



## **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

<b>Table of Contents</b> .....	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 “ <i>forking-early-media-inhibit</i> ” .....	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>

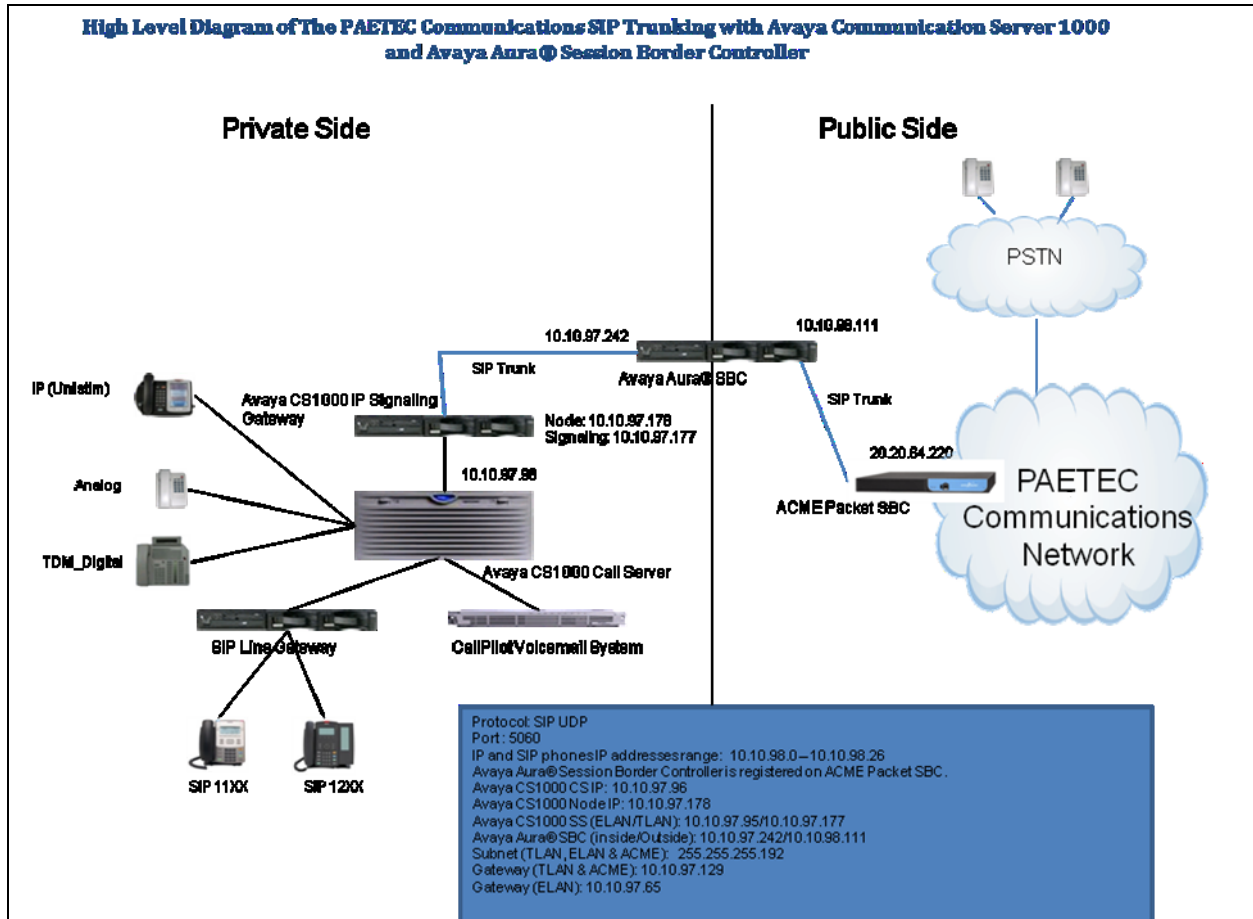
For technical support on PAETEC Commnucations system, please contact PAETEC Communications technical support at:

- 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)	<ul style="list-style-type: none"><li>● Call Server: 750 Q+ GA</li><li>● Signaling Server: 7.50.17 GA</li><li>● SIP Line Server: 7.50.17 GA</li></ul>
Avaya Aura® Session Border Controller	<ul style="list-style-type: none"><li>● SBCT 6.0.2.0.3 (sbc E362P4)</li></ul>
Avaya phones	<ul style="list-style-type: none"><li>● 2002 p2: 0604DCN (Unistim)</li><li>● 1140: 0625C8D (Unistim)</li><li>● 1120: 0624C8D (Unistim)</li><li>● 2007: 0621C8D (Unistim)</li><li>● 1120: 4 1 13 0 (SIPLine)</li><li>● 12xx: 4 1 13 0 (SIPLine)</li></ul>

### PAETEC Communications system:

System	Software/Loadware version
Acme Packet Net-Net 4250 Session Border Controller	<ul style="list-style-type: none"><li>● Firmware SC6.2.0 Patch 3 (Build 497) Build Date=02/12/10</li></ul>
Broadsoft	<ul style="list-style-type: none"><li>● Version 14.sp9</li></ul>
LCS Gateway	<ul style="list-style-type: none"><li>● Version 3.14.4.7</li></ul>

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

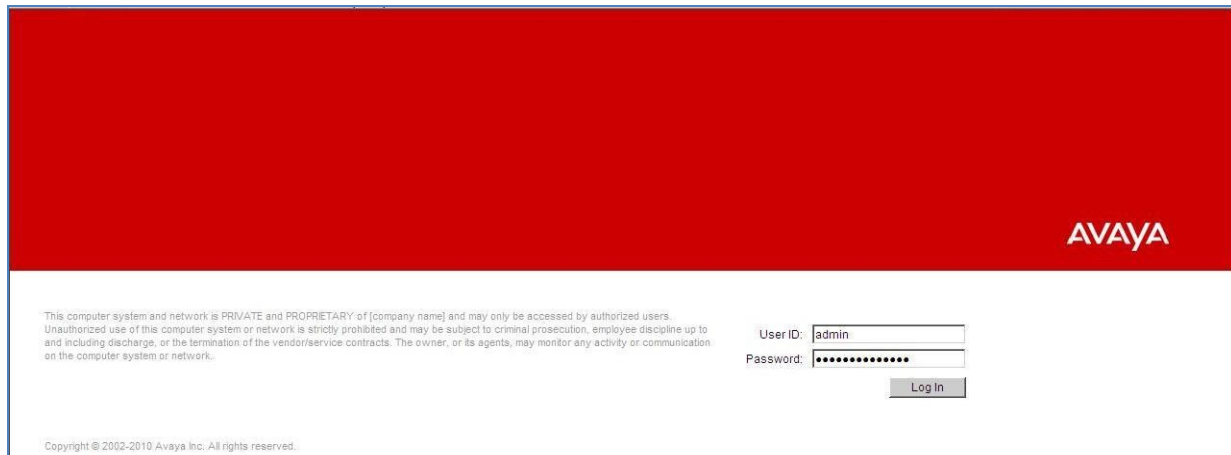
These Application Notes used the Incoming Digit Translation feature to receive the calls and used the Numbering Plan Area Code (NPA), Special Number (SPN) features to route calls from the Avaya Communication Server 1000, over the PAETEC Communications SIP trunk to PSTN. These application notes assume 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)

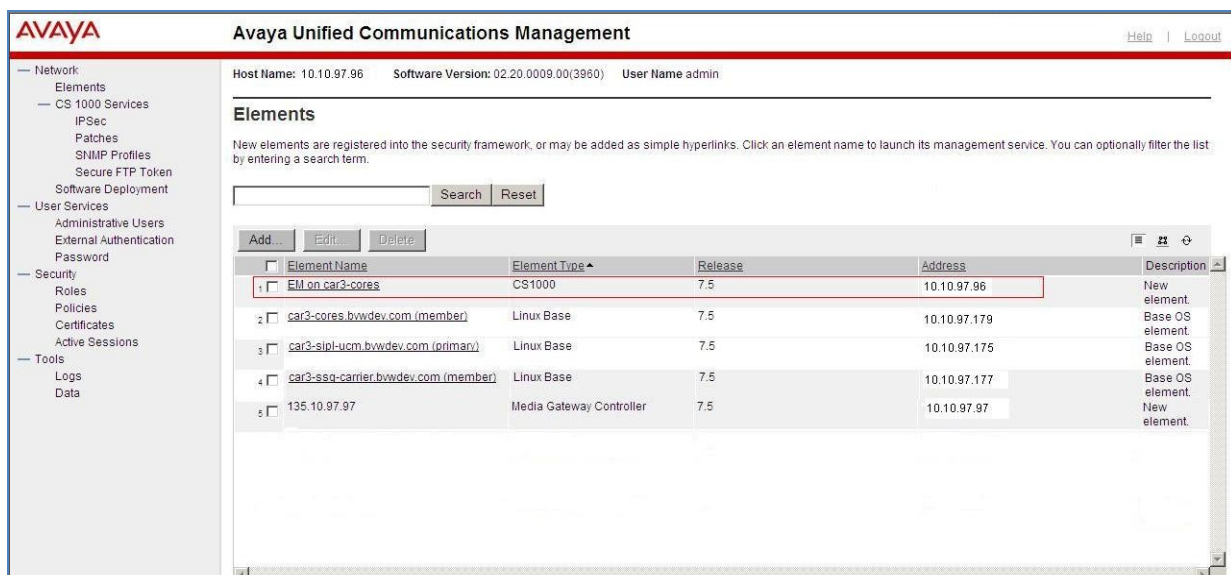
a) Open an instance of a web browser and connect to the UCM GUI at the following address: <http://<node IP address>> or <http://<UCM IP address>>. Log in using an appropriate User ID and Password.



The login screen features a red header with the AVAYA logo. Below the header is a disclaimer: "This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network." To the right of the disclaimer are input fields for "User ID:" (containing "admin") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. At the bottom left, the copyright notice "Copyright © 2002-2010 Avaya Inc. All rights reserved." is displayed.

**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**.



The interface shows the "Avaya Unified Communications Management" dashboard. The top navigation bar includes the AVAYA logo, the title "Avaya Unified Communications Management", and links for "Help" and "Logout". A sidebar on the left lists various system components like Network, Elements, CS 1000 Services, IPsec, Patches, SNMP Profiles, Secure FTP Token, Software Deployment, User Services, Administrative Users, External Authentication, Password, Security, Roles, Policies, Certificates, Active Sessions, Tools, Logs, and Data. The main content area displays "Host Name: 10.10.97.96", "Software Version: 02.20.0009.00(3960)", and "User Name admin". Below this is the "Elements" section, which includes a search bar and a table of registered elements. The first element, "EM on car3-cores", is highlighted with a red box.

Element Name	Element Type	Release	Address	Description
1 <b>EM on car3-cores</b>	CS1000	7.5	10.10.97.96	New element.
2 car3-cores.bvwdev.com (member)	Linux Base	7.5	10.10.97.179	Base OS element.
3 car3-slp-ucm.bvwdev.com (primary)	Linux Base	7.5	10.10.97.175	Base OS element.
4 car3-ssq-carrier.bvwdev.com (member)	Linux Base	7.5	10.10.97.177	Base OS element.
5 135.10.97.97	Media Gateway Controller	7.5	10.10.97.97	New element.

**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)

- Use Putty, SSH to connect to IP address of SSG Server with the admin account.
- Run the command “cslogin” and log in with the appropriate admin account and password.
- 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**.



Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IP v4	Node/TLAN IP v6	Status
3000	1	LTPS, Gateway ( SIPGw )	-	10.10.97.178		Synchronized
3002	1	SIP Line, LTPS	-	10.10.97.176		Synchronized

**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.



AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (NAT)

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Managing: 10.10.97.96 Username: admin

System > IP Network > IP Telephony Nodes > Node Details

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

Node ID: 3000 \* (0-9999)

Call server IP address: 10.10.97.96

TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 10.10.97.65

Node IPv4 address: 10.10.97.178

Subnet mask: 255.255.255.192

Subnet mask: 255.255.255.192

Node IPv6 address:

\* Required Value.

Save

Cancel

Associated Signaling Servers & Cards

Select to add

Add

Remove

Make Leader

Print | Refresh

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

Show: ☐ IPv6 address

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

Figure 6 –Node Details

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (NAT)

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Managing: 10.10.97.96 Username: admin

System > IP Network > IP Telephony Nodes > Node Details

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

Subnet mask: 255.255.255.192

Subnet mask: 255.255.255.192

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Coders
- Quality of Service (QoS)
- L3H
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

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

\* Required Value.

Save

Cancel

Associated Signaling Servers & Cards

Select to add

Add

Remove

Make Leader

Print | Refresh

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

Show: ☐ IPv6 address

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

Figure 7 –Node Details

## 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 **UNISlim Line Terminal Proxy Server** check box and then click the **Save** button as shown in **Figure 8**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The top status bar shows the managing IP address (10.10.97.96), username (admin), and navigation links (Help, Logout). The left-hand navigation menu lists various system components, with 'Nodes, Servers, Media Cards' selected. The main configuration area is titled 'Node ID: 3000 - UNISlim Line Terminal Proxy Server (LTPS) Configuration Details'. It features three tabs: 'Firmware', 'DTLS', and 'Network Connect Server'. The 'Firmware' tab is active, showing the 'UNISlim Line Terminal Proxy Server' section with a checked checkbox for 'Enable proxy service on this node'. Below this, the 'Firmware' section contains fields for 'IP address' (0.0.0.0), 'Full file path' (download/firmwa), 'Server Account/User ID', and 'Password'. The 'DTLS' section shows a 'DTLS policy' dropdown set to 'Off' and two options: 'Client authentication' and 'Periodic re-keying'. The 'Network Connect Server' section is currently empty. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' The 'Save' and 'Cancel' buttons are located at the bottom right.

