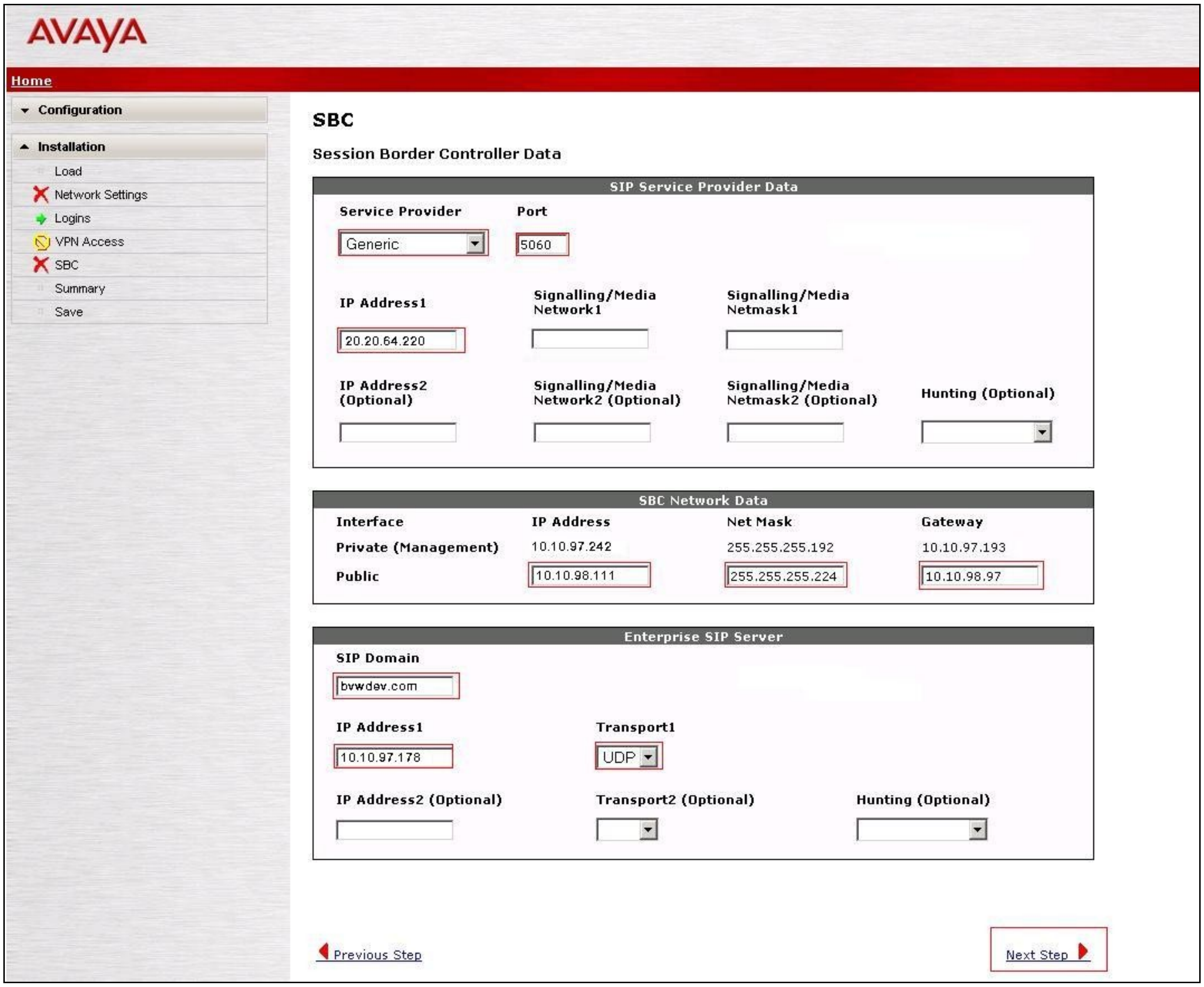


Figure 52: SP Pre-installation Wizard; Session Border Controller Data

f) Next step, **Summary** is to give an overview of the configuration as shown in **Figure 53**. Scroll down then click on the **Next Step** (not shown)

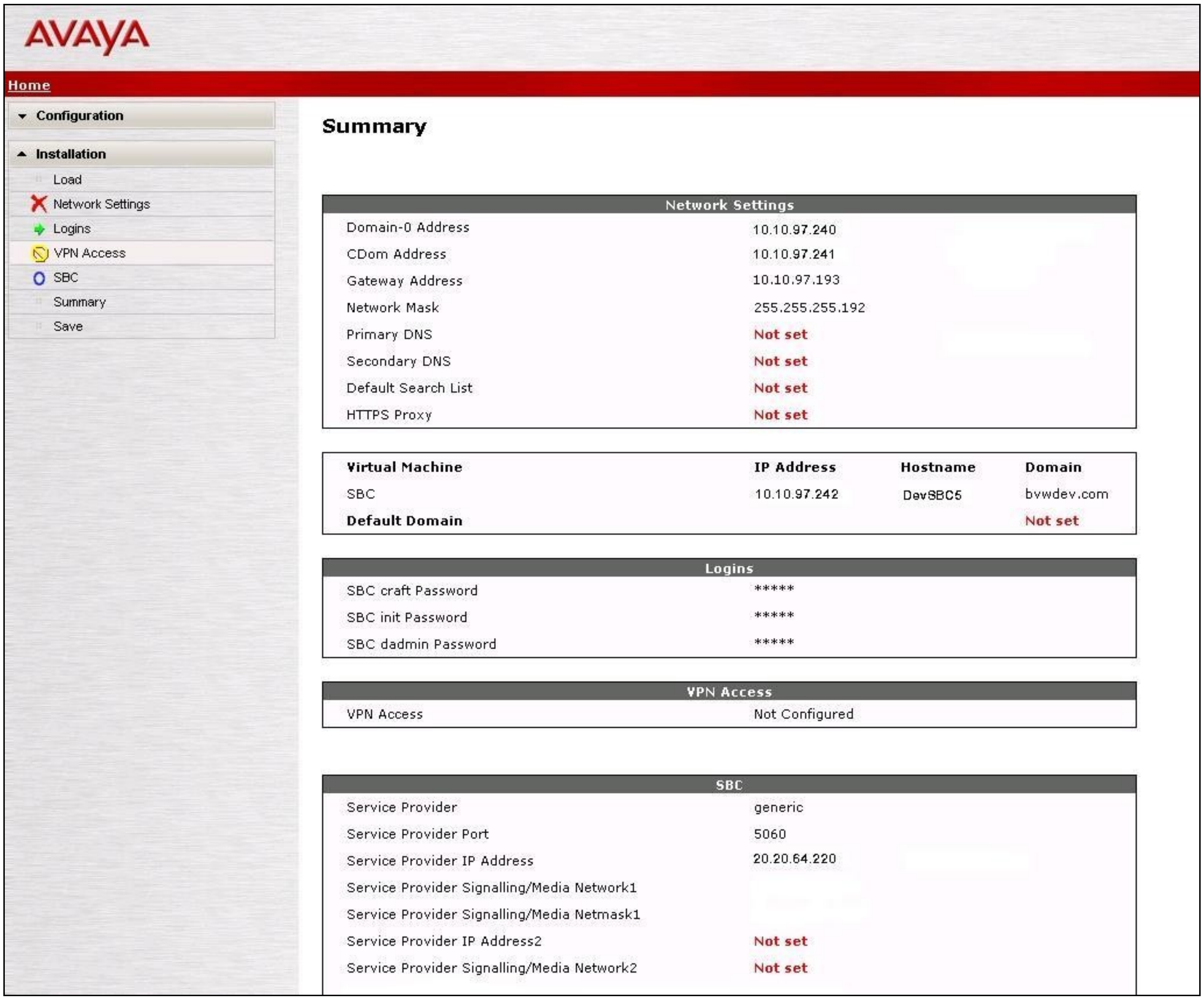


Figure 53: SP Pre-installation Wizard; Summary

g) Next step, **Save** is to give an option to save the configuration as an EPW file. Click **Accept** then **Save EPW file** as shown in **Figure 54**.

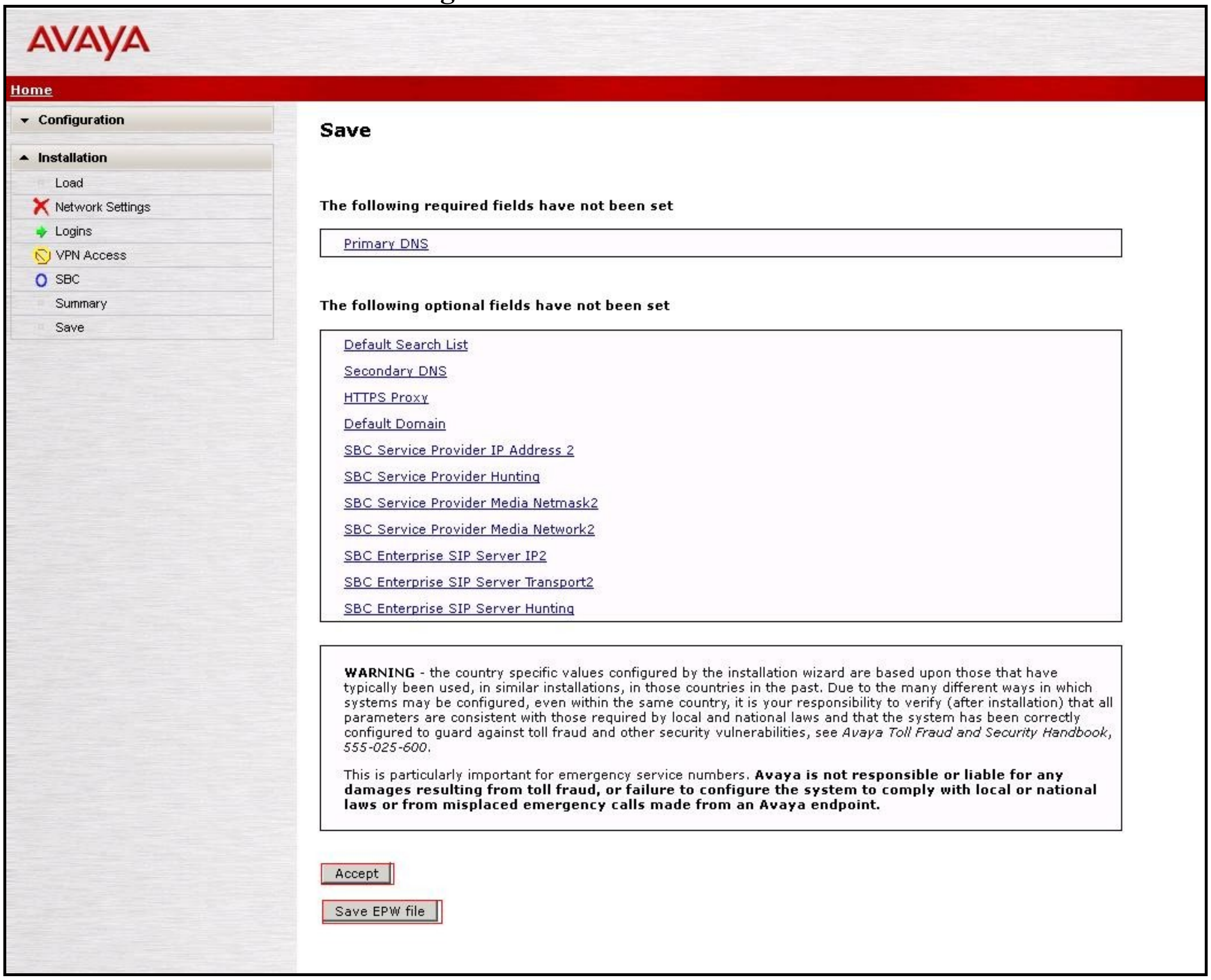


Figure 54: SP Pre-installation Wizard; Save

h) Download and save the EPW file.

6.2. DevSBC5 Installation

To install Avaya Aura SBC, follow installation guide provided on http://support.avaya.com. The installation wizard (not shown) is an automation tool.

During installation, EPW file is needed. Please use EPW file created in **Section 6.1** to upload to the wizard. After the installation is complete, continue to configure the SBC as described in **Section 6.3**.

6.3. Administer Enterprise Servers

To login to DevSBC5, https://SBCIPAddress/. Enter username as craft and appropriate password to login.

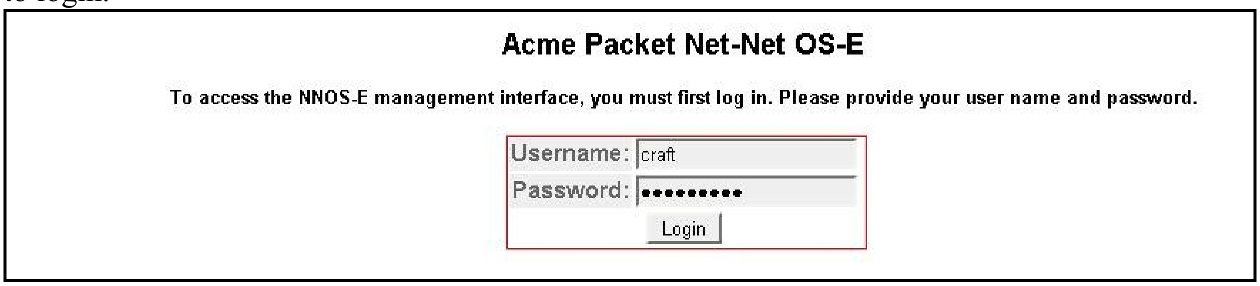


Figure 55: Login to AA-SBC

During installation, the information in EPW file was used to populate the entry "**server Paetec**", which is information of PAETEC Communications SBC for SIP Trunking and the entry "**server PBX**" which is the information of CS1000 server.

6.3.1. Configuration of "server Paetec"

To verify the configuration of "**server Paetec**", select **Configuration > vsp > enterprise > servers > sip-gateway Paetec > server-pool > server Paetec**. The entry "**server Paetec**" is shown in **Figure 56**.

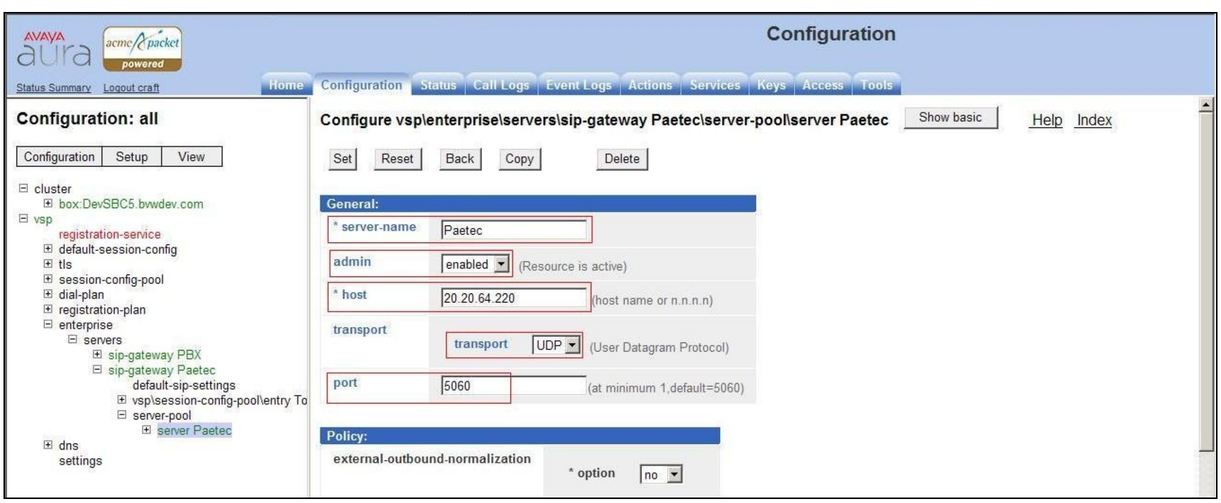


Figure 56: Server-Paetec Configuration

6.3.2. Configuration of "server PBX"

To verify the configuration of "**server PBX**", select **Configuration > vsp > enterprise > servers > sip-gateway PBX > server-pool > server PBX**. The entry "**server PBX**" is shown in **Figure 57**

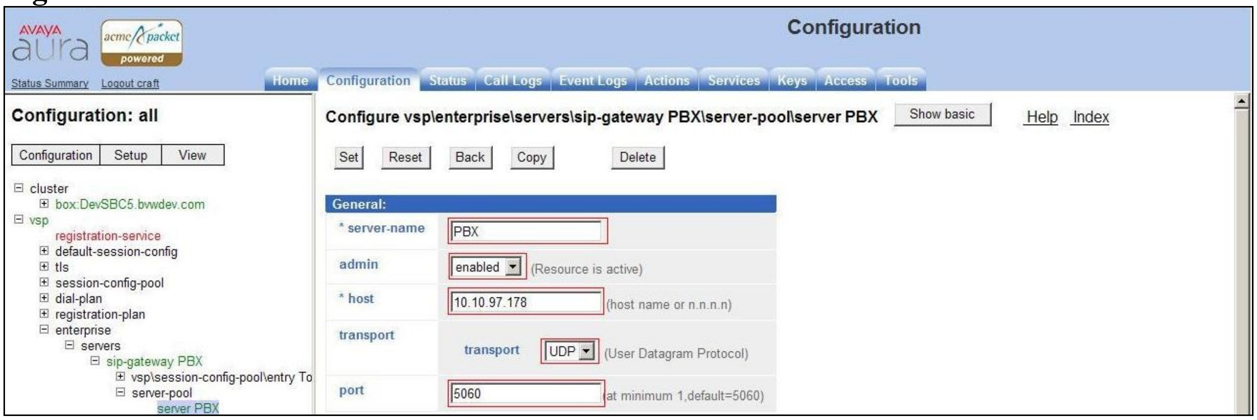


Figure 57: Server-PBX Configuration.