**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.

The screenshot shows the 'CS1000 Element Manager' interface. The top navigation bar includes the Avaya logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. The main content area is titled 'Node ID: 3000 - Quality of Service (QoS)'. On the left is a sidebar menu with categories like 'UCM Network Services', 'System', 'Interfaces', 'Customers', and 'Dialing and Numbering Plans'. The 'System' category is expanded, showing sub-items like 'Alarms', 'Maintenance', 'Core Equipment', 'Peripheral Equipment', 'IP Network', 'Nodes, Servers, Media Cards', 'Media Gateways', 'Zones', 'Host and Route Tables', 'Network Address Translation (NAT)', 'QoS Thresholds', 'Personal Directories', and 'Unicode Name Directory'. The 'QoS Thresholds' item is selected. The main configuration area is titled 'Diffserv Codepoint (DSCP)' and contains the following settings: 'Enable Avaya automatic QoS' (unchecked), 'Control packets' (40, range 0-63), 'Voice packets' (40, range 0-63), 'VLAN tagging' (unchecked, with '802.1Q support' text), and '802.1Q bits value (802.1P)' (6, range 0-7). At the bottom, there is a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' and two buttons: 'Save' and 'Cancel'.

**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.

- 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).
- On the **Node Details** page as shown in **Figure 7**, click on **Voice Gateway (VGW) and Codec**.
- The PAETEC Communications system supports **G.729/ptime 20ms** and **G.711/ptime 20ms** with **VAD disabled**. Then click on the **Save** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and Interfaces. The main content area is titled 'Node ID: 3000 - Voice Gateway (VGW) and Codes'. It has tabs for 'General', 'Voice Codes', and 'Fax'. The 'Voice Codes' tab is active, showing a list of voice codecs. Codec G711 is checked and labeled 'Enabled (required)'. Its settings include a 'Voice payload size' of 20 (milliseconds per frame) and a 'Voice payout (jitter buffer) delay' with a nominal value of 40 and a maximum value of 80 (milliseconds). A note below these settings states: 'Maximum delay may be automatically adjusted based on nominal settings.' There is an unchecked checkbox for 'Voice Activity Detection (VAD)'. Codec G722 is unchecked and labeled 'Enabled'. Its settings are similar to G711, with a payload size of 20 and a jitter buffer delay of 40-80 ms. Codec G729 is checked and labeled 'Enabled', with a payload size of 20. At the bottom, there is a note: '\* Required Value.' and another note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

**Figure 10 – Voice Gateway and Codec Configuration Details**

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

### 5.3.2. Enable Voice Codec on Media Gateways.

- From the left menu of the Element Manager page in **Figure 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.
- 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**

- 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**.

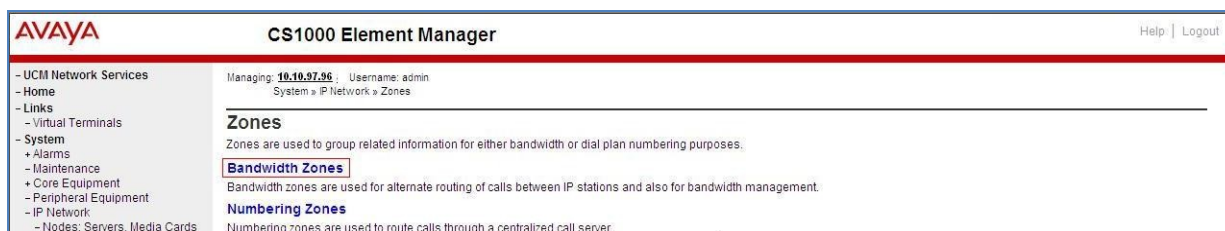


Figure 12 – Zones Page

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

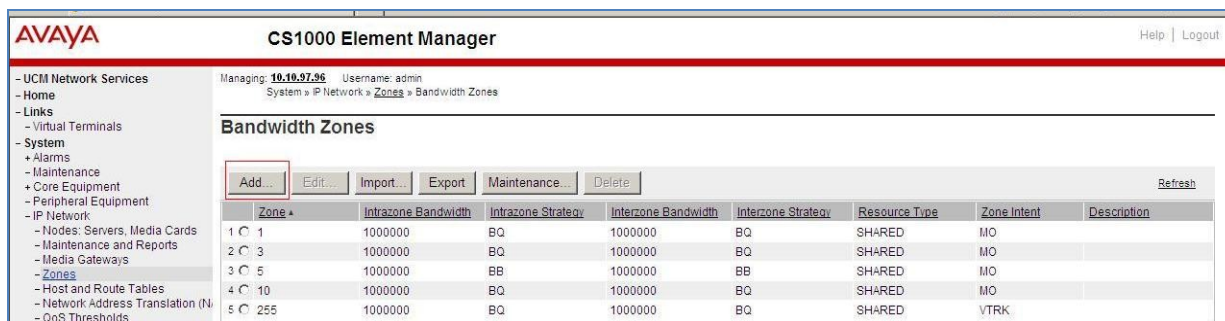


Figure 13 – Bandwidth Zones



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.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.96 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Submit Refresh Cancel

**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.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.96 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

Submit Refresh Cancel

**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)

- 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.
- 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

- 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**.
- On the **Node Details** screen, select **SIP Gateway (SIPGw)**.
- 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.

The screenshot displays the Avaya CS1000 Element Manager interface. The left sidebar shows a navigation tree with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, Routes and Trunks, D-Channels, Digital Trunk Interface, and Dialing and Numbering Plans. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. It features a 'General' tab and a 'Virtual Trunk Network Health Monitor' section. The 'General' tab contains the following fields: 'Vtrk gateway application' (SIP Gateway (SIPGw)), 'SIP domain name' (bwdev.com), 'Local SIP port' (5060), 'Gateway endpoint name' (car3-ssg-carrier), 'Gateway password', 'Application node ID' (3000), and 'Enable failsafe NRS' (unchecked). The 'Virtual Trunk Network Health Monitor' section includes a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor addresses' with 'Add' and 'Remove' buttons. The interface also shows a status bar at the bottom with 'Managing: 10.10.97.96 Username: admin' and a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

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.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin

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

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.10.97.242  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration  
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

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

**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.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.96 Username: admin

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

**Node ID: 3000 - Virtual Trunk Gateway Configuration Details**

**SIP URI Map:**

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: <input type="text"/>	CDP: <input type="text"/>
Special number: <input type="text"/>	Special number: <input type="text"/>
Unknown: <input type="text"/>	Vacant number: <input type="text"/>
	Unknown: <input type="text"/>

**SIP Gateway Services**

SIP Converged Desktop: ☒ Enable CD service

Service DN:  Used for making VTRK call from agent.

Converged telephone call forward DN:

RAN route for announce:  (route number 0 - 511)

Wait time before RAN queue:  (-1 - 32767 msec)

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

**Save** **Cancel**

**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.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.96 Username: admin

Routes and Trunks > D-Channels

**D-Channels**

**Maintenance**

- [D-Channel Diagnostics \(LD 98\)](#)
- [Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)
- [ISDL Diagnostics \(LD 98\)](#)
- [TMDI Diagnostics \(LD 98\)](#)
- [D-Channel Expansion Diagnostics \(LD 48\)](#)

**Configuration**

Choose a D-Channel Number:  and type:  **to Add**

Channel	Type	Card Type	Description	Edit
Channel: 11	Type: DCH	Card Type: DCIP	Description: sip1	<b>Edit</b>
Channel: 100	Type: DCH	Card Type: DCIP	Description: VoIP	<b>Edit</b>

**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.

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

**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**.

AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
    - Nodes: Servers, Media Cards
    - Maintenance and Reports
    - Media Gateways
    - Zones
    - Host and Route Tables
    - Network Address Translation (NAT)
    - QoS Thresholds
    - Personal Directories
    - Unicode Name Directory
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
    - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - Date and Time
  - + Logs and reports
- Security
  - + Passwords
  - + Policies
  - + Login Options

Action Device And Number (ADAN): DCH

D channel Card Type: DCIP

Designator: VoIP

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (ISLD)

Interface type for D-channel: Meridian Meridian 1 (SL1)

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRI loop number:

Primary Rate Interface: [more PRI](#)

Secondary PRI2 loops:

Meridian 1 node type: Slave to the controller (USR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 1800 Range: 0 - 3700

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive, (1)

- Remote Capabilities: [Edit](#)

- B channel Service messaging: ☐

- Basic options (BSCOPT)

+ - Change protocol timer value (TIMR)

+ Advanced options (ADVOPT)

+ Feature Packages

Submit

Refresh

Delete

Cancel

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

Figure 22 – D-Channel Configuration Details



Managing: **10.10.97.96** Username: admin  
Routes and Trunks > D-Channels > D-Channels 100 Property Configuration > - Remote Capabilities Configuration

### - Remote Capabilities Configuration

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

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

**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.

Managing: **10.10.97.96** Username: admin  
System > Core Equipment > Superloops

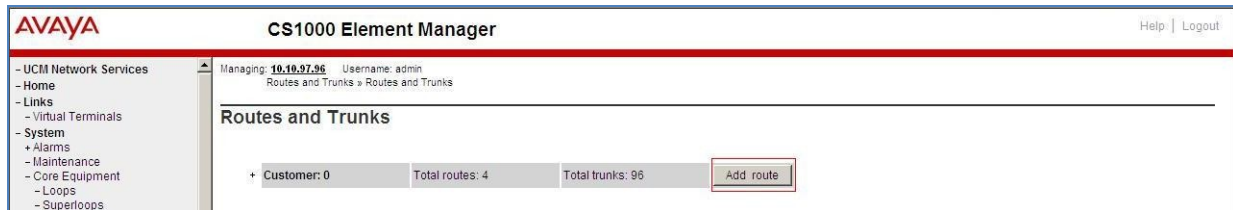
### Superloops

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

**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.
  - o **Mode of operation (MODE)**: Route uses ISDN Signalling Link (ISLD)
  - o **D channel number (DCH)**: D-Channel number 100 (created in **Section 5.5.3**)
  - o **Network calling name allowed (NCNA)**: Check the field.
  - o **Network call redirection (NCRD)**: Check the field.
  - o **Insert ESN access code (INAC)**: Check the field.

**AVAYA** **CS1000 Element Manager** Help | Logout

---

Managing: **10.10.97.95** Username: admin  
 Routes and Trunks » Routes and Trunks » Customer 0, Route 100 Property Configuration

### Customer 0, Route 100 Property Configuration

**- Basic Configuration**

Route data block (RDB) (TYPE):	RDB
Customer number (CUST):	00
Route number (ROUT):	100
Designator field for trunk (DES):	100
Trunk type (TKTP):	TIE
Incoming and outgoing trunk (ICOG):	Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD):	8100
Trunk type M911P (M911P):	<input type="checkbox"/>

The route is for a virtual trunk route (VTRK): <input checked="" type="checkbox"/>	
- Zone for codec selection and bandwidth management (ZONE):	00255 (0 - 8000)
- Node ID of signaling server of this route (NODE):	3000 (0 - 9999)
- Protocol ID for the route (PCID):	SIP (SIP)
- Print correlation ID in CDR for the route (CRID):	<input type="checkbox"/>

Integrated services digital network option (ISDN): <input checked="" type="checkbox"/>	
- Mode of operation (MODE):	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH):	100 (0 - 254)
- Interface type for route (IFC):	Meridian M1 (SL1)
- Private network identifier (PNI):	00001 (0 - 32700)
- Network calling name allowed (NCNA):	<input checked="" type="checkbox"/>
- Network call redirection (NCRD):	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO):	<input type="checkbox"/>
- Recognition of DTI2 ABCD FALT signal for ISL (FALT):	<input type="checkbox"/>
- Channel type (CHTY):	B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP):	Unknown Call type (UKWN)
- Insert ESN access code (INAC):	<input checked="" type="checkbox"/>

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

**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**.



AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - Core Equipment
    - Loops
    - Superloops
    - MSDLMISP Cards
    - Conference/TDS/Multifrequen
    - Tone Senders and Detectors
  - Peripheral Equipment
  - IP Network
    - Nodes: Servers, Media Cards
    - Maintenance and Reports
    - Media Gateways
    - Zones
    - Host and Route Tables
    - Network Address Translation
    - QoS Thresholds
    - Personal Directories
    - Unicode Name Directory
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
    - Digital Trunk Interface
  - Dialing and Numbering Plans
    - Electronic Switched Network
    - Flexible Code Restriction
    - Incoming Digit Translation
  - Phones
    - Templates
    - Reports
    - Views
    - Lists
    - Properties
    - Migration
  - Tools
    - + Backup and Restore
    - Date and Time
    - + Logs and reports
  - Security
    - + Passwords
    - + Policies

- Mobile extension timer (MBXT): 0 (0 - 8000 milliseconds)

Calling number dialing plan (CNDP): Unknown (UKWN)

- Basic Route Options

Attendant announcement (ATAI): No Attendant Announcement (NO)

Billing number required (BILN):

Call detail recording (CDR):

- CDR records generated on incoming calls (INC):

- CDR record printing content option for redirected calls (LAST):

- Time to answer output in CDR (TTA):

- CDR ACD Q initial connection records to be generated (QREC):

- CDR on outgoing calls (OAL):

- CDR on outgoing toll calls (OTL):

- Answered call identification allowed (AIA):

- CDR timing starts on answer supervision of outgoing calls (OAN):

- outpulsed digits in CDR (OPD):

- Number of digits printed (NDP): EXC 0

North American toll scheme (NATL):

Controls or timers (CNTL):

Conventional (Tie trunk only) (CNVT):

Incoming DID digit conversion on this route (IDC):

- Day IDC tree number (DCNO): 1 (0 - 254)

- Night IDC tree number (NDNO): 1 (0 - 254)

- Display external dialed digits (DEXT):

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

Process notification networked calls (PNNC):

+ Network Options

+ General Options

+ Advanced Configurations

Submit

Refresh

Delete

Cancel

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

**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** -> **00** -> **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**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Edit Calling Line Identification 0'. It contains three sections: 'General Properties' with fields for National Code (713), Local Code (343), Home Location Code (713343), and Local Steering Code (713343); 'Emergency Services Access' with an Emergency Local Code field and Emergency Options; and 'Calling Party Name Display' with fields for Roman characters, CPND Name, Expected Length, and Display Format. At the bottom right, there are 'Save' and 'Cancel' buttons.