6.4. Administer Heartbeat

The DEVSBC5 was configured to send "**register**" to PAETEC Communications system for keep a-live purpose.

To send "register" to PAETEC Communications system, select **Configuration > vsp > enterprise > servers > sip-gateway Paetec** then select **"enabled"** for admin**, "20.20.64.220"** for domain and **"register"** for **"failover-detection**" as shown in **Figure 58**.

Figure 58: Keep Alive Configuration for sip-gateway Paetec

To set up registration with VNI user that PAETEC Communications provides, select **Configuration > vsp > enterprise > servers > sip-gateway Paetec** then put user as "7133434387" as shown in **Figure 59**.

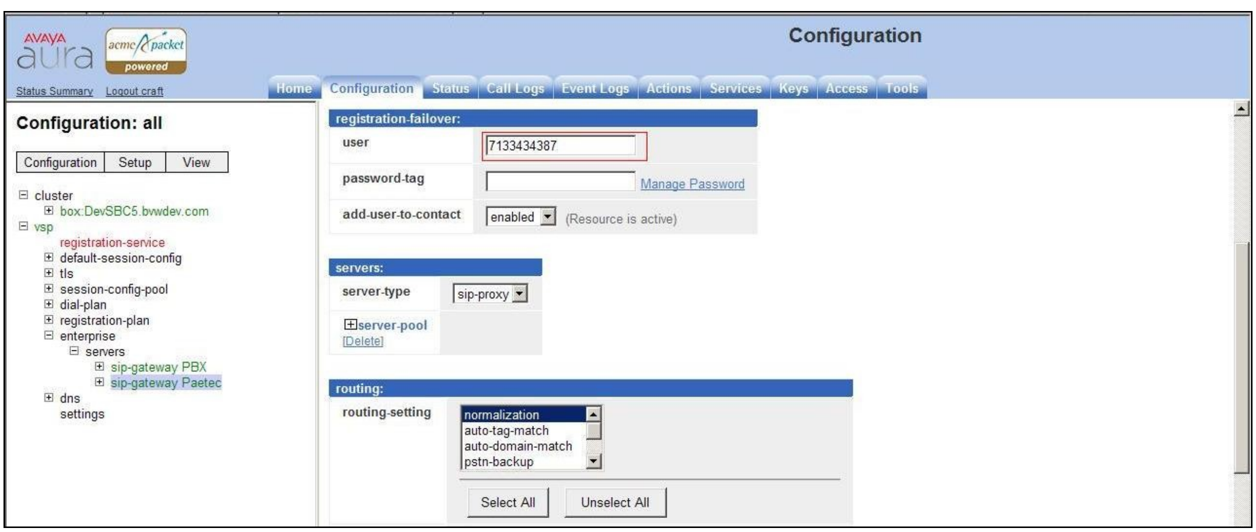


Figure 59: Registration Configuration for sip-gateway Paetec

6.5. Administer dial-plan

The DevSBC5 has typical dial-plans to route the SIP call from CS1000 to PAETEC Communications system and vice versa.

6.5.1. The entry "source-route FromPBX"

The entry "**source-route FromPBX**" as shown in **Figure 60, 61** below is to route the SIP call from CS1000 to PAETEC Communications system.

- **source-server**: vsp\enterprise\servers\sip-gateway **PBX**
- **peer server**: vsp\enterprise\servers\sip-gateway **Paetec**
- **priority**: 100 (default)
- **condition-list-match-secondary**: false
- **apply-to-methods**: Select All
- **session-config**: vsp\session-config-pool\entry ToPaetec

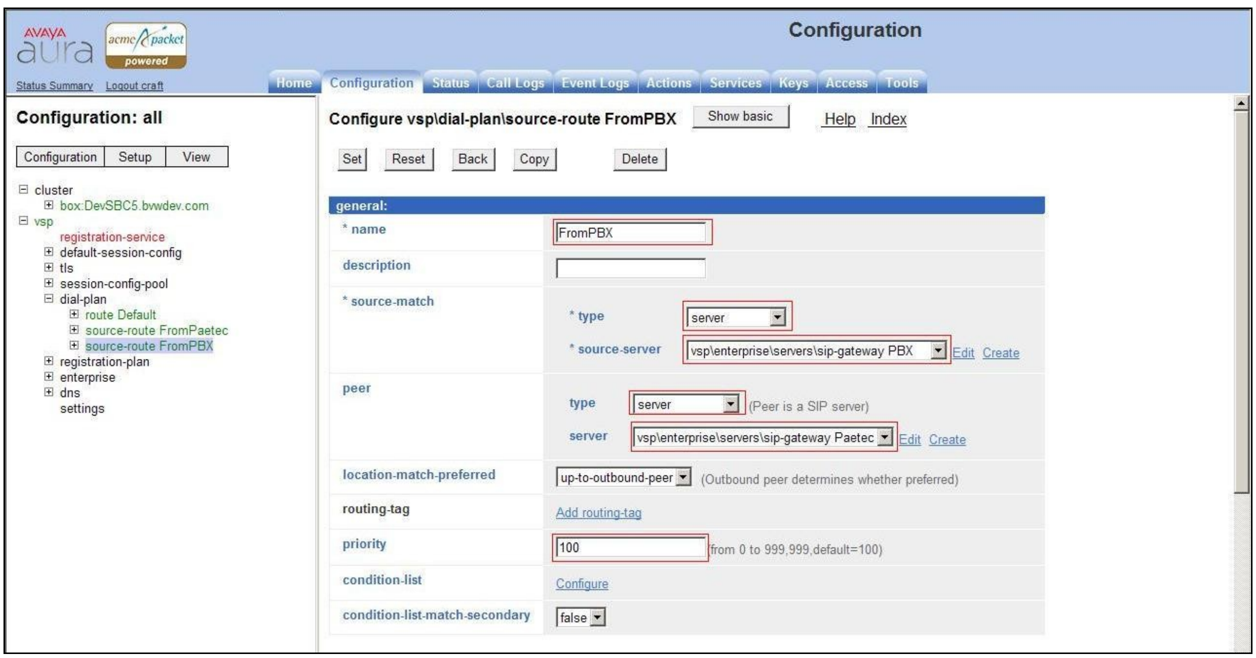


Figure 60: Dial-plan "source-route FromPBX" Page 1

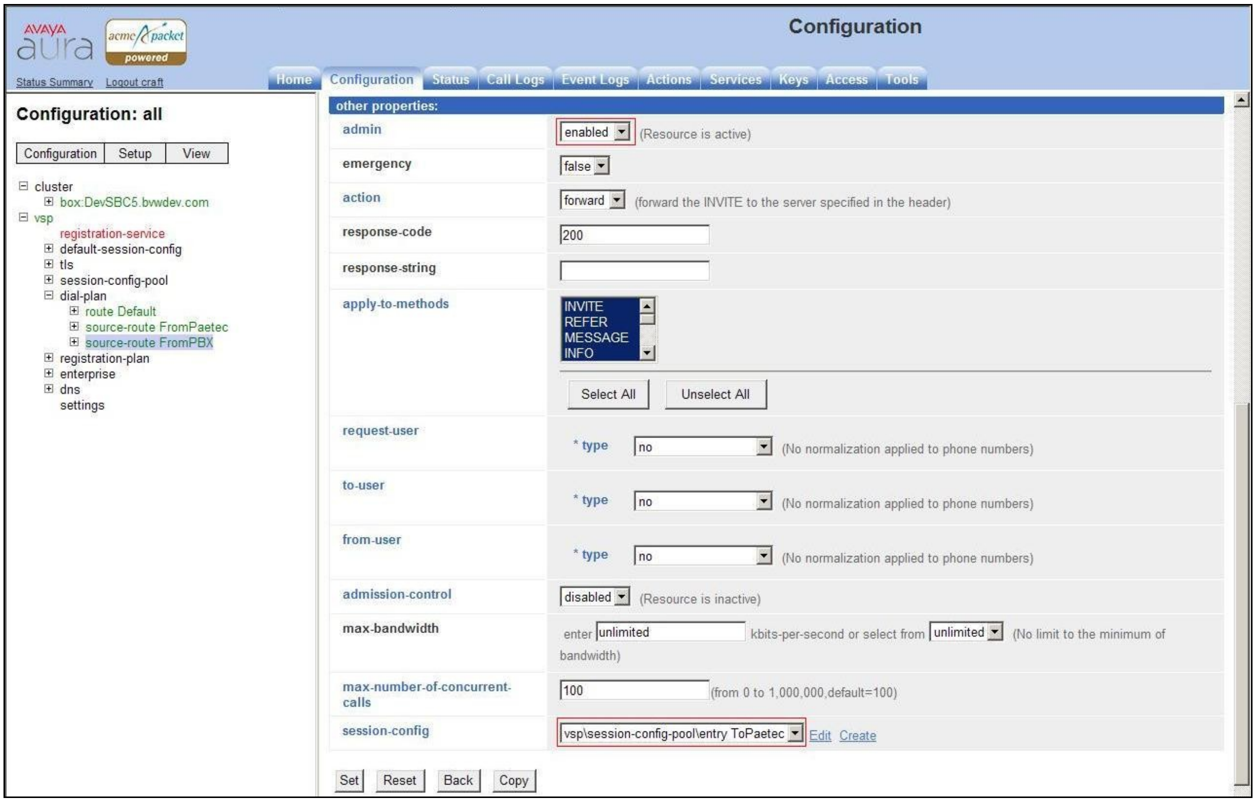


Figure 61: Dial-plan "source-route FromPBX" Page 2

6.5.2. The entry “source-route FromPaetec”

The entry “**source-route FromPaetec**” as shown in **Figure 62, 63** below is to route the SIP call from PAETEC Communications system to CS1000.

- **source-server**: vsp\enterprise\servers\sip-gateway **Paetec**
- **peer server**: vsp\enterprise\servers\sip-gateway **PBX**
- **priority**: 100 (default)
- **condition-list-match-secondary**: false
- **apply-to-methods**: Select All
- **session-config**: vsp\session-config-pool\entry **ToPBX**

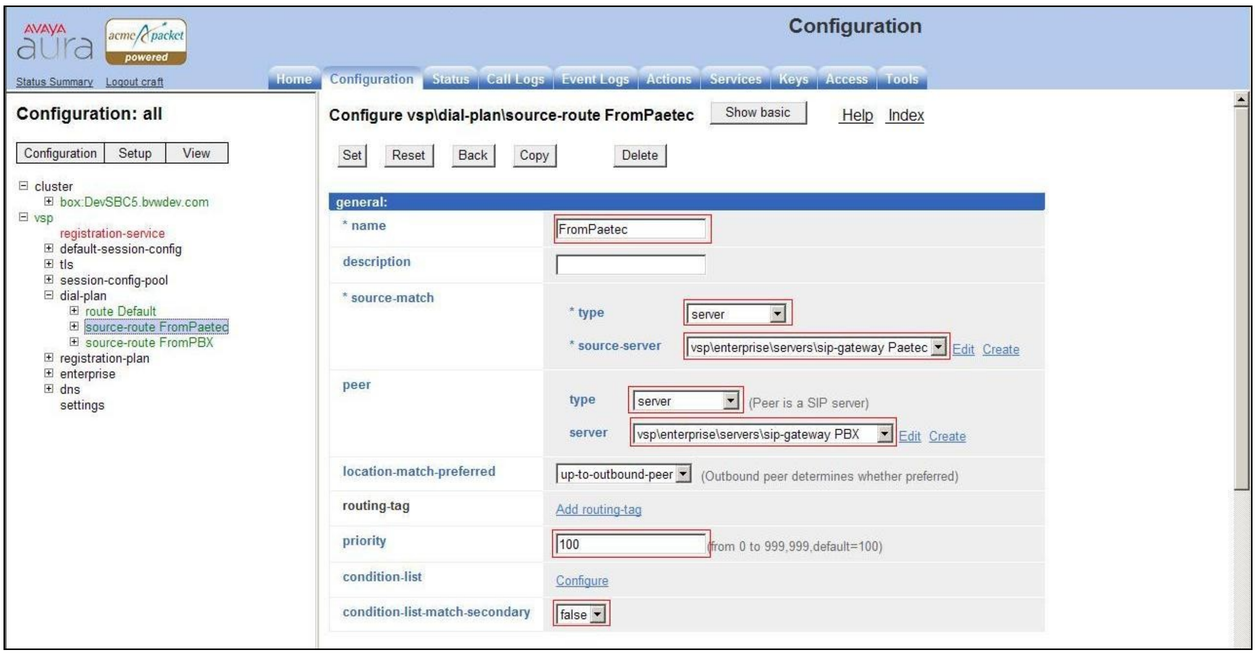


Figure 62: Dial-plan “source-route Paetec” Page 1

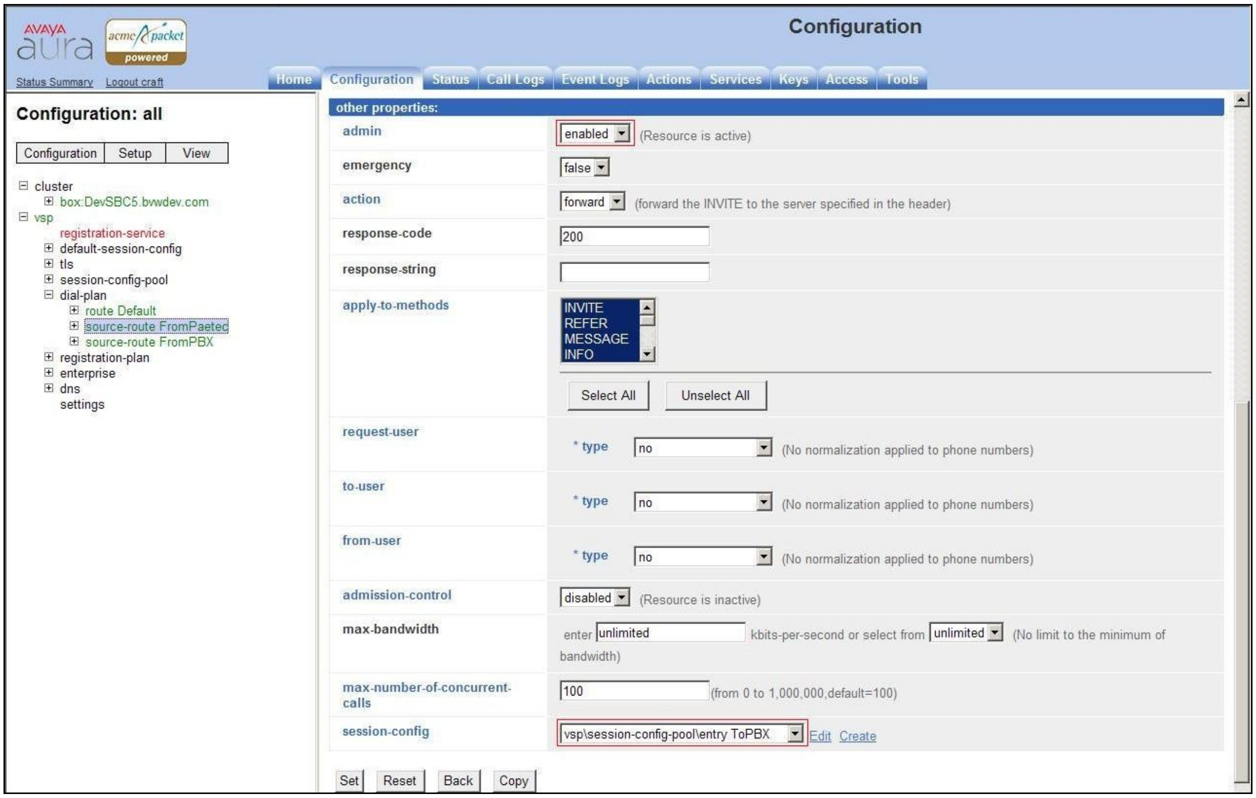


Figure 63: Dial-plan "source-route Paetec" Page 2

6.6. Administer session-config-pool "entry ToPaetec"

6.6.1. Administer sip-settings

During testing, PAETEC Communications system experiences IP packet lost when travel over internet. This issue can be preventing by increasing **max-retransmissions** on DevSBC5.