**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
```



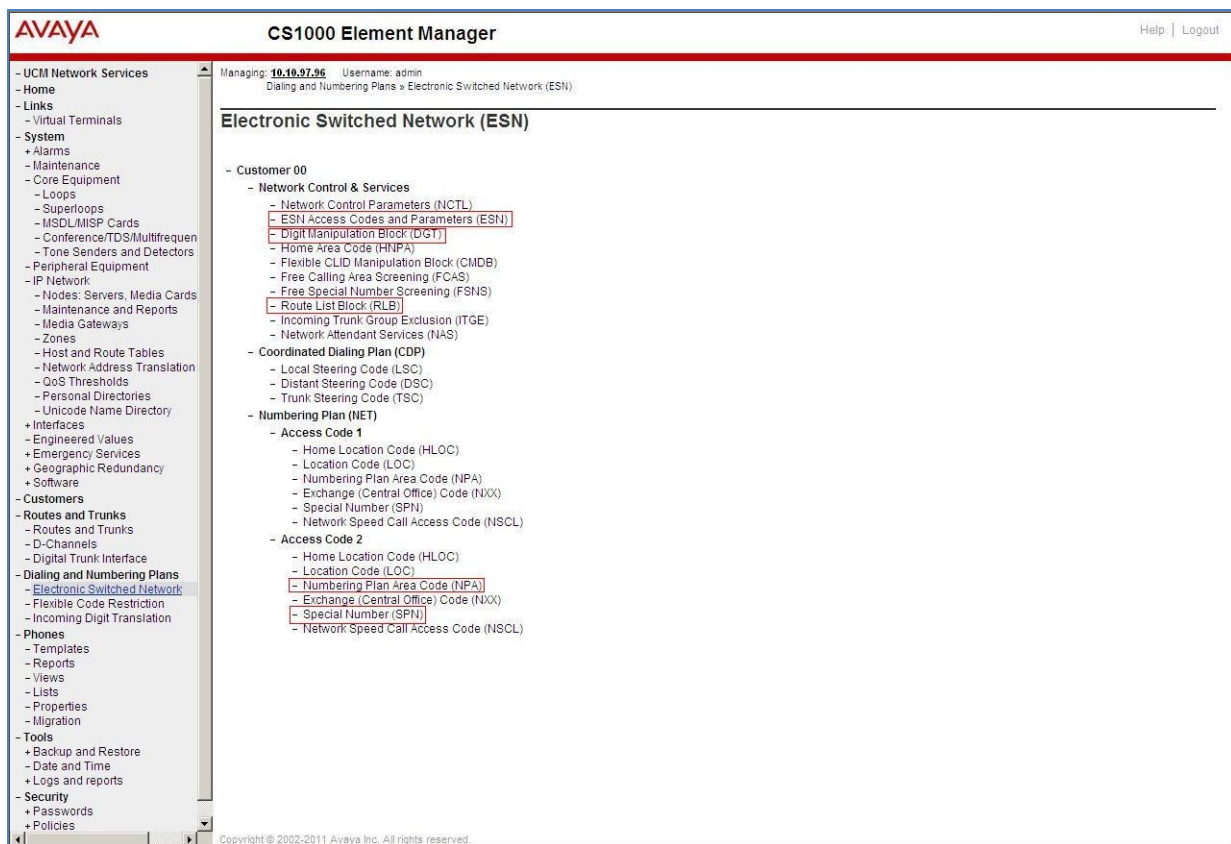
```
REQ: chg
TYPE: net

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
...
```

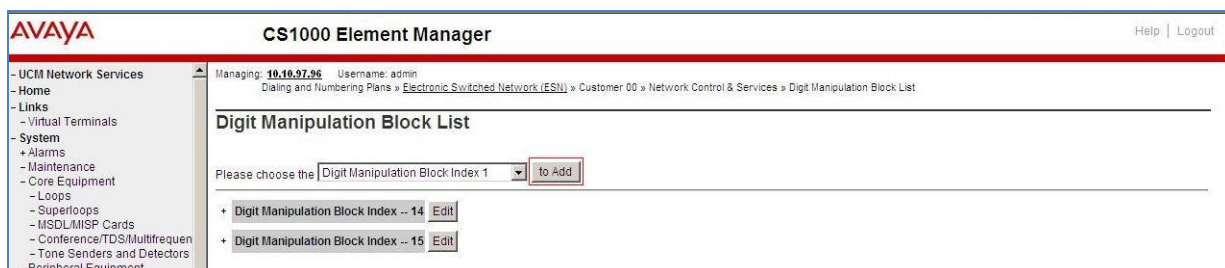
### 5.6.3. Digit Manipulation Block (DMI)

- 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**.
- 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**.
- 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).

- 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.
- In the Choose a DMI Number field, select an available DMI from the drop-down list and click **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.

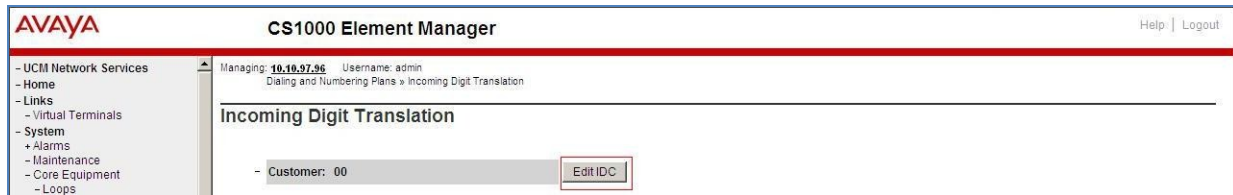
- **Route number (ROUT)** : 100 (created in **Section 5.5.5**)
- **Digit Manipulation Index (DMI)**: 15 (created in **Section 5.6.4**)
- **Incoming CLID Table**: 0 (created in **Section 5.5.7**)

**Figure 41 – RLB\_15 Route List Block Configuration Details**

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

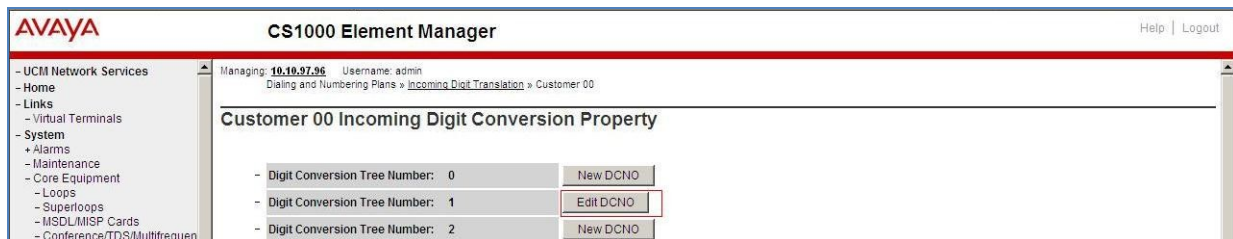
This section describes the steps for receiving the calls from PSTN via the PAETEC Communications system.

- 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.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (NAT)

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

Managing: 10.10.97.96 Username: admin

Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 1 Configuration

Digit Conversion Tree 1 Configuration

Regular IDC tree

Send calling party DID disabled

Add...

Delete IDC

Delete IDC tree

Refresh

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	2814022045	1700		Roman characters
2	2814022046	2046		Roman characters
3	2814022126	2126		Roman characters
4	2814022130	2130		Roman characters
5	7133433756	3756		Roman characters
6	7133433757	3757		Roman characters
7	7133433758	3758		Roman characters
8	7133433759	3759		Roman characters
9	7133433760	3760		Roman characters
10	7133434390	4390		Roman characters

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.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (NAT)

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Properties

Migration

Tools

Backup and Restore

Date and Time

Logs and reports

Security

Managing: 10.10.97.96 Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 2 » Special Number List

Special Number List

Please enter a Special Number  to Add

Special Number -- 0

Flexible length: 12

Inhibit time-out handler: NO

Type of call that is defined by the special number: NATL

Route list index: 14

Edit

Special Number -- 011

Flexible length: 14

Inhibit time-out handler: NO

Type of call that is defined by the special number: INTL

Route list index: 14

Edit

Special Number -- 1800

Flexible length: 11

Inhibit time-out handler: NO

Type of call that is defined by the special number: NATL

Route list index: 14

Edit

Special Number -- 411

Flexible length: 3

Inhibit time-out handler: NO

Type of call that is defined by the special number: NATL

Route list index: 14

Edit

Special Number -- 911

Flexible length: 3

Inhibit time-out handler: NO

Type of call that is defined by the special number: NATL

Route list index: 14

Edit



**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.

- 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**.
- 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**.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 2 » Numbering Plan Area Code List

### Numbering Plan Area Code List

Please enter an area code

Numbering Plan Area Code -- 1281	Edit
Route List Index: 15	
Incoming Trunk group Exclusion Index: NONE	
Numbering Plan Area Code -- 1613	Edit
Route List Index: 15	
Incoming Trunk group Exclusion Index: NONE	
Numbering Plan Area Code -- 1647	Edit
Route List Index: 15	
Incoming Trunk group Exclusion Index: NONE	
Numbering Plan Area Code -- 1713	Edit
Route List Index: 15	
Incoming Trunk group Exclusion Index: NONE	

**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

- Refer to **Section 5.5.4** to create a virtual super-loop - **96** used for IP phone.
- Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone.
- Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail).
- Create an IP phone by using **LD 11**.

```
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 RCBF  
   ICDD CDMD LLCN MCTD CLBD AUTU  
   GPUD DPUD DNDD CFXD ARHD CLTD ASCD  
   CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD  
   UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD  
   DRDD EXR0  
   USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF 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**

**UCM Network Services**

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

Days for day option 1:

Days for day option 2:

Days for day option 3:

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit:

Options: ☐ Call forward reminder tone for 500/2500 sets

☐ CFNA treatment for call waiting calls on a DN

☐ DID call to second degree busy treatment

☒ Message center

☒ Prevention of reciprocal call forward

Call forward: ☒ Originating

☐ Forwarding

**Number of normal ringing cycles for CFNA**

Option 0:

Option 1:

Option 2:

**Number of distinctive ringing cycles for CFNA**

Option 0:

Option 1:

Option 2:

**Calls routed to message center**

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

**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 RCB
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 RCB
```

...

```
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**.

The screenshot shows the Avaya Service Provider Pre-installation Wizard web interface. The top header is red with the Avaya logo. Below the header is a navigation menu on the left with options: Home, Configuration, Installation, Load, Network Settings, Logins, VPN Access, SBC, Summary, and Save. The main content area is titled 'Load Files' and 'Select a template'. It features a 'Template' dropdown menu with 'SBCT' selected. Below this, there is a section for 'File Upload' with a text input for 'EPW File:', a 'Browse...' button, a 'Load' button, and a 'Reset All' button. A 'Next Step' button with a red arrow is located at the bottom right of the main content area.

**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:** bvwddev.com

**AVAYA**

Home

Configuration

Installation

- Load
- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Save

### Network Settings

Enter network settings

Domain-0 IP Address	10.10.97.240
CDom IP Address	10.10.97.241
Gateway IP Address	10.10.97.193
Network Mask	255.255.255.192
Primary DNS	
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC	10.10.97.242	DevSBC5	bvwddev.com	(Optional)

Default Domain

(Optional)

Apply to all VMs

Previous Step

Next Step

**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**.

Login name	Password	Re-type password
craft	.....	.....
init	.....	.....
dadmin	.....	.....

**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**.

Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

**VPN Access Configuration**

VPN Router IP Address  (Optional)

Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

**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



AVAYA

Home

▼ Configuration

▲ Installation

Load

✖ Network Settings

✔ Logins

🔒 VPN Access

🔒 SBC

Summary

Save

Summary

Network Settings

Domain-0 Address	10.10.97.240
CDom Address	10.10.97.241
Gateway Address	10.10.97.193
Network Mask	255.255.255.192
Primary DNS	Not set
Secondary DNS	Not set
Default Search List	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname	Domain
SBC	10.10.97.242	DevSBC5	bvwdev.com
Default Domain			Not set

Logins

SBC craft Password	*****
SBC init Password	*****
SBC dadmin Password	*****

VPN Access

VPN Access	Not Configured
------------	----------------

SBC

Service Provider	generic
Service Provider Port	5060
Service Provider IP Address	20.20.64.220
Service Provider Signalling/Media Network1	
Service Provider Signalling/Media Netmask1	
Service Provider IP Address2	Not set
Service Provider Signalling/Media Network2	Not set

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**.

**AVAYA**

Home

▼ Configuration

▲ Installation

- Load
- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Save

### Save

The following required fields have not been set

[Primary DNS](#)

The following optional fields have not been set

[Default Search List](#)

[Secondary DNS](#)

[HTTPS Proxy](#)

[Default Domain](#)

[SBC Service Provider IP Address 2](#)

[SBC Service Provider Hunting](#)

[SBC Service Provider Media Netmask2](#)

[SBC Service Provider Media Network2](#)

[SBC Enterprise SIP Server IP2](#)

[SBC Enterprise SIP Server Transport2](#)

[SBC Enterprise SIP Server Hunting](#)

**WARNING** - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

**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.

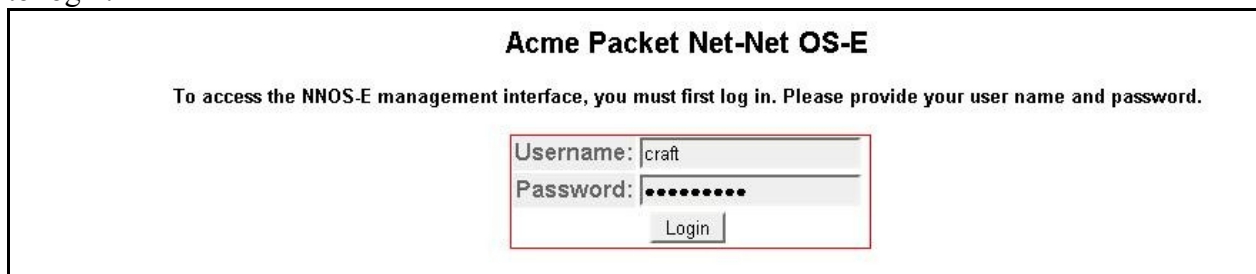
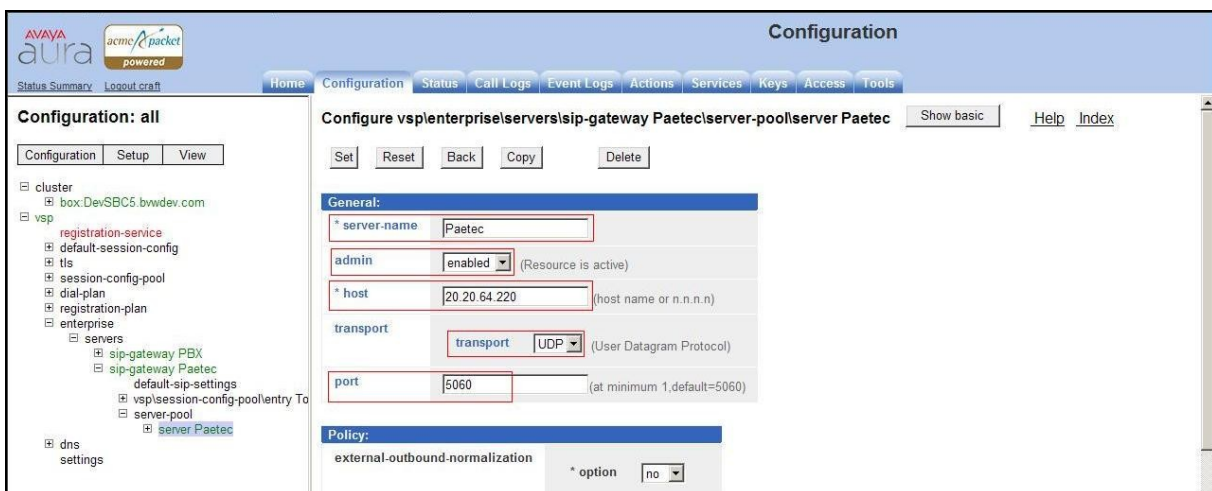


Figure 55: Login to AA-SBC

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**

The screenshot displays the Avaya Aura Configuration web interface. The top navigation bar includes tabs for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy: cluster > vsp > enterprise > servers > sip-gateway PBX > server-pool > server PBX. The main content area is titled 'Configure vspenterprise\servers\sip-gateway PBX\server-pool\server PBX' and contains a 'General' tab. The configuration fields are as follows:

General:	
* server-name	PBX
admin	enabled (Resource is active)
* host	10.10.97.178 (host name or n.n.n.n)
transport	transport UDP (User Datagram Protocol)
port	5060 (at minimum 1, default=5060)

**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**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view with the following structure: cluster > box:DevSBC5.bwdev.com > vsp > registration-service > default-session-config > tis > session-config-pool > dial-plan > registration-plan > enterprise > servers > sip-gateway PBX > sip-gateway Paetec. The main content area is titled "Configure vspenterprise\servers\sip-gateway Paetec". It includes a "general:" section with the following fields: "name" (Paetec), "peer-identity" (empty), "admin" (enabled), "domain" (20.20.64.220), "directory" (Create), and "failover-detection" (register). The "failover-detection" field has a note: "(Use REGISTER to detect failures)".

**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**.

The screenshot shows the Avaya Aura Configuration interface for the same configuration page as Figure 58. The "registration-failover:" section is expanded, showing the following fields: "user" (7133434387), "password-tag" (empty), and "add-user-to-contact" (enabled). The "servers:" section is also expanded, showing "server-type" (sip-proxy) and "server-pool" (Delete). The "routing:" section is expanded, showing "routing-setting" (normalization) and "auto-tag-match" (auto-domain-match). The "pstin-backup" field is also visible.



**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

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'source-route FromPBX' selected under 'dial-plan'. The main area shows the configuration for 'source-route FromPBX' with the following fields:

- general:**
  - \* name: FromPBX
  - description: (empty)
  - \* source-match: (empty)
  - \* type: server
  - \* source-server: vsp\enterprise\servers\sip-gateway PBX
- peer:**
  - type: server (Peer is a SIP server)
  - server: vsp\enterprise\servers\sip-gateway Paetec
- location-match-preferred:** up-to-outbound-peer (Outbound peer determines whether preferred)
- routing-tag:** Add routing-tag
- priority:** 100 (from 0 to 999,999, default=100)
- condition-list:** Configure
- condition-list-match-secondary:** false

**Figure 60: Dial-plan “source-route FromPBX” Page 1**

AVAYA

aura

acme

packet

powered

[Status Summary](#)
[Logout/craft](#)

[Home](#)
[Configuration](#)
[Status](#)
[Call Logs](#)
[Event Logs](#)
[Actions](#)
[Services](#)
[Keys](#)
[Access](#)
[Tools](#)

Configuration: all

Configuration

Setup

View

cluster

box:DevSBC5.bwwdev.com

vsp

registration-service

default-session-config

tls

session-config-pool

dial-plan

route Default

source-route FromPaetec

source-route FromPBX

registration-plan

enterprise

dns

settings

other properties:

admin

enabled

(Resource is active)

emergency

false

action

forward

(forward the INVITE to the server specified in the header)

response-code

200

response-string

apply-to-methods

INVITE

REFER

MESSAGE

INFO

Select All

Unselect All

request-user

\* type

no

(No normalization applied to phone numbers)

to-user

\* type

no

(No normalization applied to phone numbers)

from-user

\* type

no

(No normalization applied to phone numbers)

admission-control

disabled

(Resource is inactive)

max-bandwidth

enter

unlimited

kbits-per-second or select from

unlimited

(No limit to the minimum of bandwidth)

max-number-of-concurrent-calls

100

(from 0 to 1,000,000,default=100)

session-config

vsp/session-config-pool/entry ToPaetec

Edit

Create

Set

Reset

Back

Copy

**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**

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'source-route FromPaetec' selected under 'dial-plan'. The main area shows the configuration for this entry. The 'general' tab is active, displaying fields for 'name' (FromPaetec), 'description', 'source-match' (type: server, source-server: vsp\enterprise\servers\sip-gateway Paetec), 'peer' (type: server, server: vsp\enterprise\servers\sip-gateway PBX), 'location-match-preferred' (up-to-outbound-peer), 'routing-tag' (Add routing-tag), 'priority' (100), 'condition-list' (Configure), and 'condition-list-match-secondary' (false). The 'source-server' and 'server' fields are highlighted with red boxes.

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

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

**Configuration: all**

Configuration Setup View

cluster  
box:DevSBC5.bvwdev.com  
vsp  
registration-service  
default-session-config  
tls  
session-config-pool  
dial-plan  
route Default  
source-route FromPaetec  
source-route FromPBX  
registration-plan  
enterprise  
dns  
settings

**other properties:**

admin enabled (Resource is active)

emergency false

action forward (forward the INVITE to the server specified in the header)

response-code 200

response-string

apply-to-methods  
INVITE  
REFER  
MESSAGE  
INFO  
Select All Unselect All

request-user \* type no (No normalization applied to phone numbers)

to-user \* type no (No normalization applied to phone numbers)

from-user \* type no (No normalization applied to phone numbers)

admission-control disabled (Resource is inactive)

max-bandwidth enter unlimited kbits-per-second or select from unlimited (No limit to the minimum of bandwidth)

max-number-of-concurrent-calls 100 (from 0 to 1,000,000,default=100)

session-config vsp/session-config-pool/entry ToPBX Edit Create

Set Reset Back Copy

**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**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar contains a tree view with the following structure:

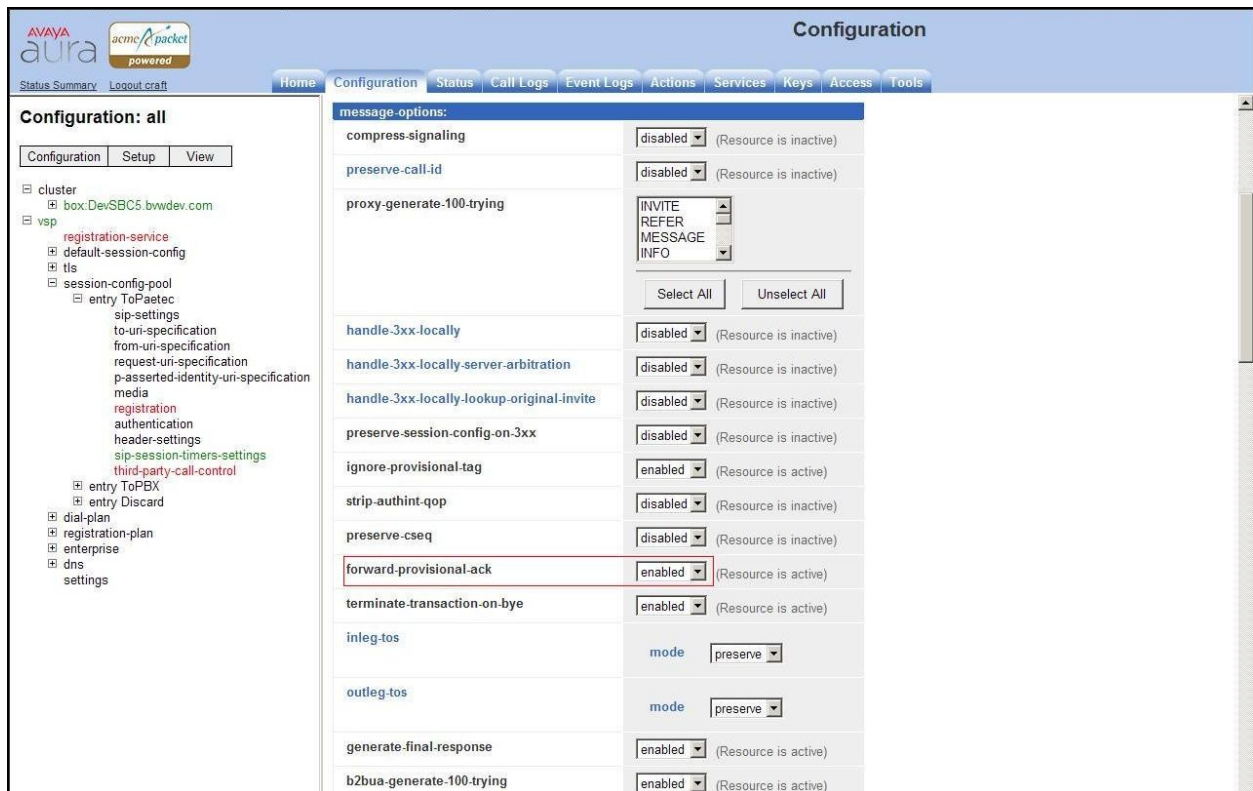
- cluster
  - box:DevSBC5.bvwddev.com
- vsp
  - registration-service
  - default-session-config
  - tls
  - session-config-pool
    - entry ToPaetec
      - sip-settings
        - to-un-specification
        - from-uri-specification
        - request-uri-specification
        - p-asserted-identity-uri-specification
        - media
        - registration
        - authentication
        - header-settings
        - sip-session-timers-settings
        - third-party-call-control
- entry ToPBX
- entry Discard
- dial-plan
- registration-plan
- enterprise
- dns
- settings

The main configuration area shows the following settings:

Setting	Value	Range/Default
max-retransmissions	10	(from 0 to 32, default=1)
outbound-local-port	0	(from 0 to 65,535)
udp-source-port	directive auto-determine	(The Net-Net OS-E sets the SIP port.)
ignore-cancel-branch	disabled	(Resource is inactive)
symmetric-signaling	disabled	(Resource is inactive)
sips-uri-scheme-setting	auto	
redirect-preserve-session-config	disabled	(Resource is inactive)
max-forwards	70	
enum-fail-response	* enum-lookup-failed-action ignore	(ignore failed lookup)
dns-fail-response-code	404	(from 0 to 65,535)
dns-fail-response-string	Not Found	
update-moc-via-csta	disabled	(Resource is inactive)
propagate-RR-headers	disabled	
ignore-via-port	disabled	(Resource is inactive)
ignore-route-header	disabled	(Resource is inactive)
supported-inleg		
supported-outleg		
persistent-destination-address	true	
loop-detection-threshold	2	(from 1 to 256, default=2)
make-provisional-resp-reliable	0	

**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.

The screenshot shows the Avaya Aura Configuration interface. On the left is a tree view of the configuration hierarchy. The main area displays the configuration for 'entry ToPaetec\from-uri-specification'. The 'host' field is highlighted with a red box and set to 'local-ip'. Other fields include 'user', 'port', 'display', 'user-agent-aware-display-translation', 'transport', 'user-param', 'user-truncate-non-digits', 'uri-parameter', 'header-parameter', 'add-oli-tag', 'copy-charge-uri-user', 'strip-digits', and 'prepend-digits'.