To increase **max-retransmissions**, select **Configuration vsp\session-config-pool\entry ToTelco\sip-settings.** Then change the value of **max-retransmissions** from 1 to 10 as shown in **Figure 64.**

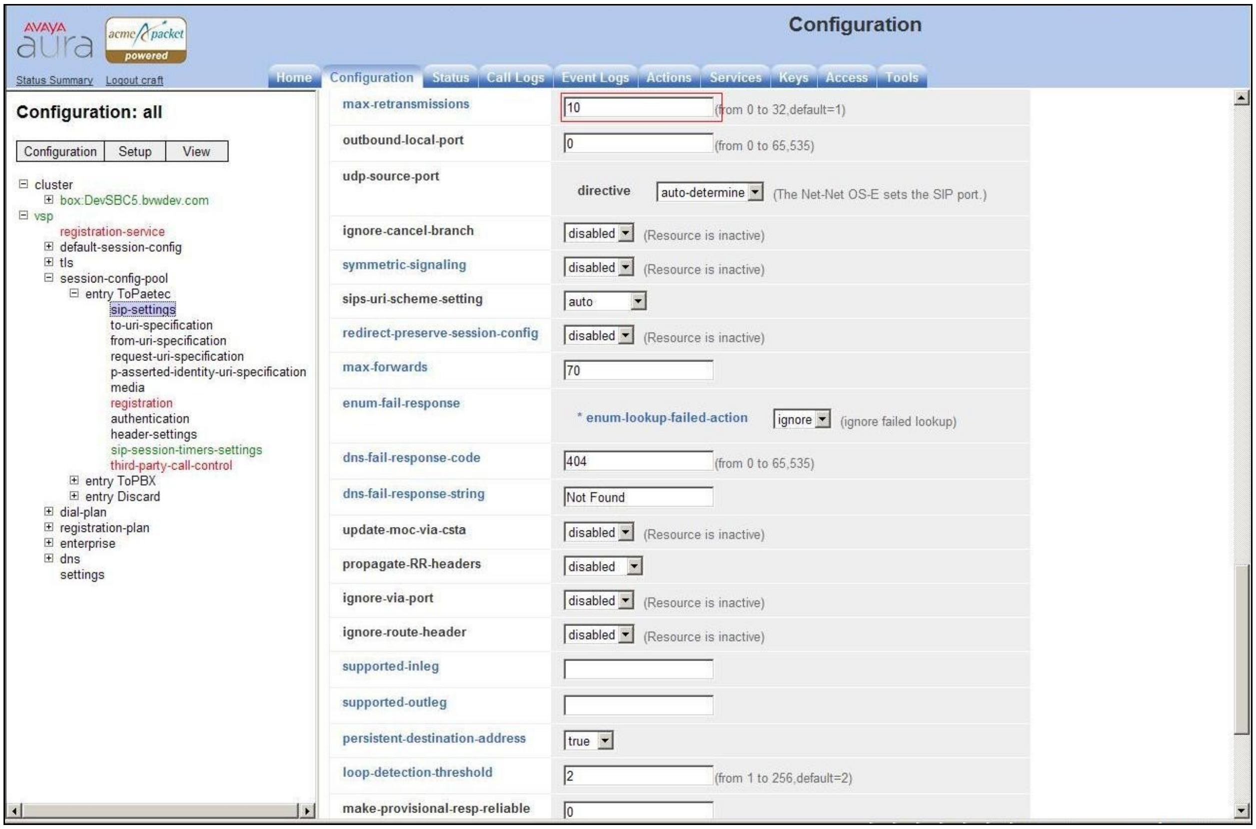


Figure 64: Increase the max- retransmissions setting

By default AA-SBC does not forward PRACK from CS1000 to PAETEC Communications system. It causes issue with ringback tone cannot be sent to PSTN in case of offnet call forward no answer. To enable PRACK forwarding, go to **Configuration vsp\session-config-pool\entry ToPaetec\sip-settings** click "**Show advance**" (not shown), then under "**message-options**" set "**forward-provisional-ack**" to **enable** (as shown in **Figure 65**)

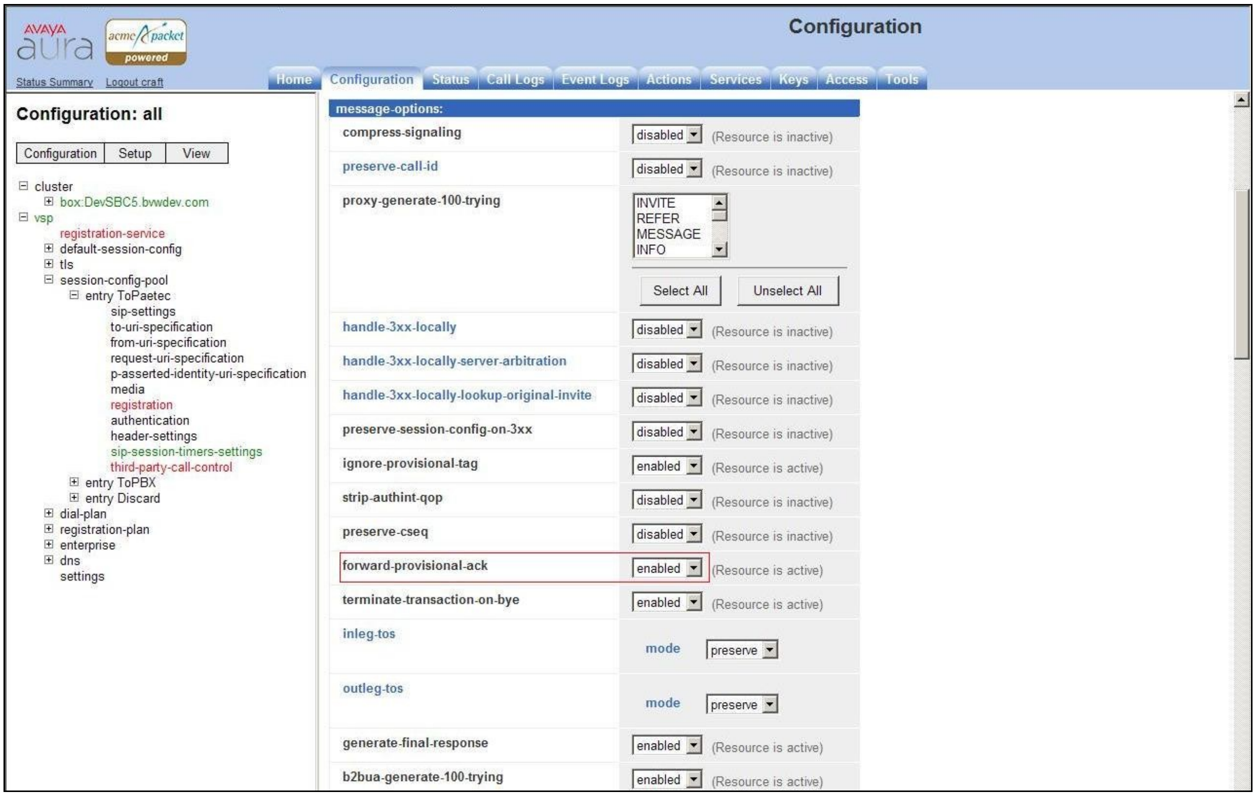


Figure 65: Enable PRACK forwarding

6.6.2. Manipulate From, To, Request-URI, and P-Asserted-Identity headers.

The CS1000 SIP gateway was configured with domain name bvwdev.com (please refer to **Section 5.5.2**). However, PAETEC Communications system expects to receive IP address instead of a valid domain name.

This section shows the configuration on DevSBC5 to change domain name bvwdev.com into an IP address. The change is applied to SIP headers From, To, Request-URI and P-Asserted-Identity.

a) Manipulate **From** header
Select **Configuration vsp\session-config-pool\entry ToPaetec\from-uri-specification.** Then change **host** to send **local-ip** as shown in **Figure 66.** The DevSBC5 presents its public IP address in the **From** header.

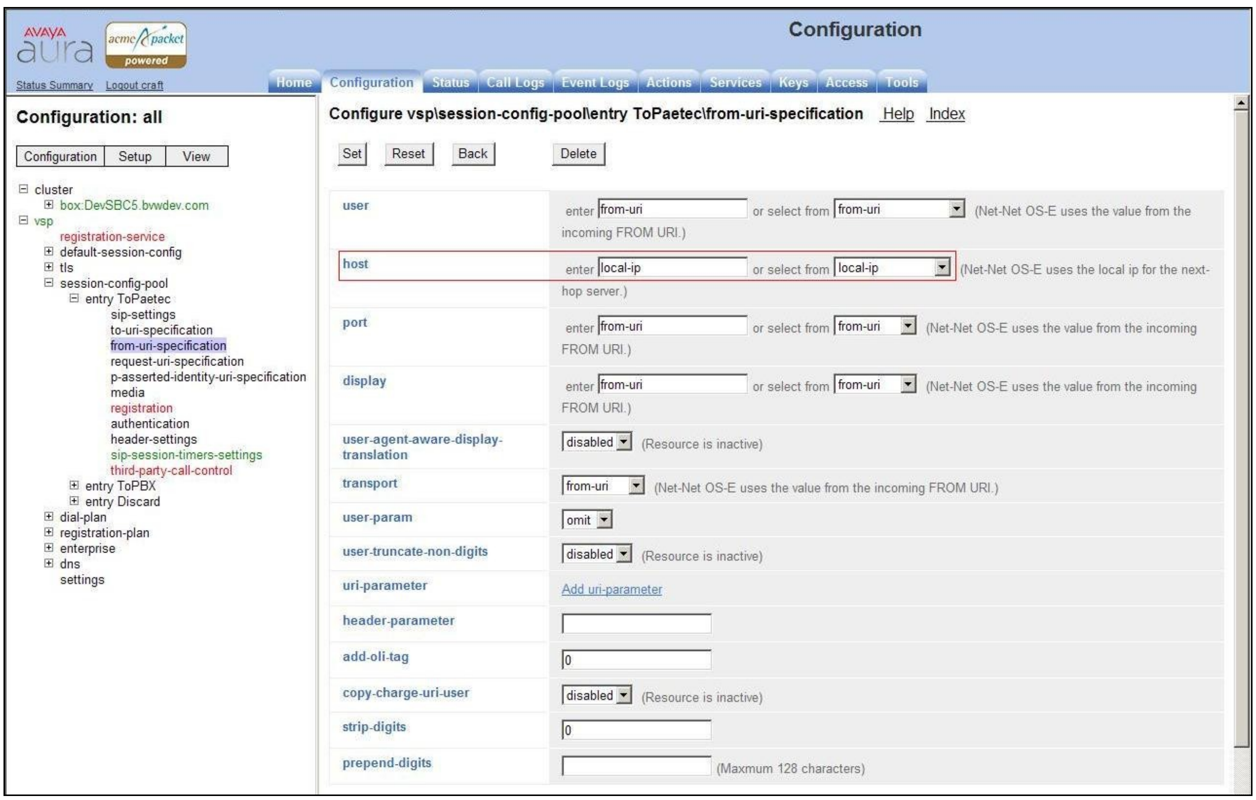


Figure 66: Manipulate From header of session-config-pool "entryToPaetec"

b) Manipulate **To** header
Select **Configuration vsp\session-config-pool\entry ToPaetec\to-uri-specification.** Then change **host** to send **next-hop** as shown in **Figure 67.** The DevSBC5 presents PAETEC Communications SBC IP address in the **To** header.

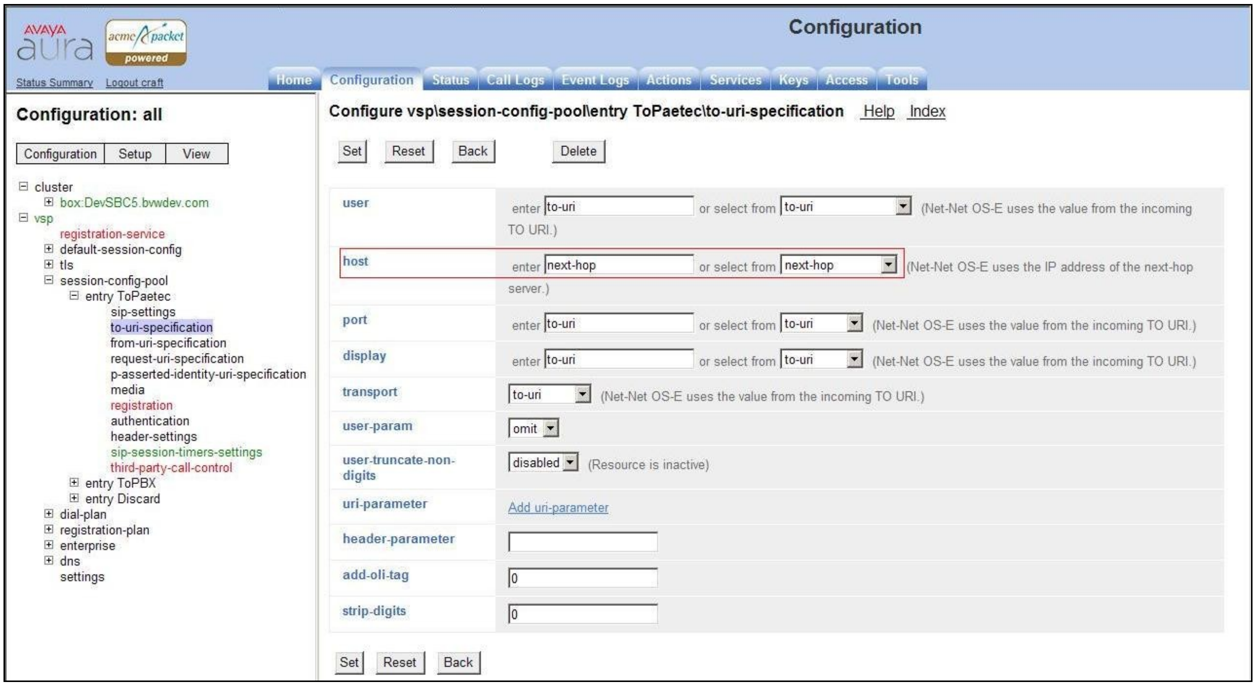


Figure 67: Manipulate To header of session-config-pool "entryToPaetec"

c) Manipulate **Request-URI** header

Select **Configuration vsp\session-config-pool\entry ToPaetec\request-uri-specification.** Then change **host** to send **next-hop** as shown in **Figure 68.** The DevSBC5 presents PAETEC Communications SBC IP address in the **Request-URI** header.

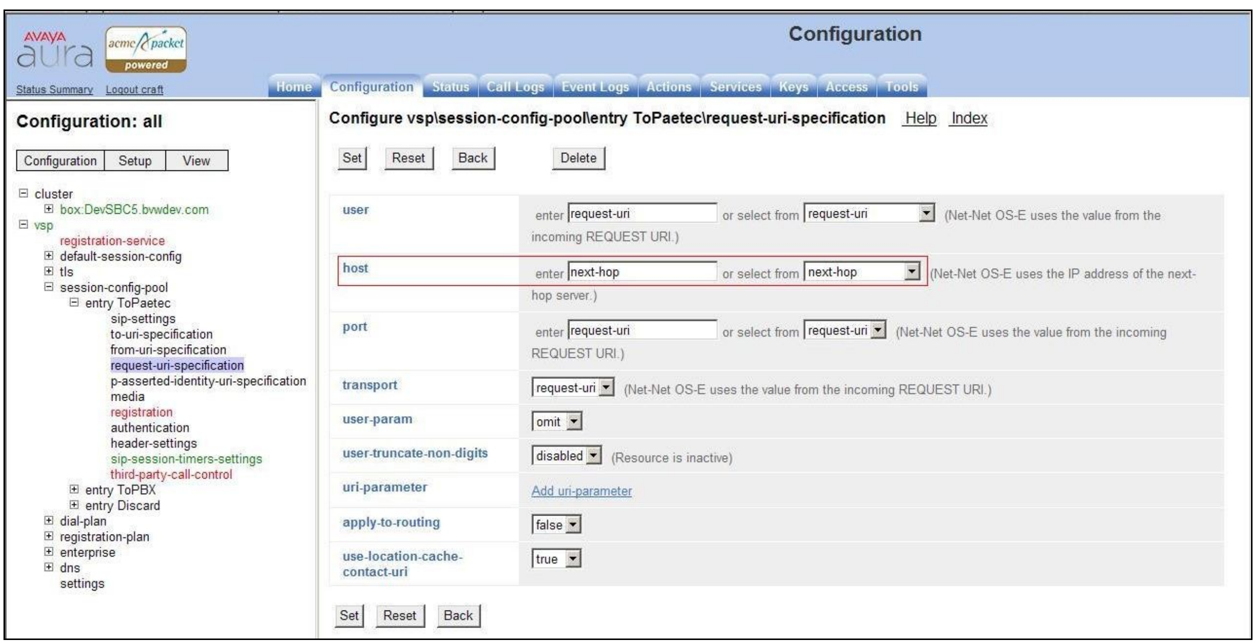


Figure 68: Manipulate Request-URI header of session-config-pool "entryToPaetec"

d) Manipulate **P-Asserted-Identity** header
Select **Configuration vsp\session-config-pool\entry ToPaetec\p-asserted-identity-uri-specification.** Then change **host** to send **local-ip** as shown in **Figure 69.** The DevSBC5 presents its public IP address in the **P-Asserted-Identity** header.