Field	Value	Notes
user	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
host	local-ip	(Net-Net OS-E uses the local ip for the next-hop server.)
port	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
display	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-agent-aware-display-translation	disabled	(Resource is inactive)
transport	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-param	omit	
user-truncate-non-digits	disabled	(Resource is inactive)
uri-parameter	Add uri-parameter	
header-parameter		
add-oli-tag	0	
copy-charge-uri-user	disabled	(Resource is inactive)
strip-digits	0	
prepend-digits		(Maximum 128 characters)

**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.



**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

Configuration Setup View

- cluster
  - box:DevSBC5.bvwddev.com
- vsp
  - registration-service
  - default-session-config
  - tls
  - session-config-pool
    - entry ToPaetec
      - sip-settings
        - to-uri-specification
        - from-uri-specification
        - request-uri-specification
        - p-asserted-identity-uri-specification
        - media
        - registration
        - authentication
        - header-settings
        - sip-session-timers-settings
        - third-party-call-control
      - entry ToPBX
      - entry Discard
    - dial-plan
    - registration-plan
    - enterprise
    - dns
    - settings

**Configure vsp\session-config-pool\entry ToPaetec** [Help](#) [Index](#)

Set Reset Back Delete

user	enter <input type="text" value="to-uri"/> or select from <input type="text" value="to-uri"/> (Net-Net OS-E uses the value from the incoming TO URI.)
host	enter <input type="text" value="next-hop"/> or select from <input type="text" value="next-hop"/> (Net-Net OS-E uses the IP address of the next-hop server.)
port	enter <input type="text" value="to-uri"/> or select from <input type="text" value="to-uri"/> (Net-Net OS-E uses the value from the incoming TO URI.)
display	enter <input type="text" value="to-uri"/> or select from <input type="text" value="to-uri"/> (Net-Net OS-E uses the value from the incoming TO URI.)
transport	<input type="text" value="to-uri"/> (Net-Net OS-E uses the value from the incoming TO URI.)
user-param	<input type="text" value="omit"/>
user-truncate-non-digits	<input type="text" value="disabled"/> (Resource is inactive)
uri-parameter	<a href="#">Add uri-parameter</a>
header-parameter	<input type="text"/>
add-oli-tag	<input type="text" value="0"/>
strip-digits	<input type="text" value="0"/>

Set Reset Back

**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.

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

Configuration Setup View

- cluster
  - box:DevSBC5.bvwddev.com
- vsp
  - registration-service
  - default-session-config
  - tls
  - session-config-pool
    - entry ToPaetec
      - sip-settings
        - to-uri-specification
        - from-uri-specification
        - request-uri-specification
        - p-asserted-identity-uri-specification
        - media
        - registration
        - authentication
        - header-settings
        - sip-session-timers-settings
        - third-party-call-control
      - entry ToPBX
      - entry Discard
    - dial-plan
    - registration-plan
    - enterprise
    - dns
    - settings

**Configure vsp\session-config-pool\entry ToPaetec\request-uri-specification** [Help](#) [Index](#)

Set Reset Back Delete

user	enter <input type="text" value="request-uri"/> or select from <input type="text" value="request-uri"/> (Net-Net OS-E uses the value from the incoming REQUEST URI.)
host	enter <input type="text" value="next-hop"/> or select from <input type="text" value="next-hop"/> (Net-Net OS-E uses the IP address of the next-hop server.)
port	enter <input type="text" value="request-uri"/> or select from <input type="text" value="request-uri"/> (Net-Net OS-E uses the value from the incoming REQUEST URI.)
transport	<input type="text" value="request-uri"/> (Net-Net OS-E uses the value from the incoming REQUEST URI.)
user-param	<input type="text" value="omit"/>
user-truncate-non-digits	<input type="text" value="disabled"/> (Resource is inactive)
uri-parameter	<a href="#">Add uri-parameter</a>
apply-to-routing	<input type="text" value="false"/>
use-location-cache-contact-uri	<input type="text" value="true"/>

Set Reset Back

**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.

The screenshot shows the Avaya Aura Configuration interface. On the left is a tree view of the configuration hierarchy. The main area displays the configuration for 'vsp\session-config-pool\entry ToPaetec\p-asserted-identity-uri-specification'. The 'host' field is highlighted with a red box and set to 'local-ip'. Other fields include 'user' (same-uri), 'port' (same-uri), 'display' (same-uri), 'transport' (same-uri), 'user-param' (omit), 'uri-parameter' (Add uri-parameter), 'create' (false), and 'use-original-from-header' (false).

Field	Value	Notes
user	same-uri	(Net-Net OS-E uses the value from the uri being altered.)
host	local-ip	(Net-Net OS-E uses the local ip for the next-hop server.)
port	same-uri	(Net-Net OS-E uses the value from the incoming uri being altered.)
display	same-uri	(Net-Net OS-E uses the value from the uri being altered.)
transport	same-uri	(Net-Net OS-E uses the value from the incoming uri being altered.)
user-param	omit	
uri-parameter	Add uri-parameter	
create	false	
use-original-from-header	false	

**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**.

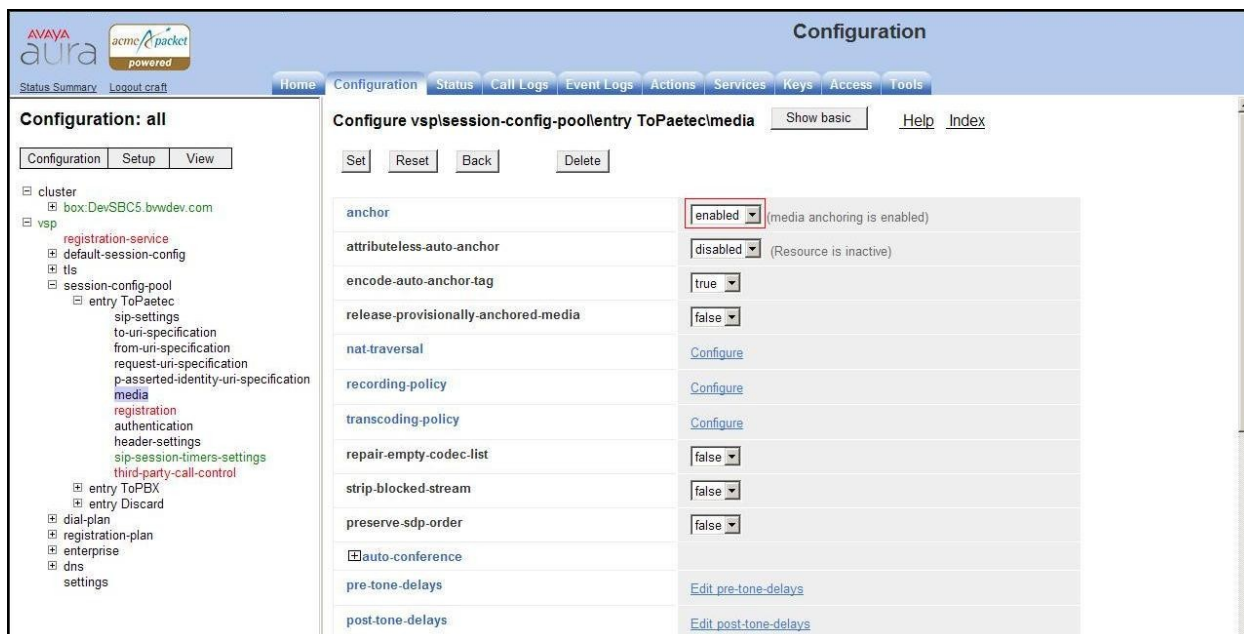


Figure 70: Enable media anchoring

#### 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**.

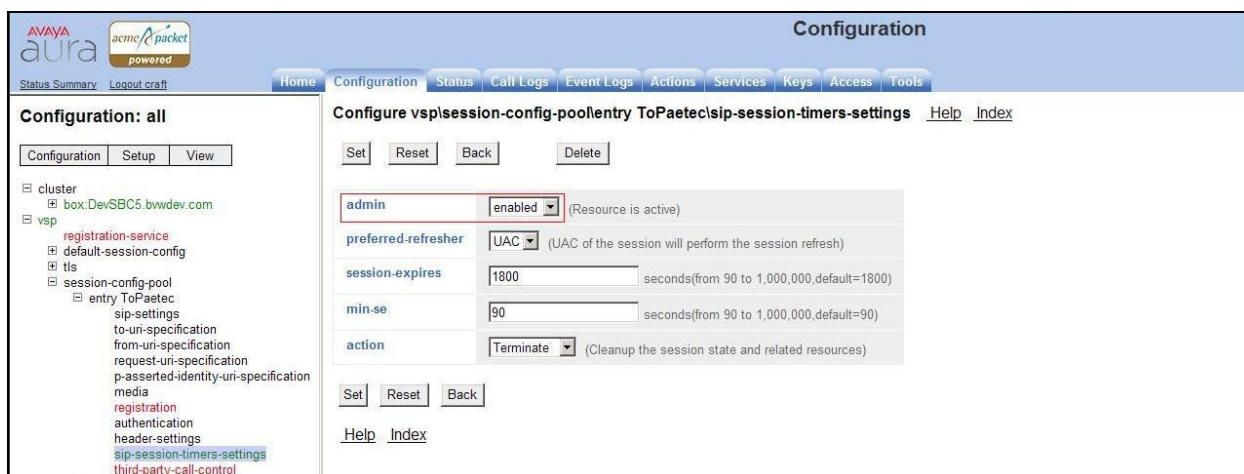


Figure 71: Enable SIP session timers

### 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**.

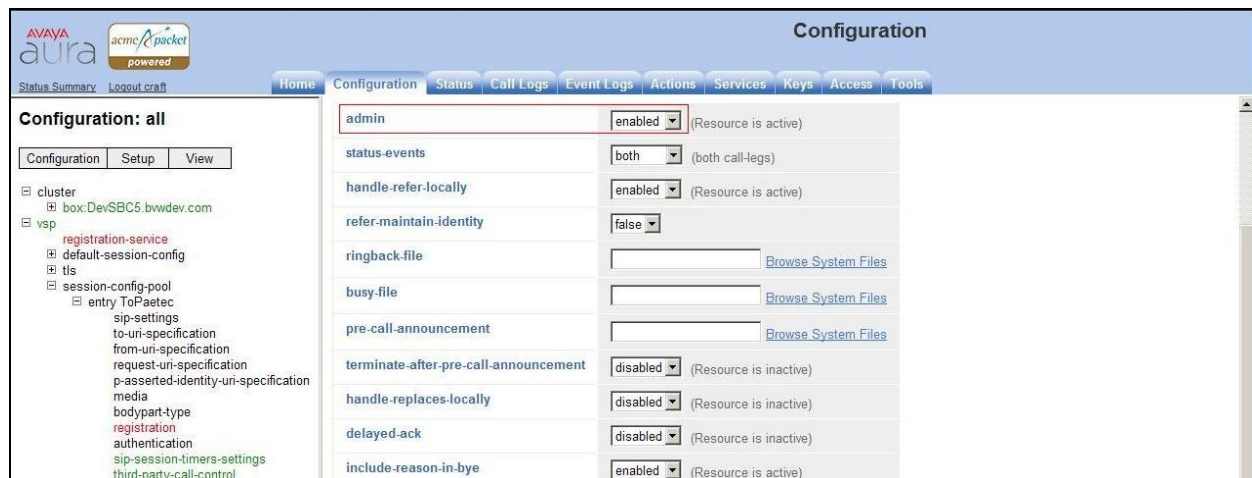


Figure 72: Enable third-party-call-control

## 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 bwvdev.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 **bwvdev.com** in the **To** header sent to CS1000.