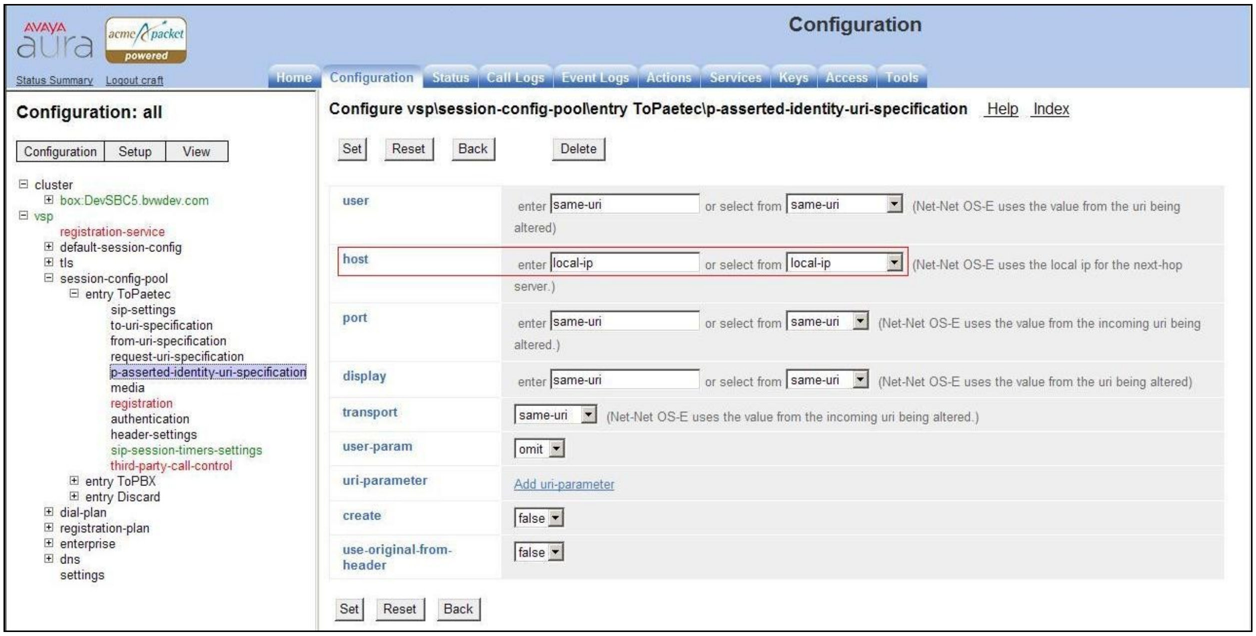


Figure 69: Manipulate P-Asserted-Identity header of session-config-pool "entryToPaetec"

6.6.3. Administer media

This session shows the configuration to enable media anchoring on DevSBC5.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToPaetec\media.** Then change **anchor** to **enable** as shown in **Figure 70.**

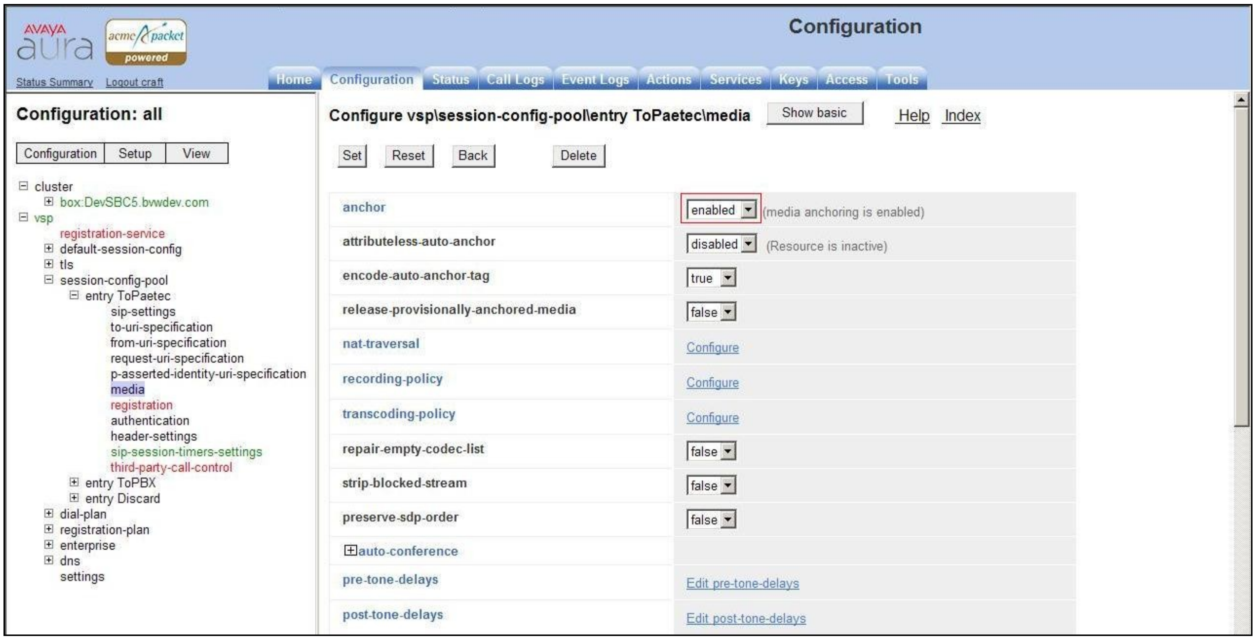


Figure 70: Enable media anchoring

6.6.4. Administer sip-session-timers-setting

By default the **sip-session-timers-setting** was disabled on DevSBC5. The session timers should be turned on to let DevSBC5 terminate the unsuccessfully call attempts to PSTN.

To enable **sip-session-timers-setting**, select **Configuration vsp\session-config-pool\entry ToPaetec\ sip-session-timers-setting.** Then change **admin** state to **enable** as shown in **Figure 71.**

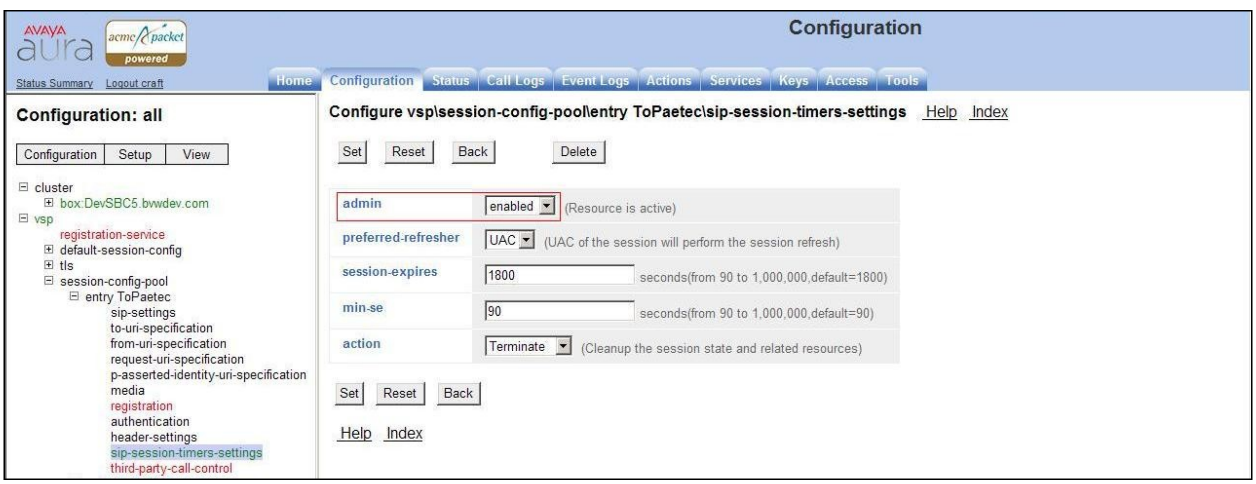


Figure 71: Enable SIP session timers

6.6.5. Enable third-party-call-control

The third-party-call-control has to be enabled on DevSBC5 to interworking with PAETEC Communications system.

To enable the **third-party-call-control**, select **Configuration > vsp > session-config-pool > entry ToPaetec > third-party-call-control.** Then change the **admin** state to **Enabled** as shown in **Figure 72.**

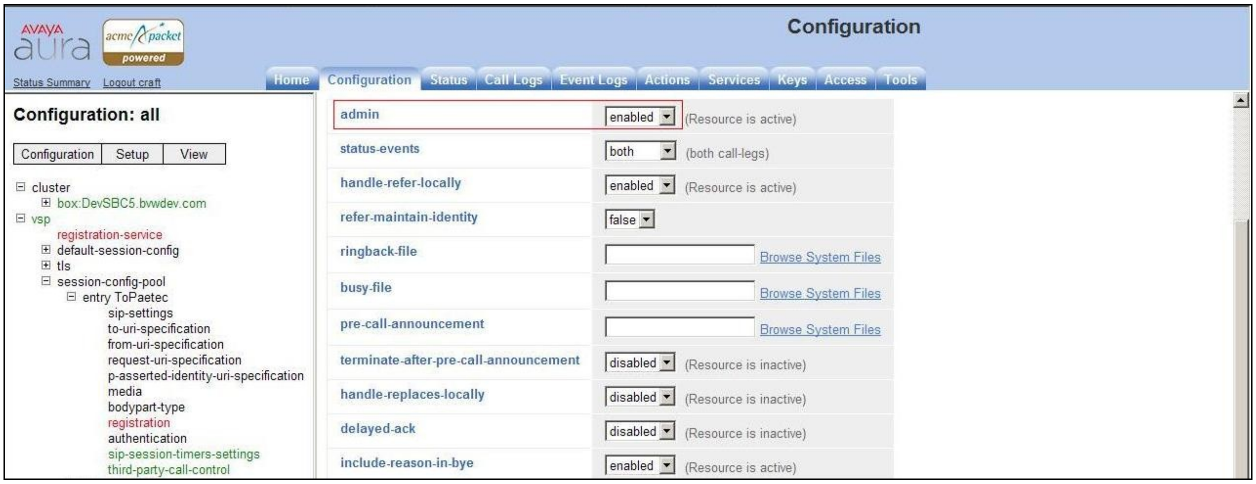


Figure 72: Enable third-party-call-control

6.7. Administer session-config-pool "entry ToPBX"

6.7.1. Manipulate To, Request-URI headers.

The CS1000 SIP gateway was configured with domain name bvwdev.com (please refer to Section 5.5.2). However, PAETEC Communications system prefers to IP address in SIP headers. This section shows the configuration on DevSBC5 to manipulate SIP headers To and Request-URI before sending to CS1000.

a) Manipulate **To** header
Select **Configuration vsp\session-config-pool\entry ToPBX\to-uri-specification.** Then change **host** to send **next-hop-domain** as shown in **Figure 73.** The DevSBC5 presents domain **bvwdev.com** in the **To** header sent to CS1000.

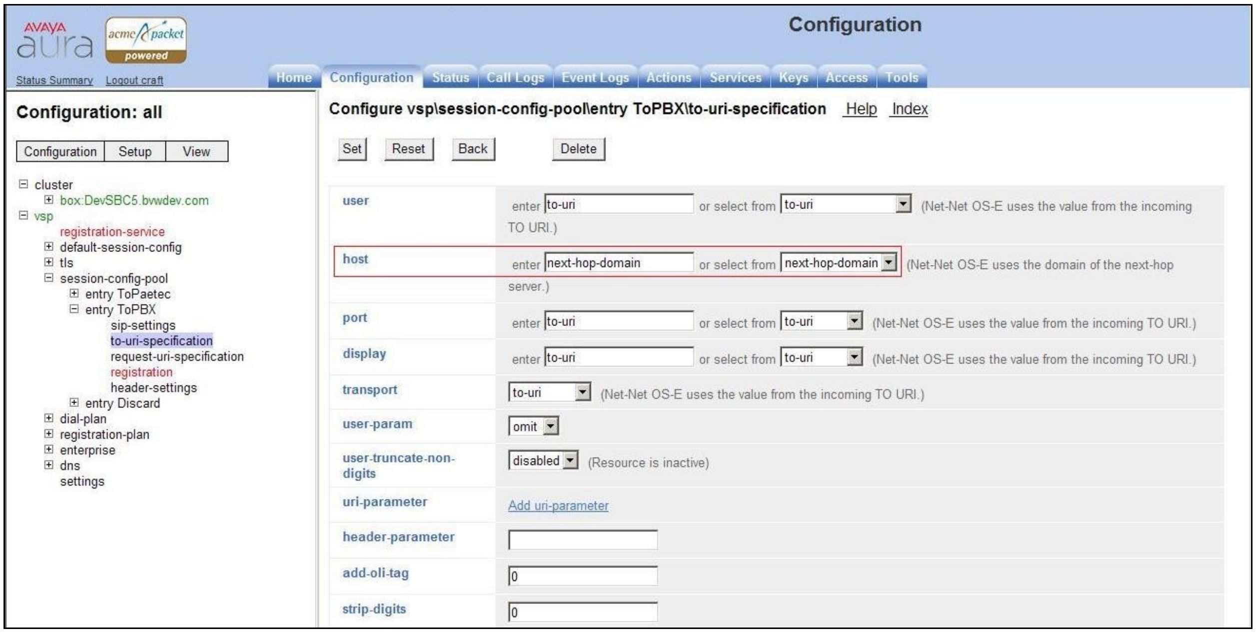


Figure 73: Manipulate To header of session-config-pool "entryToPBX"

b) Manipulate **Request-URI** header
Select **Configuration vsp\session-config-pool\entry ToPBX\request-uri-specification.** Then change **host** to send **next-hop-domain** as shown in **Figure 74.** The DevSBC5 presents domain **bvwdev.com** in the **Request-URI** header sent to CS1000.

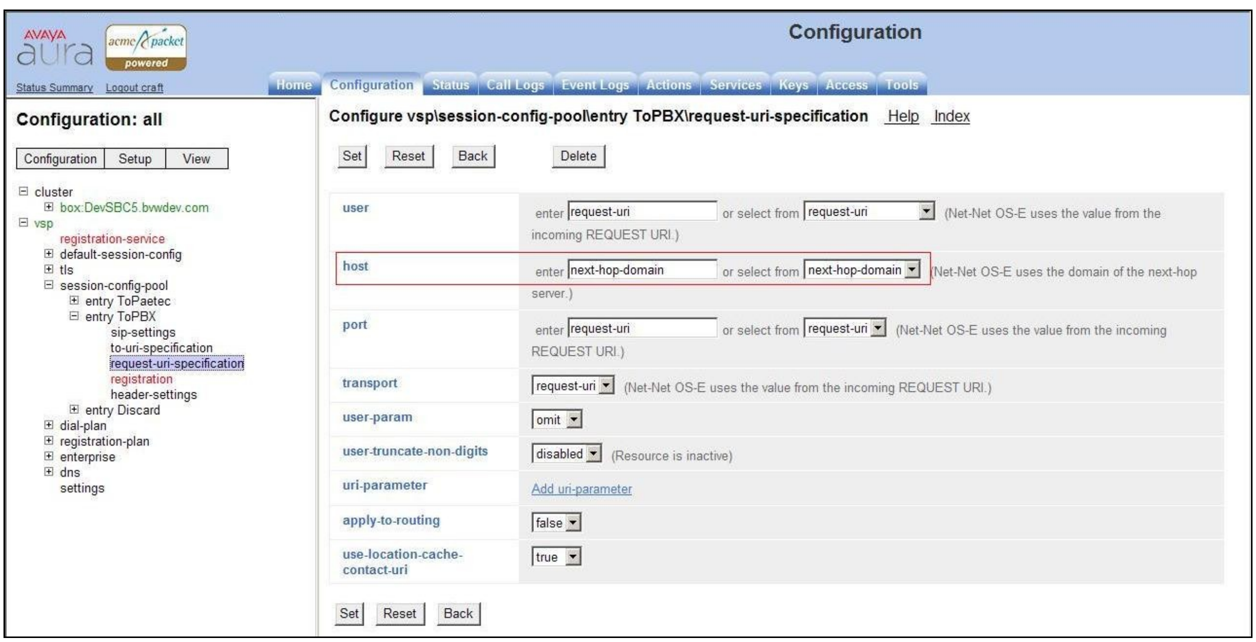


Figure 74: Manipulate Request-URI header of session-config-pool "entryToPBX"

6.7.2. Administer media

This session shows the configuration to enable media anchoring on DevSBC5.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToPBX\media.** Then change **anchor** to **enable** as shown in **Figure 75.**

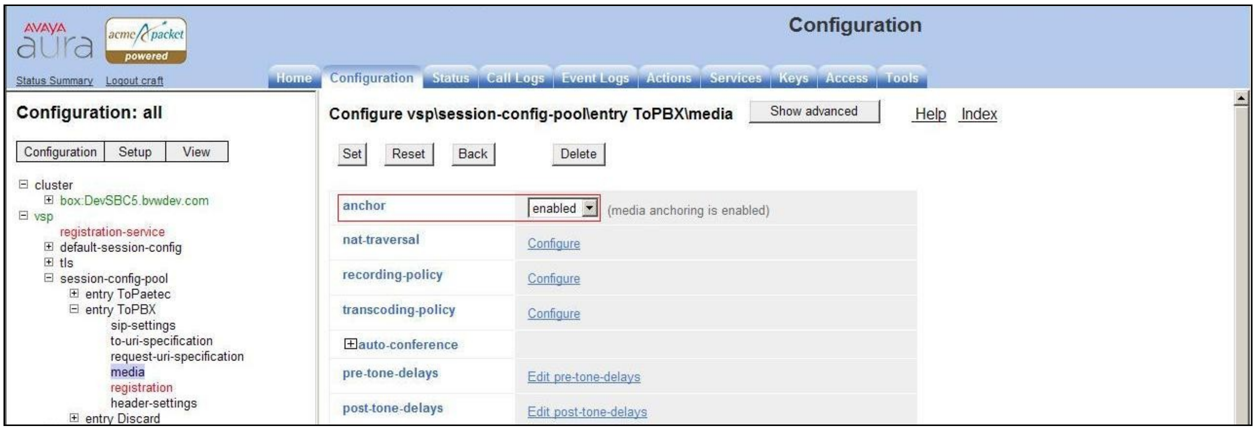


Figure 75: Enable media anchoring

6.8. Convert History-Info to Diversion header for Call Forward All Call Scenario

The procedure to create a rule to convert History-Info to Diversion header on DevSBC5 is as below:

- Create an entry in session-config-pool with a particular regular expression header rule to convert History-Info to Diversion header
- Create a "condition-matching" **source-route dial-plan** with higher priority than default **source-route dial-plan "FromPBX"**. The priority tells DevSBC5 to apply this dial-plan if the condition is matched.