**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

Configuration Setup View

cluster

box:DevSBC5.bvwdev.com

vsp

registration-service

default-session-config

tls

session-config-pool

entry ToPaetec

entry ToPBX

sip-settings

to-uri-specification

request-uri-specification

registration

header-settings

entry Discard

dial-plan

registration-plan

enterprise

dns

settings

Configure vsp\session-config-pool\entry ToPBX\to-uri-specification Help Index

Set Reset Back Delete

user enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

host enter next-hop-domain or select from next-hop-domain (Net-Net OS-E uses the domain of the next-hop server.)

port enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

display enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

transport to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

user-param omit

user-truncate-non-digits disabled (Resource is inactive)

uri-parameter Add uri-parameter

header-parameter

add-oli-tag 0

strip-digits 0

**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 **bwvdev.com** in the **Request-URI** header sent to CS1000.

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

Configuration Setup View

cluster

box:DevSBC5.bvwdev.com

vsp

registration-service

default-session-config

tls

session-config-pool

entry ToPaetec

entry ToPBX

sip-settings

to-uri-specification

request-uri-specification

registration

header-settings

entry Discard

dial-plan

registration-plan

enterprise

dns

settings

Configure vsp\session-config-pool\entry ToPBX\request-uri-specification Help Index

Set Reset Back Delete

user enter request-uri or select from request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)

host enter next-hop-domain or select from next-hop-domain (Net-Net OS-E uses the domain of the next-hop server.)

port enter request-uri or select from request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)

transport request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)

user-param omit

user-truncate-non-digits disabled (Resource is inactive)

uri-parameter Add uri-parameter

apply-to-routing false

use-location-cache-contact-uri true

Set Reset Back

**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**.

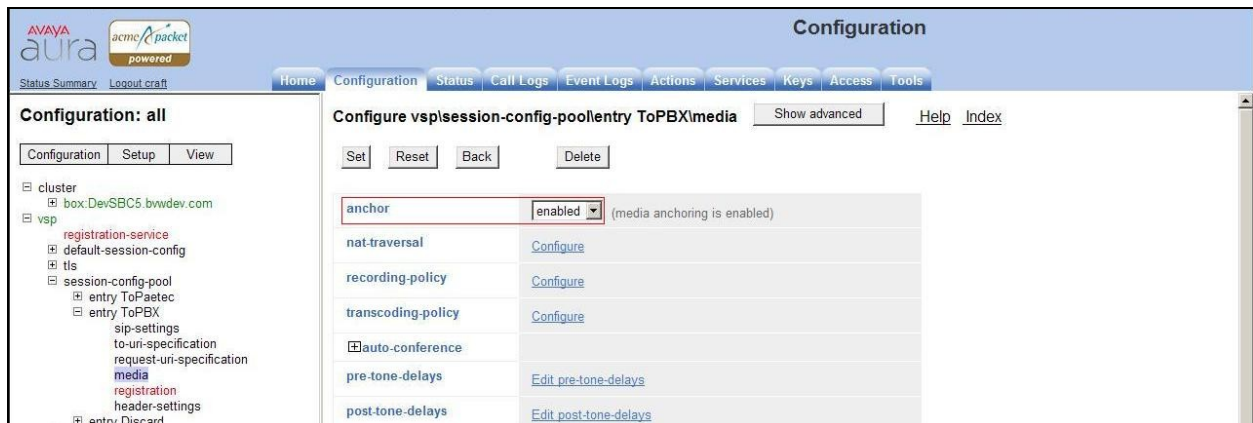


Figure 75: Enable media anchoring

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

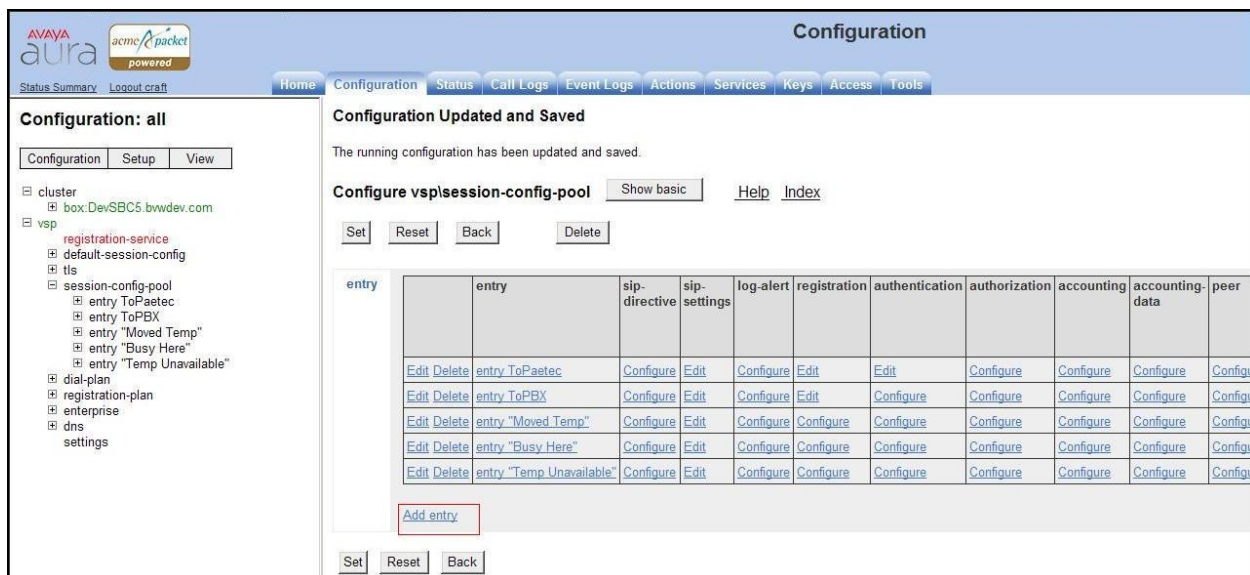
The procedure to create a rule to convert History-Info to Diversion header on DevSBC5 is as below:

- 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”

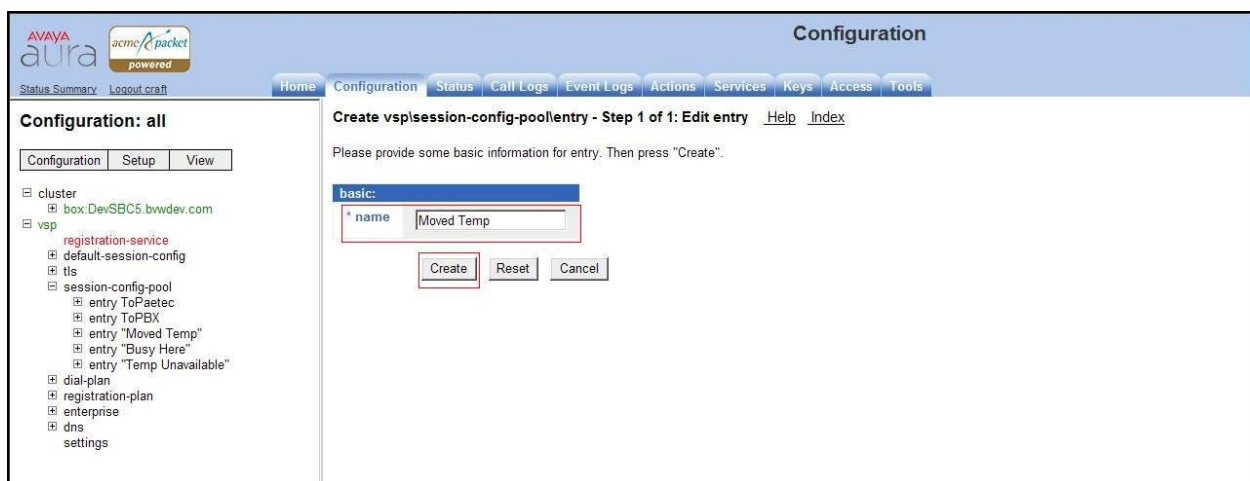
a) Create entry session-config-pool “Moved Temp”

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”**

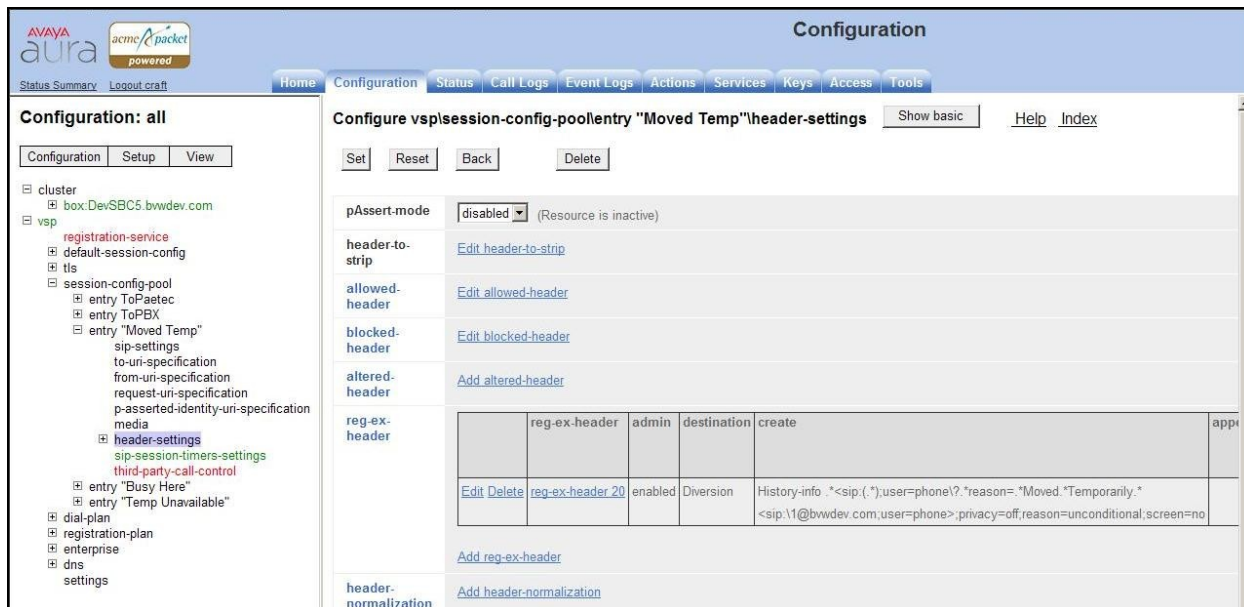
c) Create basic configuration

- 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”**

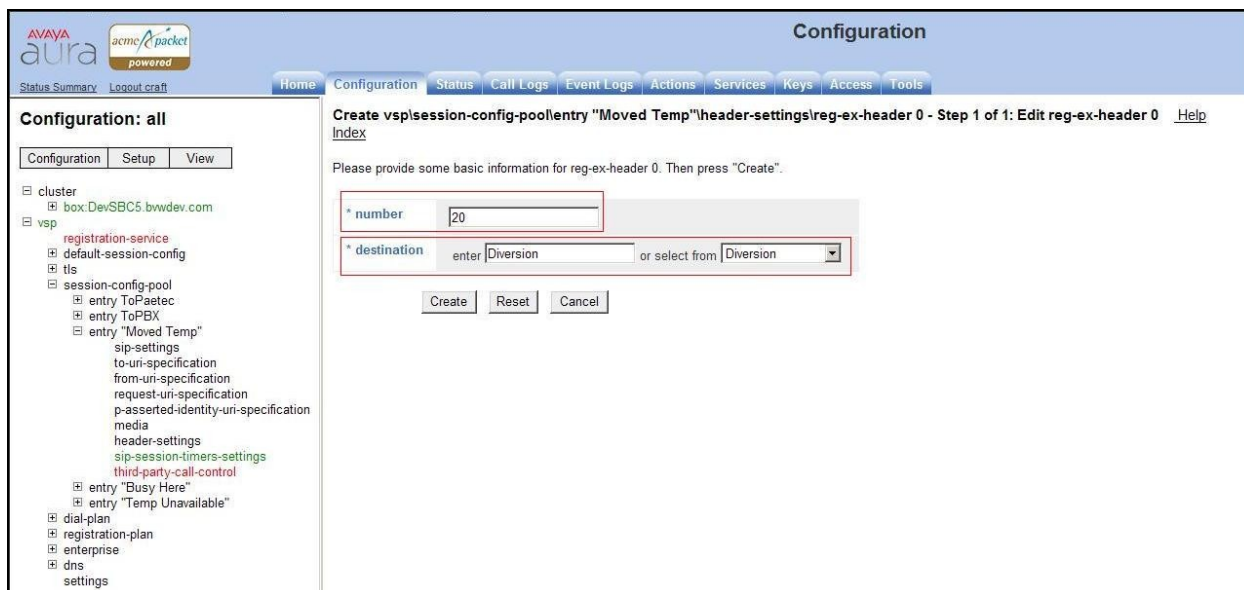


To create a regular expression rule, select **Configuration vsp\session-config-pool\entry “Moved Temp”\header settings**. Click **Add reg-ex-header** link as shown in **Figure 78**.



**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`

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, with 'session-config-pool' expanded to show 'entry "Moved Temp"'. The main panel is titled 'Configure vsp\session-config-poolentry "Moved Temp"header-settings\reg-ex-header 20'. It contains a form with the following fields:

- admin**: enabled (Resource is active)
- \* number**: 20
- \* destination**: enter Diversion or select from Diversion
- \* source**: enter History-info or select from History-info
- \* expression**: `*<sip:(.*)@.*;user=phone\?.*reason=.*Moved.*Temporarily.*` (regular expression)
- \* replacement**: `<sip:\1@bvwdev.com;user=phone>;privacy=off;reason=unconditional;screen=no`
- append**: Add append
- apply-to-methods**: INVITE, REFER, MESSAGE, INFO (Select All, Unselect All)
- apply-to-responses**: \* type: no (Do not apply to responses (requests only))
- apply-to-dialog**: both (Apply to both inbound and outbound dialogs.)
- session-persistent**: disabled (Resource is inactive)
- cseq**: 0
- create-on-failed-match**: true
- append-on-failed-match**: true

**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**.

	source-route	description	source-match	peer	location-match-preferred	priority	con list
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">source-route FromPaetec</a>		server vsp\enterprise\servers\sip-gateway Paetec	server vsp\enterprise\servers\sip-gateway PBX	up-to-outbound-peer	100	<a href="#">Con</a>
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">source-route FromPBX</a>		server vsp\enterprise\servers\sip-gateway PBX	server vsp\enterprise\servers\sip-gateway Paetec	up-to-outbound-peer	100	<a href="#">Con</a>
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">source-route "Moved Temp"</a>		server vsp\enterprise\servers\sip-gateway PBX	server vsp\enterprise\servers\sip-gateway Paetec	up-to-outbound-peer	97	<a href="#">Edit</a>
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">source-route "Busy Here"</a>		server vsp\enterprise\servers\sip-gateway PBX	server vsp\enterprise\servers\sip-gateway Paetec	up-to-outbound-peer	98	<a href="#">Edit</a>
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">source-route "Temp Unavailable"</a>		server vsp\enterprise\servers\sip-gateway PBX	server vsp\enterprise\servers\sip-gateway Paetec	up-to-outbound-peer	99	<a href="#">Edit</a>

[Add source-route](#)

**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**.

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

**Configuration: all**

Configuration Setup View

cluster  
box:DevSBC5.bvwdev.com

vsp  
registration-service  
default-session-config  
tis  
session-config-pool  
dial-plan  
route Default  
source-route FromPaetec  
source-route FromPBX  
source-route "Moved Temp"  
source-route "Busy Here"  
source-route "Temp Unavailable"  
registration-plan  
enterprise  
dns  
settings

**Create vsp\dial-plan\source-route - Step 1 of 1: Edit source-route** [Help](#) [Index](#)

Please provide some basic information for source-route. Then press "Create".

**general:**

\* name

\* source-match

\* type

\* source-server  [Create](#)

**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”**

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy, with 'vsp' expanded and 'source-route "Moved Temp"' selected. The main panel shows the configuration for this entry. The 'general' section includes fields for 'name' (Moved Temp), 'description', 'source-match' type (server), and 'source-server' (vsp\enterprise\servers\sip-gateway PBX). The 'peer' section shows 'type' (server) and 'server' (vsp\enterprise\servers\sip-gateway Paetec). The 'location-match-preferred' is set to 'up-to-outbound-peer'. The 'routing-tag' is 'Add routing-tag'. The 'priority' is set to 97. The 'condition-list' is 'Configure' and 'condition-list-match-secondary' is 'true'. The 'other properties' section shows 'admin' (enabled), 'emergency' (false), 'action' (forward), and 'response-code' (200).

**Figure 83: Entry source-route dial-plan “Moved Temp” detail – Page 1**

The screenshot shows the Avaya Aura Configuration interface. On the left, a tree view shows the configuration hierarchy: Configuration > vsp > registration-service > default-session-config > session-config-pool > entry "Moved Temp". The main area displays the configuration for this entry. The "other properties" section includes fields for admin (enabled), emergency (false), action (forward), response-code (200), response-string, and apply-to-methods (INVITE, REFER, MESSAGE, INFO). The "request-user", "to-user", and "from-user" fields are set to "no" type. The "admission-control" is disabled. The "max-bandwidth" is unlimited. The "max-number-of-concurrent-calls" is 100. The "session-config" field is set to "vsp\session-config-pool\entry "Moved Temp"". At the bottom, there are buttons for Set, Reset, Back, and Copy.

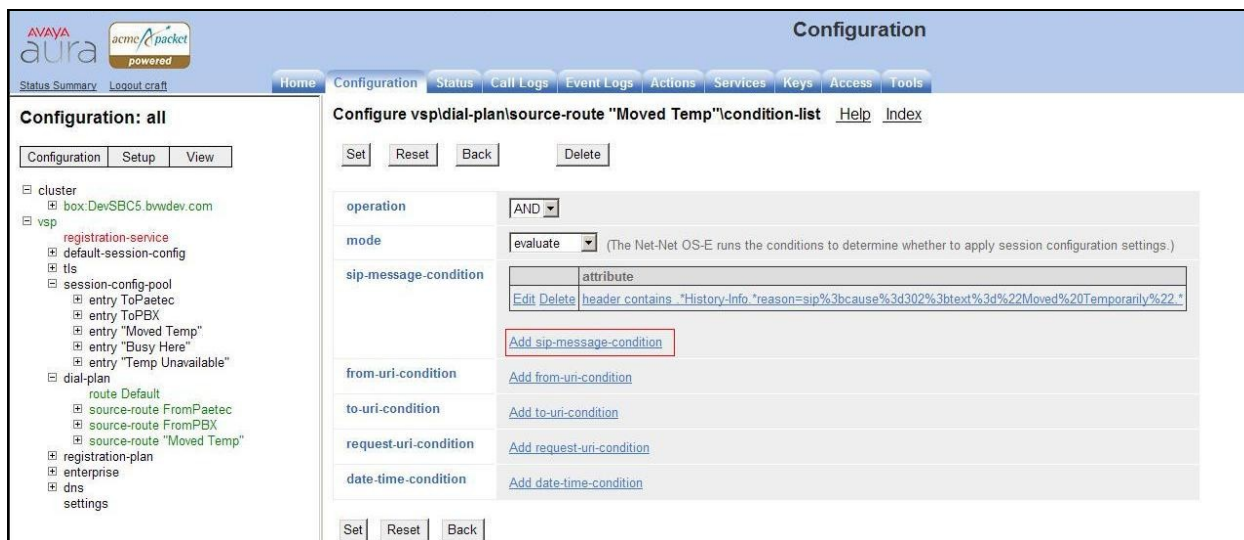
**Figure 84: Entry source-route dial-plan “Moved Temp” detail – Page 2**

#### 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**.

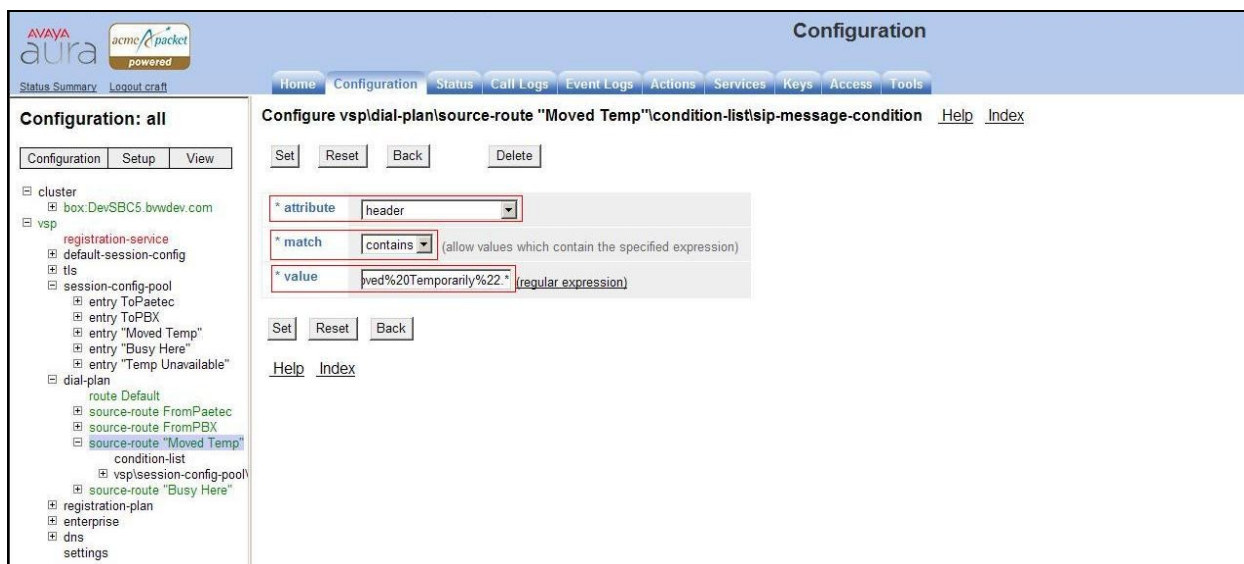




**Figure 85: Link to Add sip-message-condition**

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%3because%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`

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, with 'session-config-pool' expanded. The main area shows the configuration for the entry 'Busy Here'. The 'admin' status is 'enabled'. The 'number' is '20'. The 'destination' is 'Diversion'. The 'source' is 'History-info'. The 'expression' is `*<sip:(.*)@.*;user=phone?.*reason=.*Busy.*Here.*` and the 'replacement' is `<sip:1@bvwdev.com;user=phone>;privacy=off;reason=user-busy;screen=no`. The 'apply-to-methods' section shows 'INVITE', 'REFER', 'MESSAGE', and 'INFO' selected. The 'apply-to-responses' type is 'no'. The 'apply-to-dialog' is 'both'. The 'session-persistent' status is 'disabled'. The 'cseq' is '0'. The 'create-on-failed-match' and 'append-on-failed-match' are both set to 'true'.

**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%3d486%3btext%3d%22Busy%20Here%22.\*

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, including 'cluster', 'vsp', 'registration-service', 'default-session-config', 'tis', 'session-config-pool', 'dial-plan', 'registration-plan', 'enterprise', 'dns', and 'settings'. The main content area is titled 'Configuration' and shows the 'Create vspldial-plan\source-route "Busy Here"\condition-list\sip-message-condition - Step 1 of 1: Edit sip-message-condition' form. The form includes a 'Please provide some basic information for sip-message-condition. Then press "Create".' instruction. The form fields are: '\* attribute' (header), '\* match' (contains), and '\* value' (.\*22Busy%20Here%22.\*). There are 'Create', 'Reset', and 'Cancel' buttons at the bottom of the form.

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

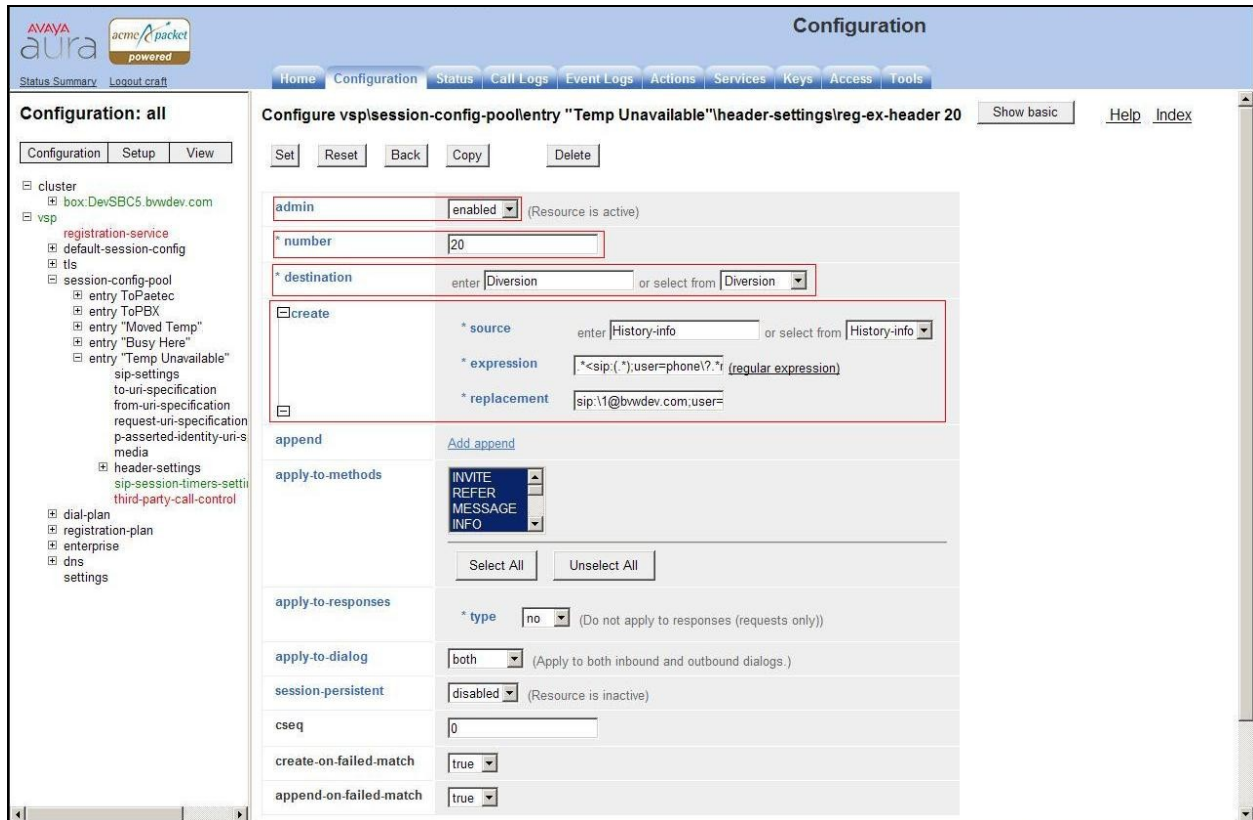
## 6.10. Convert History-Info to Diversion header for Call Forward No Answer Scenario

### 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@bvwddev.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**