6.8.1. Create entry session-config-pool "Moved Temp"

a) Create entry **session-config-pool "Moved Temp"**

To create entry **session-config-pool "Moved Temp"**, select **Configuration vsp\session-config-pool**. Click **Add entry** link as shown in **Figure 76**.

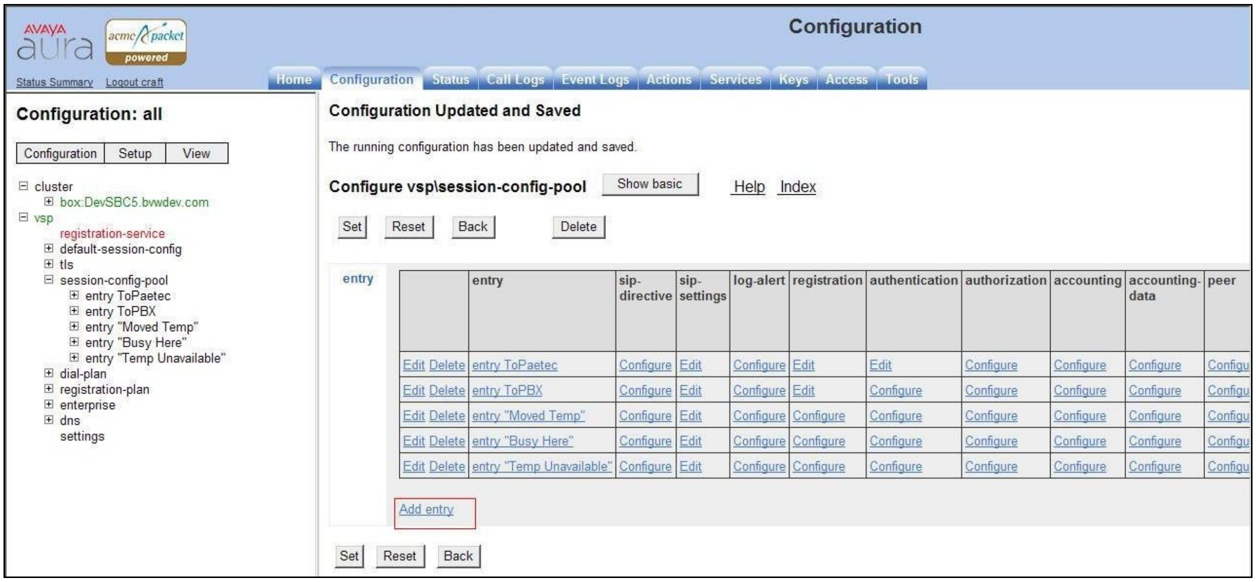


Figure 76: Link to add new session-config-pool entry

b) Define name for the new entry as **"Moved Temp"** then click **Create** as shown in **Figure 77**.

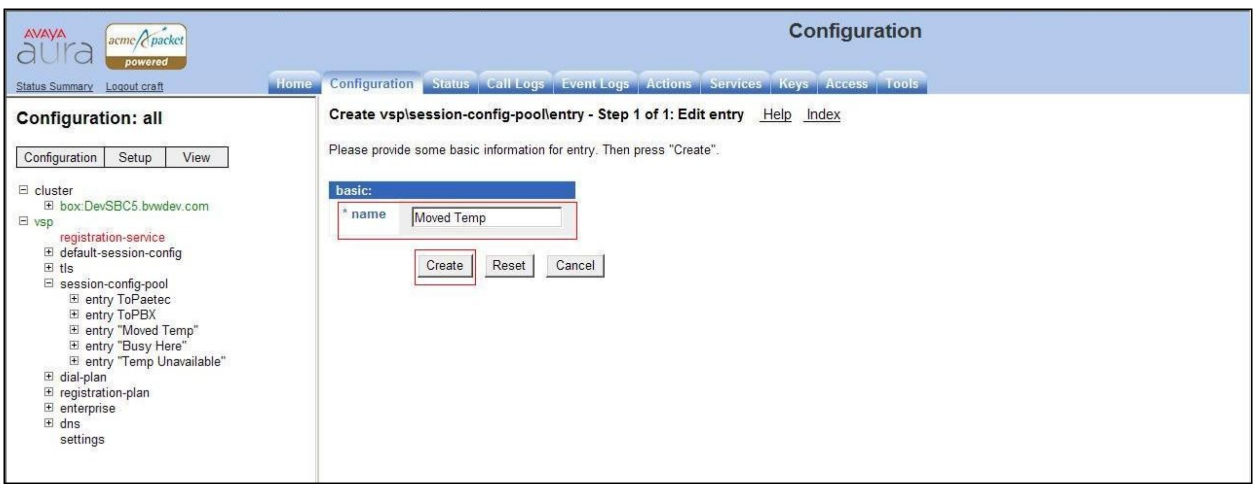


Figure 77: Create new session-config-pool entry named "Moved Temp"

c) Create basic configuration

- Refer to **Section 6.6.1** to administer sip-settings
- Refer to **Section 6.6.2** to manipulate From, To, Request-URI and P-Asserted-Identity headers
- Refer to **Section 6.6.3** to administer media
- Refer to **Section 6.6.4** to administer sip-session-timers
- Refer to **Section 6.6.5** to enable third-party-call-control

d) Create a regular expression rule associated to **session-config-pool "Moved Temp"**

To create a regular expression rule, select **Configuration vsp\session-config-pool\entry “Moved Temp”\header settings**. Click **Add reg-ex-header** link as shown in **Figure 78**.

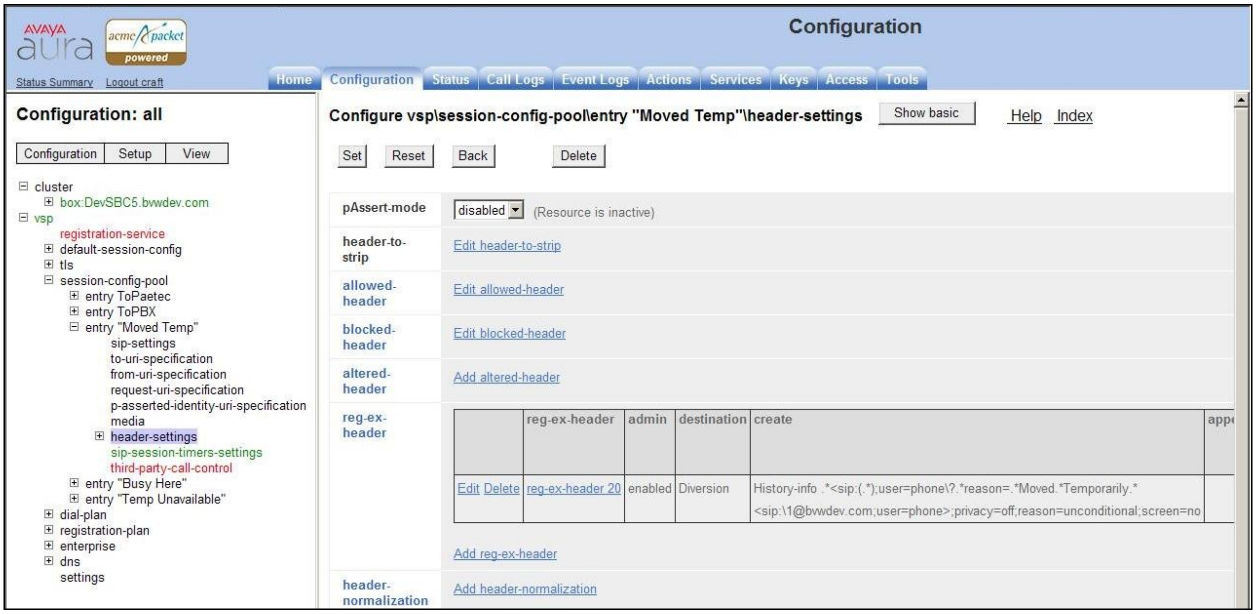


Figure 78: Link to add new regular expression rule

e) Define the rule ID and select destination as **Diversion** as show in **Figure 79**.

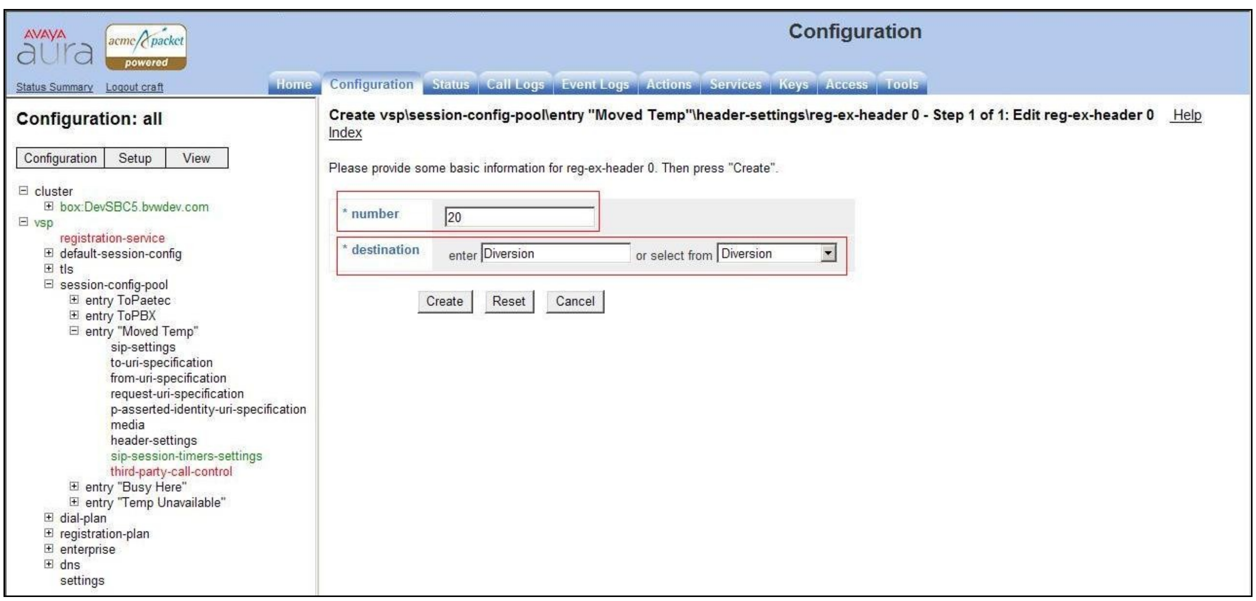


Figure 79: Define a new regular expression header

f) Define regular expression rule to convert History-Info to Diversion header for **Call Forward All Call** scenario

The regular expression rule will conditional match History-Info sent in SIP/INVITE from CS1000 for **Call Forward All Call** scenario. Then replace by a Diversion header with the appropriate reason code, in this case the reason code is **reason=unconditional**.

Figure 80 shows a rule has been defined with:

- Expression :**.*<sip:(.*)@.*;user=phone\?.*reason=.*Moved.*Temporarily.***
- Replacement:**<sip:\1@bvwdev.com;user=phone>;privacy=off;reason=unconditional;screen=no**

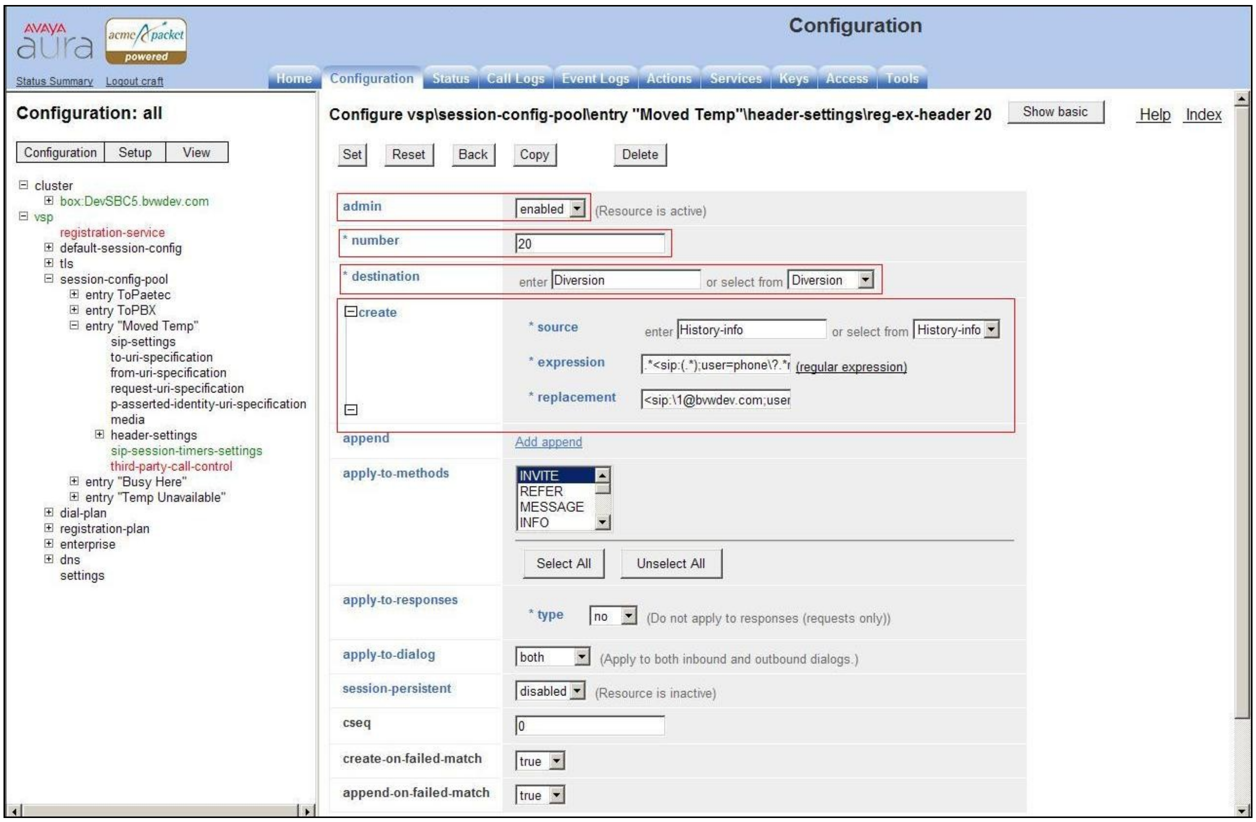


Figure 80: Regular expression rule to convert History-Info to Diversion header for Call Forward All Call scenario

6.8.2. Create entry dial-plan source-route “Moved Temp”

a) Create entry **dial-plan source-route “Moved Temp”**

Select **Configuration vsp\dial-plan**. Click **Add source-route** link as shown in **Figure 81**.

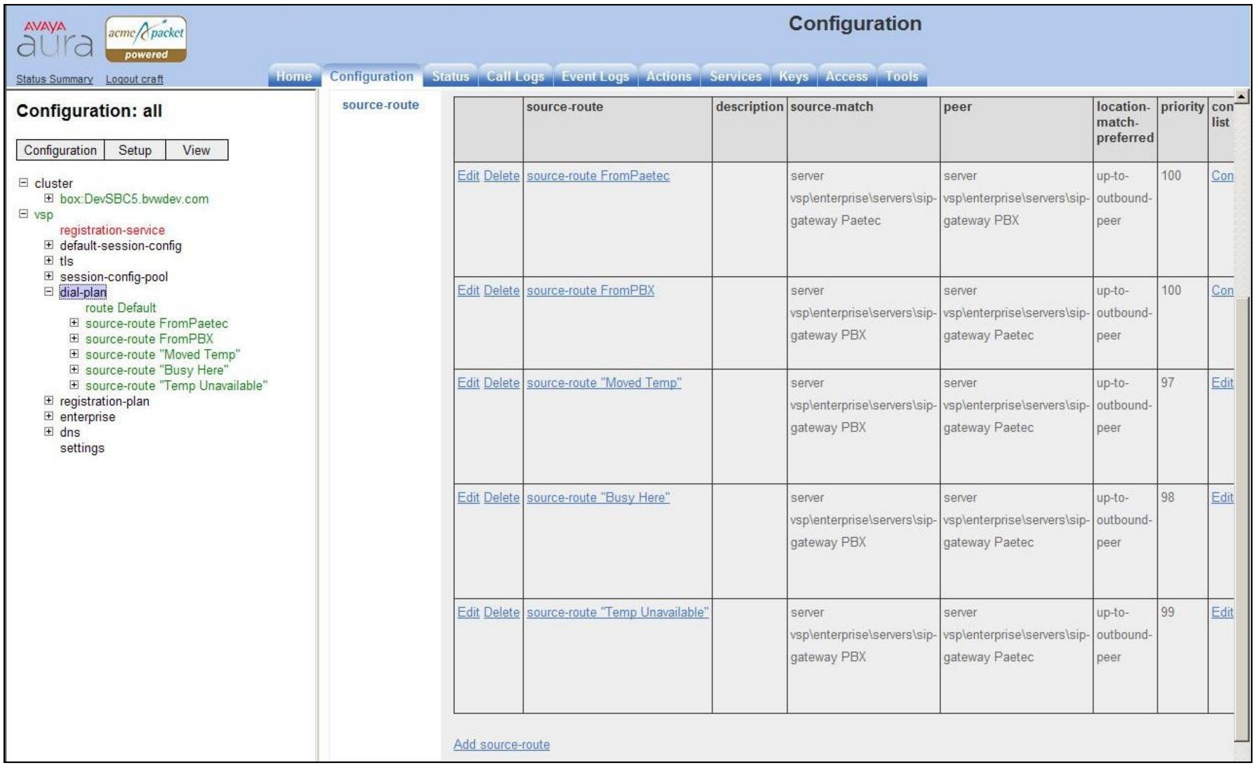


Figure 81: Link to add new source-route dial-plan

b) Define name for the new entry as **“Moved Temp”**, select **source-match type** as **server**; **source-server** as **vsp\enterprise\servers\sip-gateway- PBX** then click **Create** as shown in **Figure 82**.

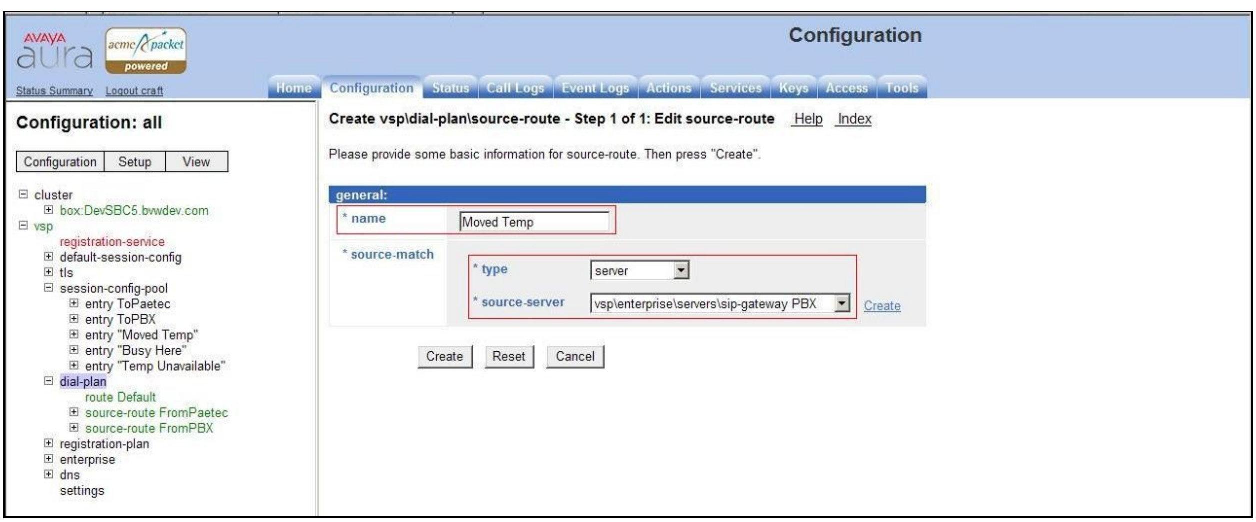


Figure 82: New source-route dial-plan “Moved Temp”

c) Configure the entry **source-route “Moved Temp”**

Refer to **Section 6.5.1** to configure the entry **source-route "Moved Temp" as shown in Figure 83, 84.**

- name: Moved Temp
- source-match type: server
- source-server: vsp\enterprise\servers\sip-gateway PBX
- peer type: server
- peer server: vsp\enterprise\servers\sip-gateway ToPaetec
- **priority: 97** which is higher than entry source-route FromPBX
- **condition-list-match-secondary**: **true**
- **session-config: vsp\session-config-pool\entry "Moved Temp"**

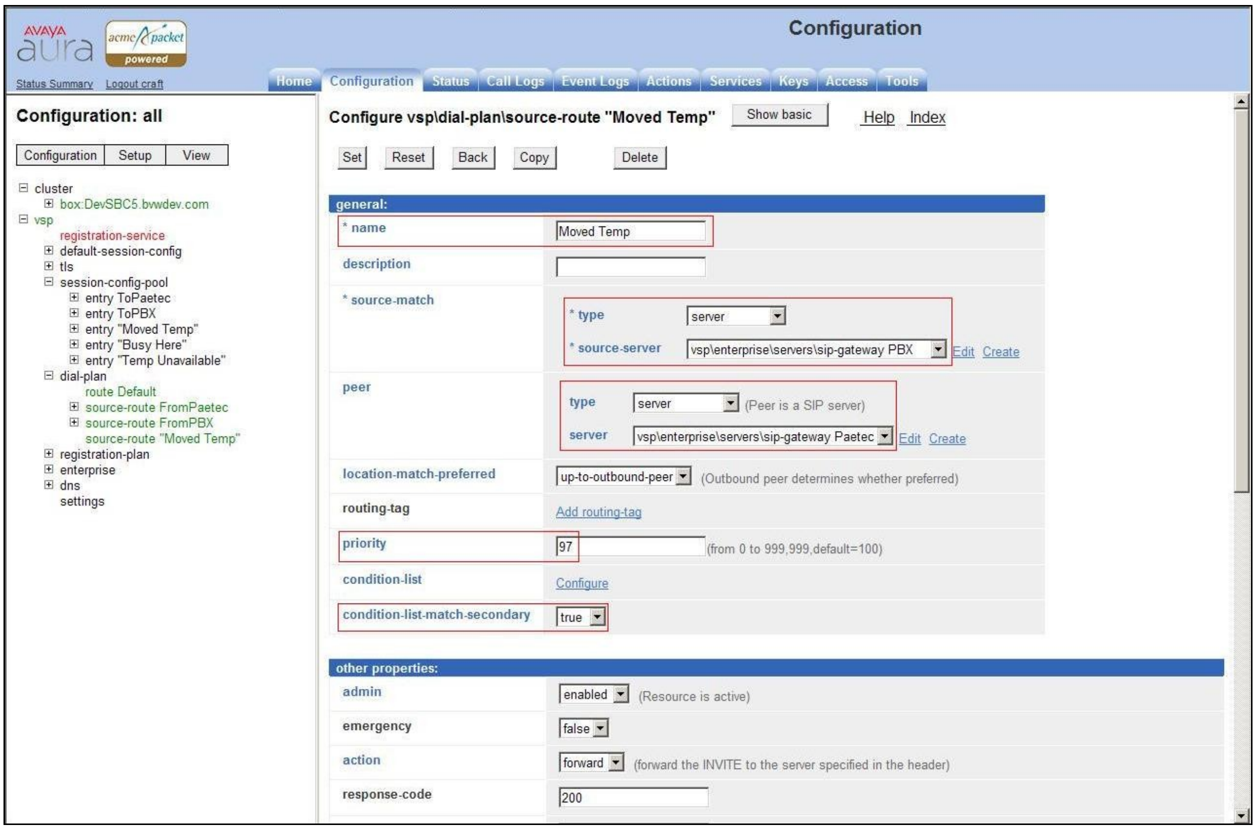


Figure 83: Entry source-route dial-plan "Moved Temp" detail – Page 1

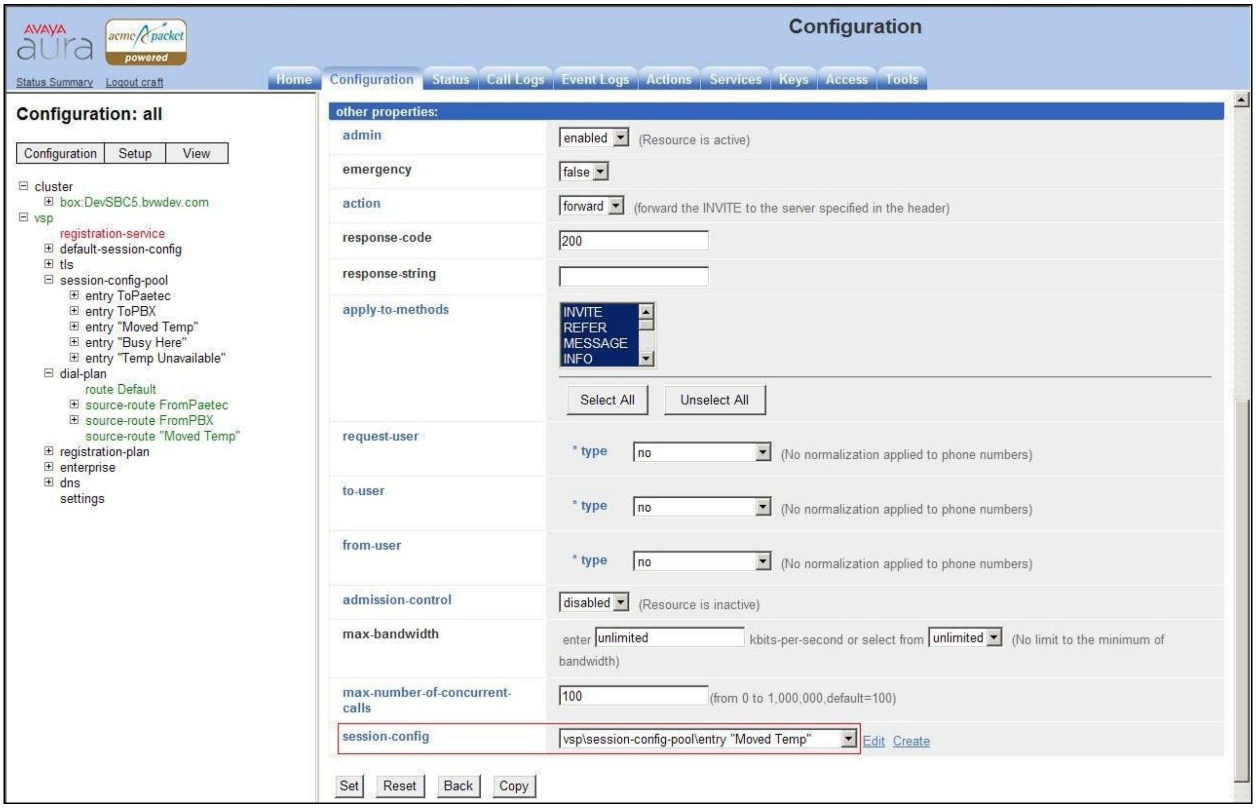


Figure 84: Entry source-route dial-plan "Moved Temp" detail – Page 2

d) Define **conditional-list**

The entry **source-route "Moved Temp"** will have a conditional matched rule and higher priority than the default source-route FromPBX. The DevSBC5 bases on the priority and condition checking to examine if it is a Call Forward All Call. If the condition matched, DevSBC5 will apply session-configure-pool "Moved Temp" to translate History-Info to Diversion header before sending out to PAETEC Communications system.

To create a conditional-list, select **Configuration vsp\dial-plan\source-route "Moved Temp"**\condition-list Click **Add sip-message-condition** link as shown in **Figure 85**.

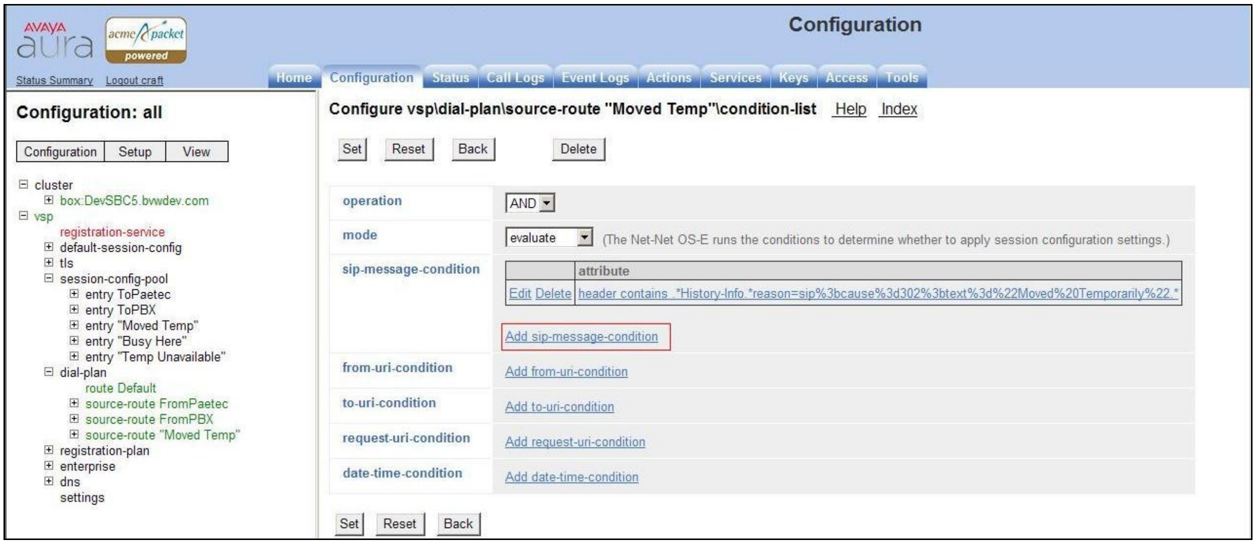


Figure 85: Link to Add sip-message-condition

CS1000 sends History-Info contains particular reason code of call forward. **Figure 86** shows a condition with regular expression rule to match Call Forward All Call scenario.