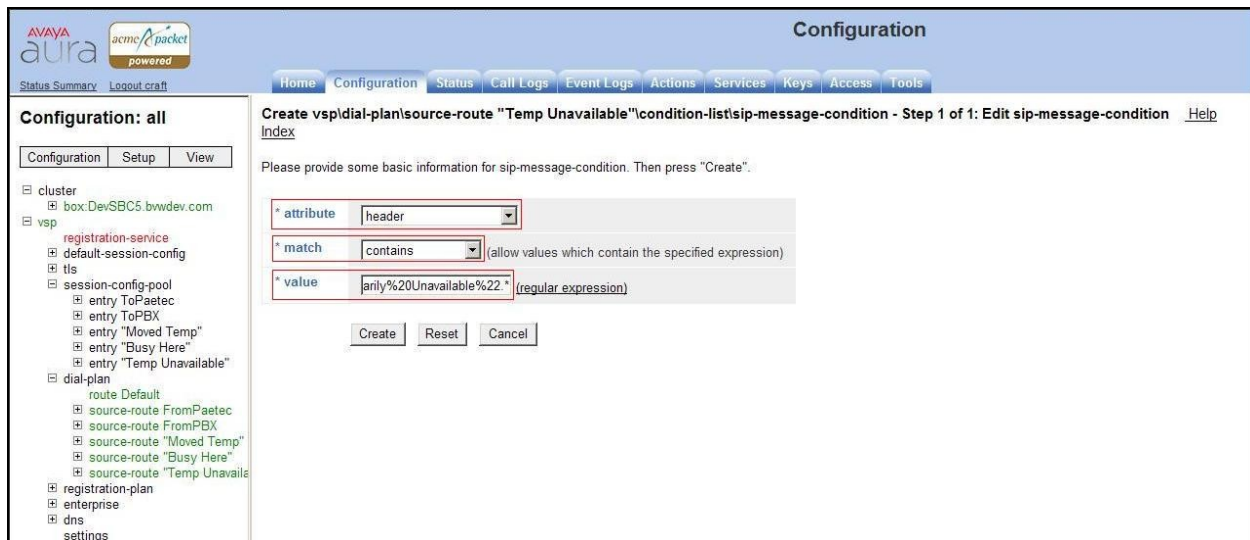
### 6.10.2. Create entry source-route dial-plan “Temp Unavailable”

Refer to Session 6.8.2 to create entry source-route dial-plan “Temp Unavailable” 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**

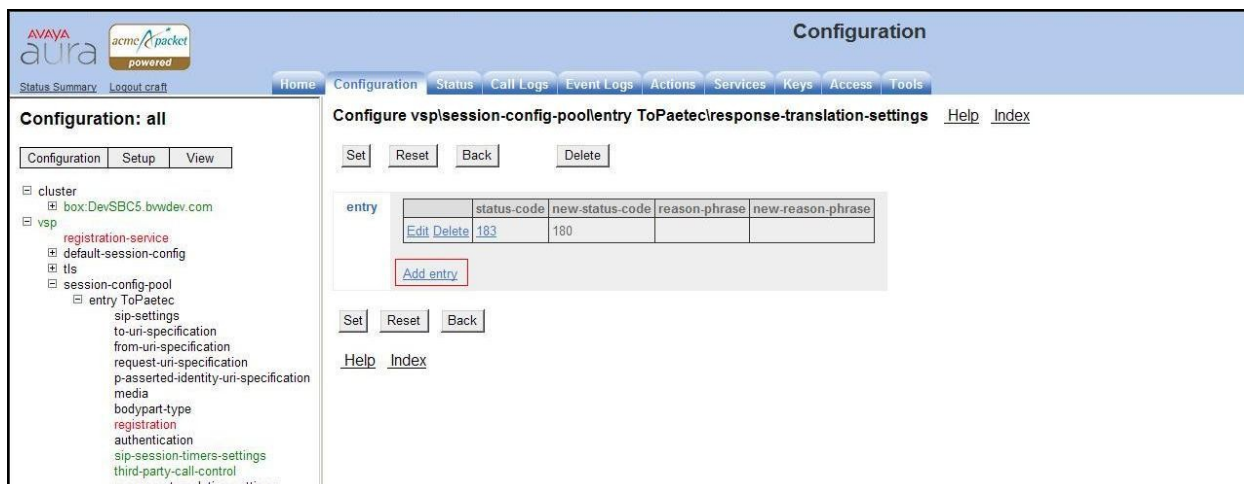
## 6.11. Convert 183 with SDP to 180 without SDP for Ring-Back-Tone in Call Blind Transfer Scenario

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.

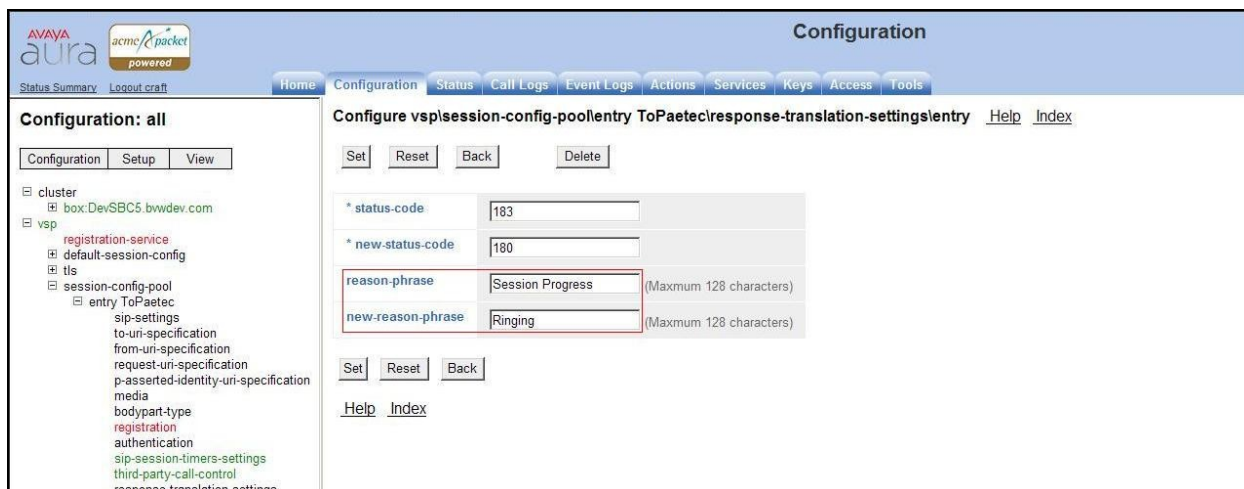
### 6.11.1. Create an entry to convert SIP 183 with SDP to SIP 180 with SDP

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.

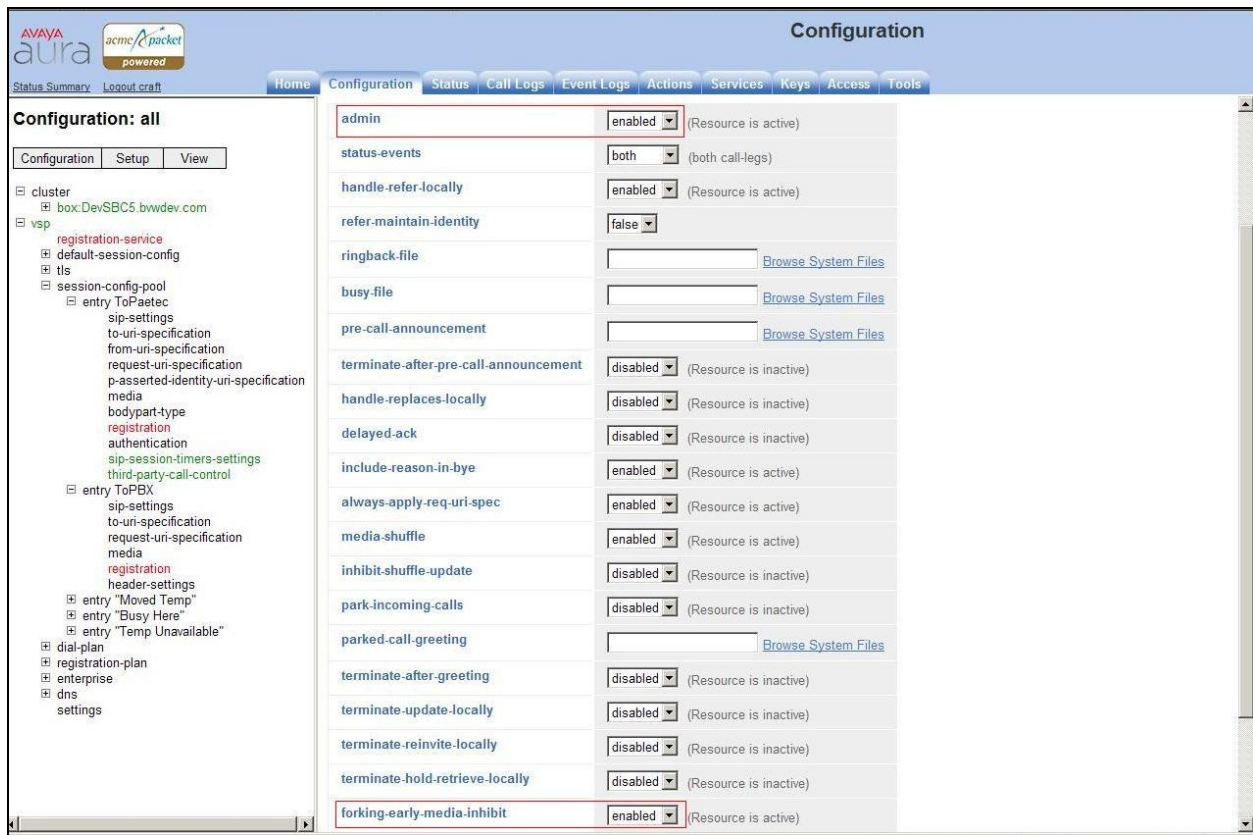


**Figure 92: Edit entry to convert SIP 183 with SDP to SIP 180 with SDP**

### 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
QUEUE 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
```

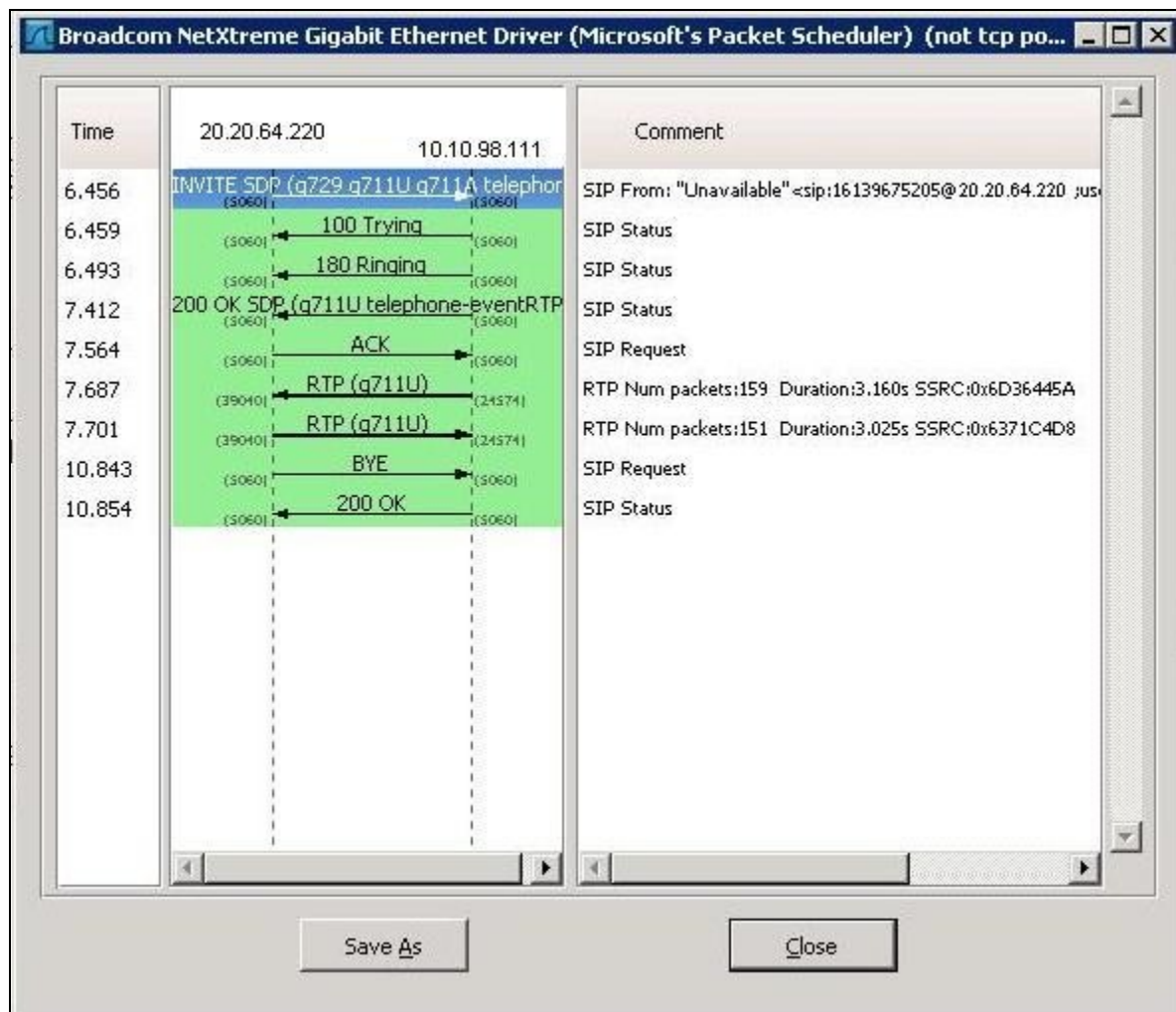


After the call is released, check all SIP trunk status changed to IDLE state.

```
.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-1ecpqqa1h9ba>;tag=244833123-13202597
      SIP Display info: "Unavailable"
    ■ SIP from address: sip:16139675205@20.20.64.220;user=phone;broadworks=BWWESTSIGIS-1ecpqqa1h9ba
      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: BW1848431190211111827754577@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*

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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