- **attribute**: header
- **match**: contains
- **value**: **.*History-info.*reason=sip%3bcause%3d302%3btext%3d%22Moved%20Temporarily%22.***

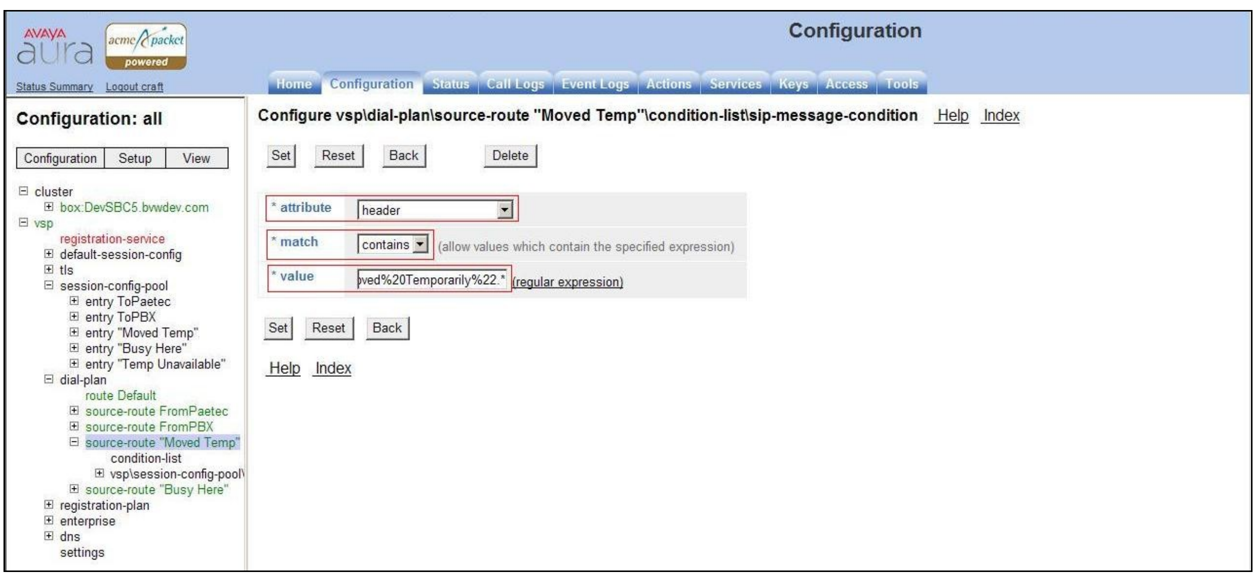


Figure 86: condition-list to match History-Info of Call Forward All Call scenario

6.9. Convert History-Info to Diversion header for Call Forward Busy Scenario

6.9.1. Create entry session-config-pool "Busy-Here"

Refer to **Session 6.8.1** to create entry **session-configure-pool "Busy-Here"**

The regular expression for Call Forward Busy will be different than Call Forward All Call. At step f), change the regular expression rule as show in **Figure 87** as follow.

- Expression :**.*<sip:(.*)@.*;user=phone\?.*reason=.*Busy.*Here.***
- Replacement: **<sip:\1@bvwdev.com;user=phone>;privacy=off;reason=user-busy;screen=no**

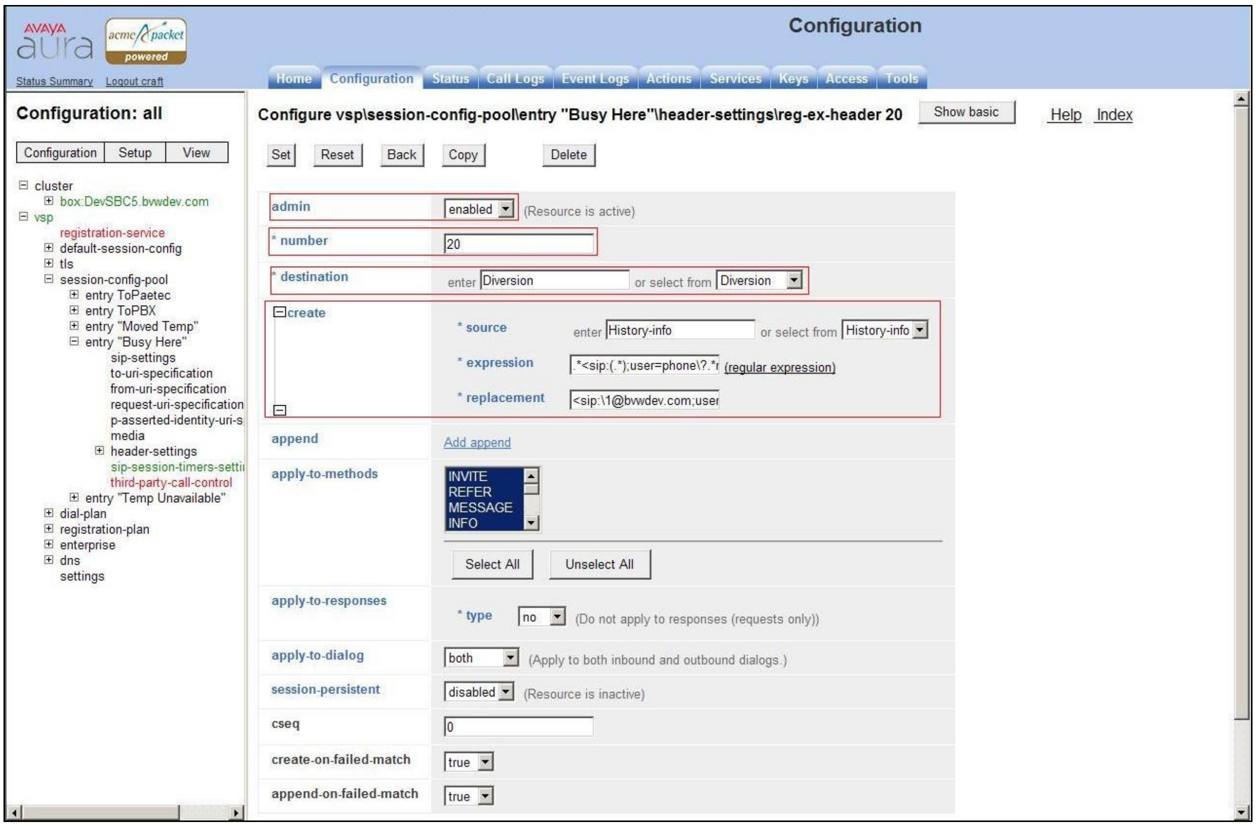


Figure 87: Regular expression rule to convert History-Info to Diversion header for Call Forward Busy scenario

6.9.2. Create entry source-route dial-plan "Busy-Here"

Refer to **Session 6.8.2** to create entry **source-route dial-plan "Busy-Here"** with:

- **priority 98**
- **session-config vsp\session-config-pool\entry "Busy-Here"**

The regular expression for Call Forward Busy will be different than Call Forward All Call. At step d), change the regular expression rule as show in **Figure 88** as follow.

- **attribute**: header
- **match**: contains
- **value**: **.*History-info.*reason=sip%3bcause%3d486%3btext%3d%22Busy%20Here%22.***

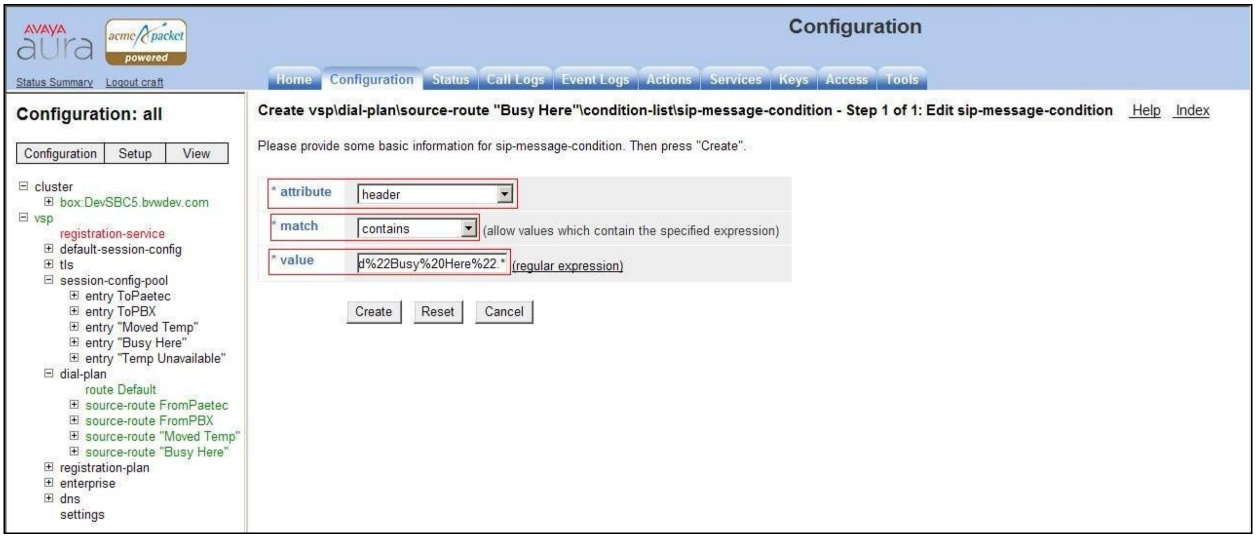


Figure 88: Condition-list to match History-Info of Call Forward Busy scenario

6.10. Convert History-Info to Diversion header for Call Forward No Answer Scenario

6.10.1. Create entry session-config-pool "Temp Unavailable"

Refer to **Session 6.8.1** to create entry **session-configure-pool "Temp Unavailable"**

The regular expression for Call Forward No Answer will be different than Call Forward All Call. At step f), change the regular expression rule as show in **Figure 89** as follow.

- Expression : ***<sip:(.*)@.*;user=phone\?.*reason=.*Temporarily.*Unavailable.***
- Replacement: **<sip:\1@bvwdev.com;user=phone>;privacy=off;reason=no-answer;screen=no**

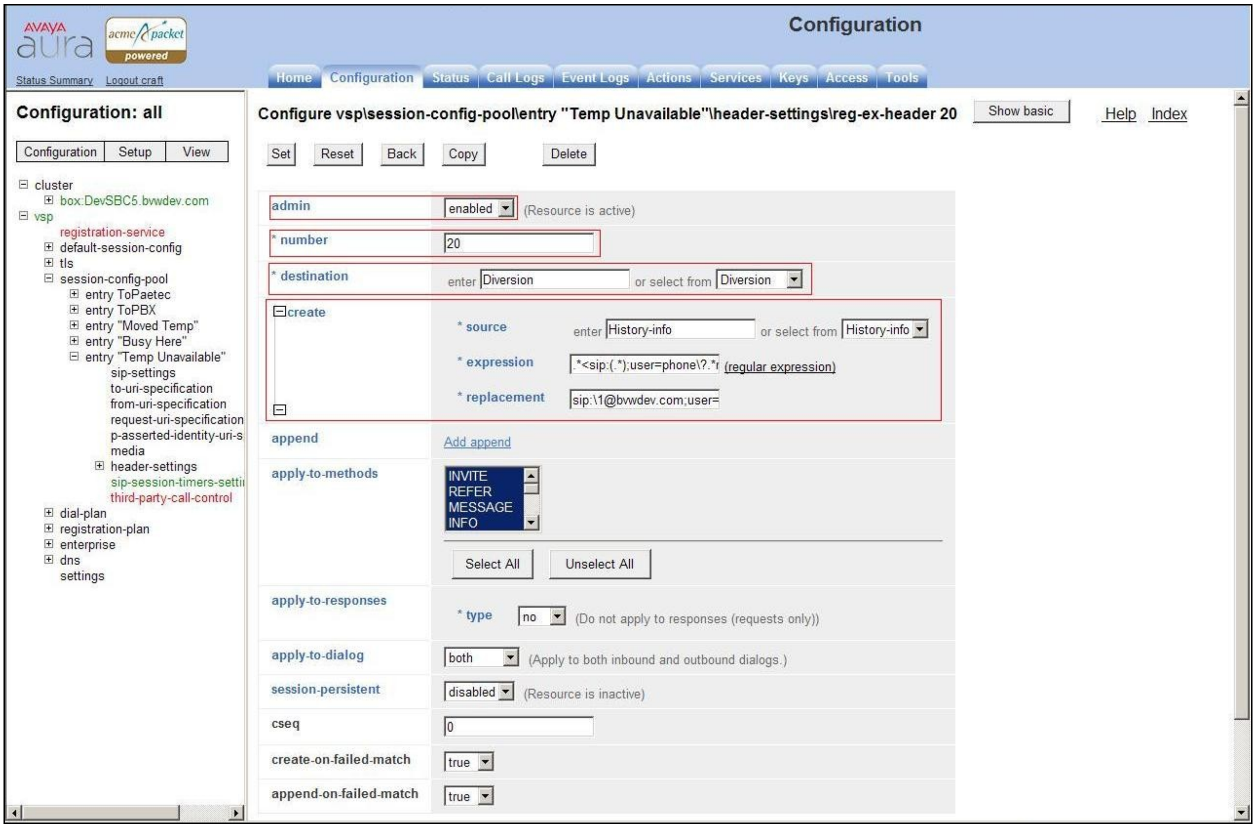


Figure 89: Regular expression rule to convert History-Info to Diversion header for Call Forward No Answer scenario

6.10.2. Create entry source-route dial-plan "Temp Unavailable"

Refer to **Session 6.8.2** to create entry **source-route dial-plan "Temp Unavaible"** with:

- **priority 99**
- **session-config vsp\session-config-pool\entry "Temp Unavailable"**

The regular expression for Call Forward No Answer will be different than Call Forward All Call. At step d), change the regular expression rule as show in **Figure 90** as follow.

- **attribute**: header
- **match**: contains
- **value**: **.*History-info.*reason=sip%3bcause%3d480%3btext%3d%22Temporarily%20Unavailable%22.***

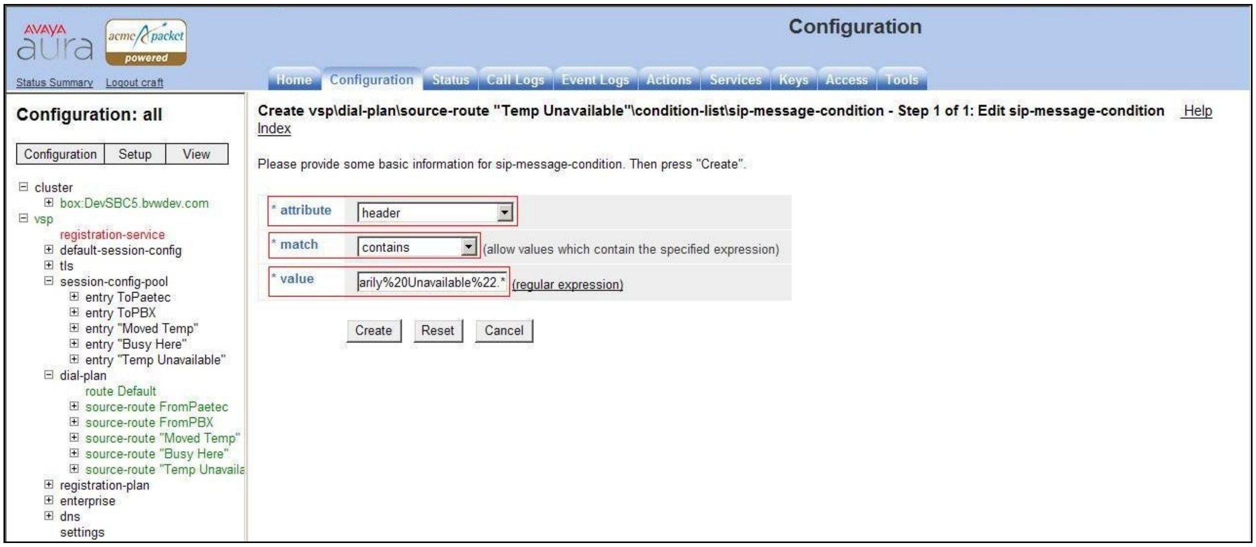


Figure 90: Condition-list to match History-Info of Call Forward No Answer scenario

6.11. Convert 183 with SDP to 180 without SDP for Ring-Back-Tone in Call Blind Transfer Scenario

The procedure to create a rule to convert SIP 183 with SDP to 180 without SDP on DevSBC5 is as below:

- Create an entry in “response-translation-settings” to convert SIP 183 with SDP to SIP 180 with SDP
- Enable “forking-early-media-inhibit” to prevent the SDP body from being sent in the 180 response.

6.11.1. Create an entry to convert SIP 183 with SDP to SIP 180 with SDP

1. Select **Configuration > vsp > session-config-pool > entry ToPaetec > response-translation-settings.** Then click **Add entry** as shown in **Figure 91.**
   - Input “status-code” as “183”
   - Input “new-status-code” as “180”
   - Click **Create** to save the configuration.

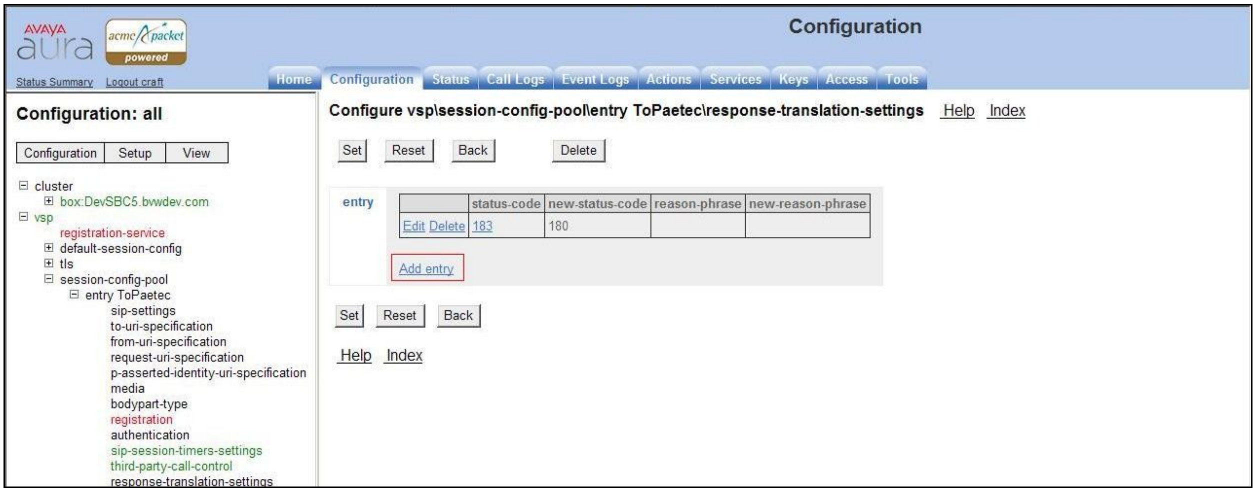


Figure 91: Create an entry to convert SIP 183 with SDP to SIP 180 with SDP

2. In order to edit the entry, select **Configuration > vsp > session-config-pool > entry ToPaetec > response-translation-settings.** Then click **Edit** as shown in **Figure 92**
   - Modify “reason-phrase” as “Session Progress”
   - Modify “new-reason-phrase” as “Ringing”
   - Click **Set** to save the configuration.
   -

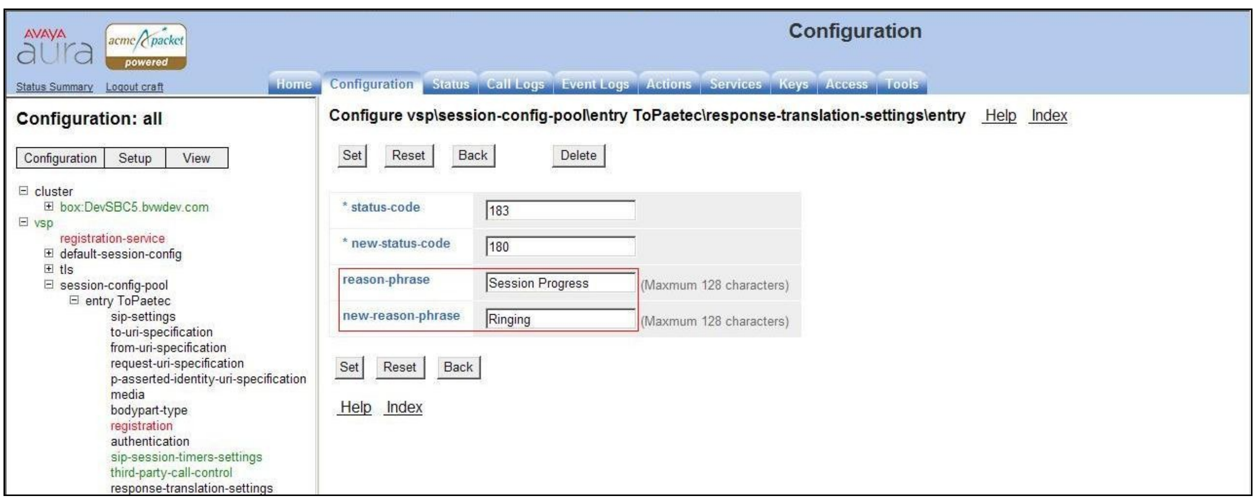


Figure 92: Edit entry to convert SIP 183 with SDP to SIP 180 with SDP

6.11.2. Enable third party-call-control and “forking-early-media-inhibit”

To enable the **third-party-call-control**, select **Configuration > vsp > session-config-pool > entry ToPaetec > third-party-call-control.** Then change the **admin** state to **Enabled** as shown in **Figure 93.**

To enable the **forking-early-media-inhibit,** select **Configuration > vsp > session-config-pool > entry ToPaetec > third-party-call-control.** Then change the **forking-early-media-inhibit** state to **Enabled** as shown in **Figure 93.**

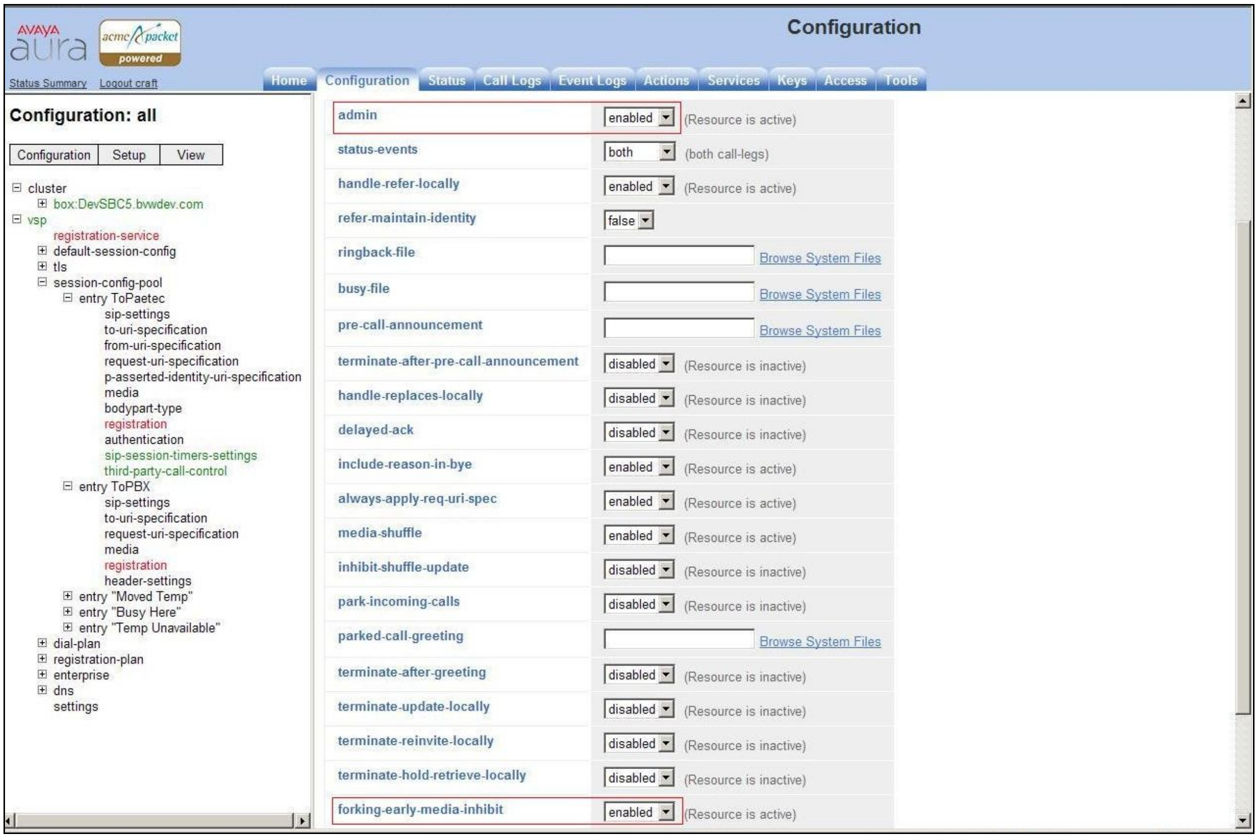


Figure 93: Enable the "forking-early-media-inhibit"

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 that the call remains stable for several minutes and disconnects properly.

7.2. Verification of 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 for which the call is in progress or idle. The call scenario involved PSTN phone number 6139675205 calling 7133433758.

- Login on to Signaling Server 10.10.97.177 with admin account and password.
- Issue a command "cslogin" to login on to the Call Server.
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trace 0 3758**.

- After the call is released, issue command **trac 0 3758** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when the 3758 is in call state:

```
>ld 80

.trac 0 3758

ACTIVE  VTN 096 0 00 02

ORIG   VTN 100 0 00 00   VTRK IPTI  RMBR  100 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 20.20.64.220
  FAR-END MEDIA ENDPOINT IP: 10.10.97.242  PORT: 24574
  FAR-END VendorID: Not available
TERM   VTN 096 0 00 02  KEY 0  SCR MARP  CUST 0  DN 3758  TYPE 2002P2
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.10.98.3  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 3758
MAIN_PM  ESTD
TALKSLOT  ORIG  20   TERM  25
EES_DATA:
NONE
QUEU  NONE
CALL ID 501 76


----  ISDN ISL CALL (ORIG) ----
CALL REF # =  484
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  16139675205  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  7133433758  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call on 3758 is finished.

```
.trac 0 3758
IDLE VTN 96 0 00 02   MARP
```

b) SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675205) to an internal device (7133433758). Then check the SIP trunk status by using LD 32, one trunk is BUSY

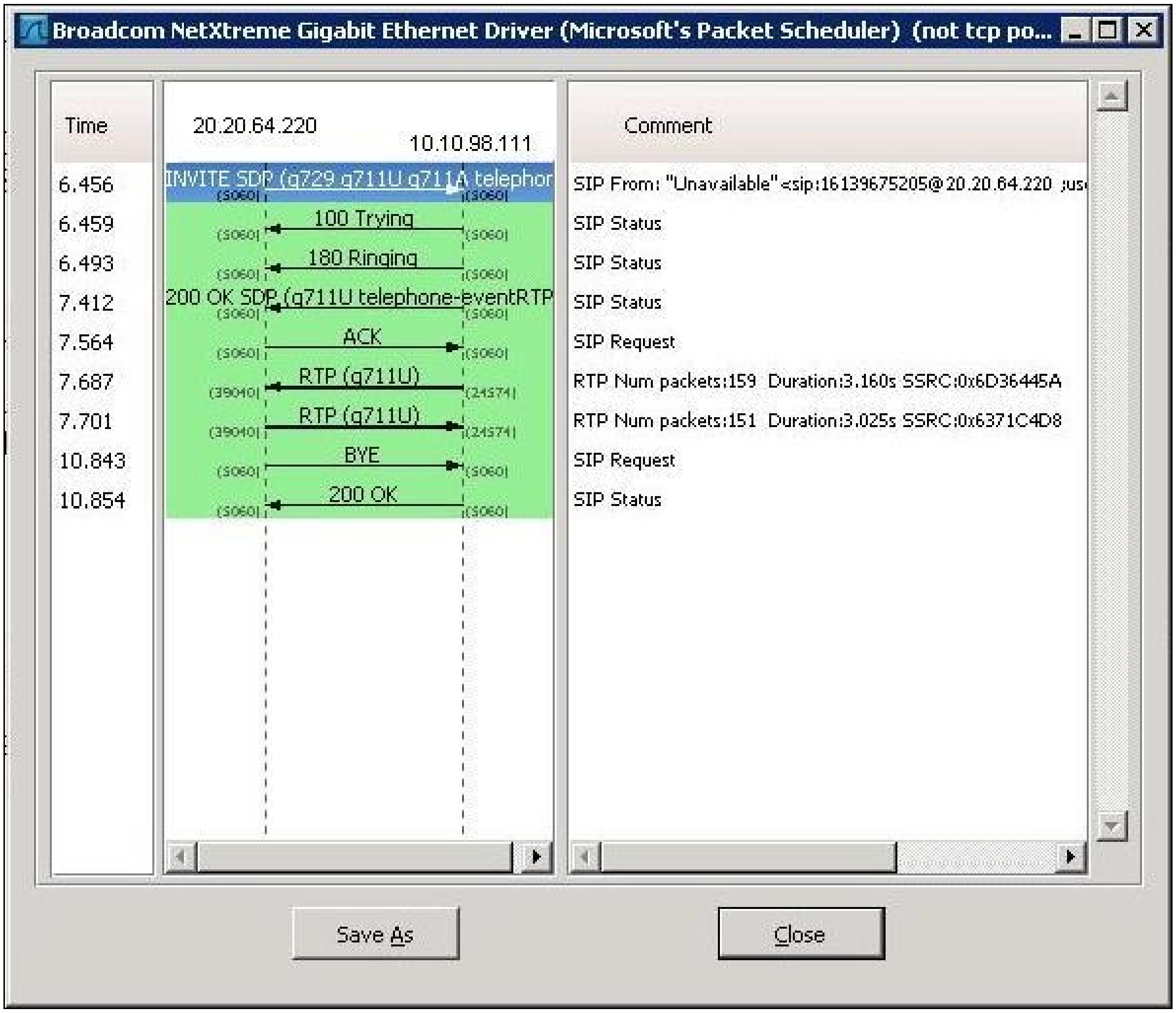
```
>ld 32
NPR000
.stat 100 0
091 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

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

```
.stat 100 0
092 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**. Note that only detail of the INVITE message is being shown here.



```
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: INVITE sip:7133433758@10.10.98.111:5060;transport=UDP SIP/2.0
      Method: INVITE
    ⊞ Request-URI: sip:7133433758@10.10.98.111:5060;transport=UDP
      [Resent Packet: False]
  ⊟ Message Header
      Via: SIP/2.0/UDP 20.20.64.220:5060;branch=z9hG4bKajd14b008o6121s3m180.1
    ⊟ From: "Unavailable"<sip:16139675205@20.20.64.220;user=phone;broadworks=BWWESTSIGIS-1ecpqqca1h9ba>;tag=244833123-13202597
        SIP Display info: "Unavailable"
      ⊞ SIP from address: sip:16139675205@20.20.64.220;user=phone;broadworks=BWWESTSIGIS-1ecpqqca1h9ba
        SIP tag: 244833123-1320259723119-
    ⊟ To: "CS1K 8"<sip:7133433758@10.10.98.111;interopis=interopis-h3bnp35pc3i58>
        SIP Display info: "CS1K 8"
      ⊞ SIP to address: sip:7133433758@10.10.98.111;interopis=interopis-h3bnp35pc3i58
      Call-ID: BW184843119021111827754577@20.20.51.199
    ⊟ CSeq: 852381624 INVITE
        Sequence Number: 852381624
        Method: INVITE
    ⊟ Contact: <sip:16139675205@20.20.64.220:5060;broadworks=BWWESTSIGIS-o6i7c69dv2579;transport=udp>
      ⊞ Contact-URI: sip:16139675205@20.20.64.220:5060;broadworks=BWWESTSIGIS-o6i7c69dv2579;transport=udp
        Contact parameter: broadworks=BWWESTSIGIS-o6i7c69dv2579
        Contact parameter: transport=udp>
      Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
      Accept: multipart/mixed,application/media_control+xml,application/sdp
      Supported: timer
      Min-SE: 60
      Max-Forwards: 47
      Content-Type: application/sdp
      Content-Length: 283
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): BroadWorks 206875 1 IN IP4 20.20.64.220
        Session Name (s): -
      ⊞ Connection Information (c): IN IP4 20.20.64.220
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 39040 RTP/AVP 18 0 8 101
```

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 **Section 2.1**. The PAETEC Communications system is considered **compliant** with Avaya Communication Server 1000 Release 7.5 and Avaya Aura® Session Border Controller Release 6.0.

9. Appendix

The ring-back-tone issue has been found on another PAETEC solution tested with One X Mobile Lite application on iPhone. In order to make sure this issue has not been observed on our solution testing, the below additional test cases were executed for this verification.

Call Scenario_01: Inbound call: PSTN1 ----call ----- CS1000 number (associated with a CS1000 desk phone paired with a 1xMobile LITE iPhone)

Result: PASSED

- Both CS1000 desk phone and iPhone (pop up on cell phone native function) rang.
- PSTN1 heard ring back tone. (Observed the 2nd leg, CS1000 sent out INVITE without SDP, and PAETEC responded 180 Ringing without SDP. As the result, PSTN1 could hear the ring back tone).
- The speech path was good after iPhone answered the call.

Call Scenario_02: Outbound call: 1xMobile LITE application on iPhone -----call--- - PSTN1 thru CS1000 DISA number

Result: PASSED.

- iPhone acted in two stage dialing:
  + Dialed DISA number and waited for dial tone.
  + Dialed the destination as PSTN1 number.
- iPhone heard ring back tone.
- There was speech path after PSTN1 answered the call.

Call Scenario_03: PSTN_1 ----call ---> DISA CS1000 number --- call----> PSTN_2

Result: PASSED

1) PSTN_1 dialed CS1000 DISA number over SIP Trunk.
2) PSTN_1 entered access code then heard dial tone.
3) PSTN_1 entered PSTN_2 number to use DISA feature to out dialing to PSTN_2 over SIP Trunk.
4) PSTN_1 received the ring back tone.
5) PSTN_1 talked to PSTN_2 with 2-way speech path after PSTN2 answered the call.

Call Scenario_04: Inbound call: PSTN1 ----call ----- CS1000 number (associated with a CS1000 desk phone paired with a Mobile X - cell phone number)

Result: PASSED

- Both CS1000 desk phone and cell phone rang.
- PSTN1 heard ring back tone. (Observed the 2nd leg, CS1000 sent out INVITE without SDP, and PAETEC responded 180 Ringing without SDP. As the result, PSTN1 could hear the ring back tone).
- The speech path was good after cell phone answered the call.

10. Additional References

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

[1] *Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.*

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010*

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011*

[4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011*

[5] *Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010*

[6] *Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011*

[7] *Installing and Configuring Avaya Aura® Session Border Controller System Administration Guide, Release 6.0.3, Document Number 100147622, Aug 2011*

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.