



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TELUS SIP Trunking with the Avaya Communication Server 1000 Release 7.5 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.5, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 4.0.5 with the TELUS system.

The TELUS offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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

Table of Contents

Table of Contents	2
1. Introduction.....	5
2. General Test Approach and Test Results.....	5
2.1. Interoperability Compliance Testing.....	5
2.2. Test Results	6
2.3. Support	7
3. Reference Configuration	8
4. Equipment and Software Validated	9
5. Configure Communication Server 1000	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)	12
5.2. Administer a Node IP Telephony	12
5.2.1. Obtain Node IP address	12
5.2.2. Administer Terminal Proxy Server (TPS)	15
5.2.3. Administer Quality of Service (QoS)	15
5.2.4. Synchronize the New Configuration.....	16
5.3. Administer Voice Codec	16
5.3.1. Enable Voice Codec G.729, G.711	16
5.3.2. Enable Voice Codec on Media Gateways.....	17
5.4. Zones and Bandwidth Management.....	17
5.4.1. Create a zone for IP phones (zone 10)	17
5.4.2. Create a zone for virtual SIP trunk (zone 255)	19
5.5. Administer SIP Trunk Gateway	19
5.5.1. Integrated Services Digital Network (ISDN).....	19
5.5.2. Administer SIP Trunk Gateway to Avaya SBCE	20
5.5.3. Administer Virtual D-Channel.....	22
5.5.4. Administer Virtual Super-Loop	25
5.5.5. Administer Virtual SIP Routes	26
5.5.6. Administer Virtual Trunks.....	28
5.5.7. Administer Calling Line Identification Entries.....	31
5.5.8. Enable External Trunk to Trunk Transferring	32
5.6. Administer Dialing Plans	33
5.6.1. Define ESN Access Codes and Parameters (ESN)	33
5.6.2. Associate NPA and SPN call to ESN Access Code 1	34

5.6.3.	Digit Manipulation Block (DMI).....	35
5.6.4.	Digit Manipulation Block (DMI) for Outbound Call	35
5.6.5.	Route List Block (RLB) (RLB 14)	36
5.6.6.	Route List Block (RLB) (RLB 15)	38
5.6.7.	Inbound Call – Incoming Digit Translation Configuration	38
5.6.8.	Outbound Call - Special Number Configuration	40
5.6.9.	Outbound Call - Numbering Plan Area (NPA).....	40
5.7.	Administer Phone.....	41
5.7.1.	Phone creation.....	41
5.7.2.	Enable Privacy for Phone.....	43
5.7.3.	Enable Call Forward for Phone.....	43
5.7.4.	Enable Call Waiting for Phone	46
6.	Configure Avaya SBCE.....	47
6.1.	Log in Avaya SBCE.....	47
6.2.	Global Profiles.....	48
6.2.1.	Configure Server Interworking - Avaya Side	48
6.2.2.	Configure Server Interworking – TELUS side	49
6.2.3.	Configure Routing – Avaya side.....	50
6.2.4.	Configure Routing - TELUS side	51
6.2.5.	Configure Server – Communication Server 1000.....	51
6.2.6.	Configure Server – TELUS ACME packet SBC.....	52
6.2.7.	Configure Topology Hiding – Avaya side.....	54
6.2.8.	Configure Topology Hiding – TELUS side.....	55
6.2.9.	Configure Signaling Manipulation	55
6.3.	Domain Policies	56
6.3.1.	Create Application Rules	56
6.3.2.	Create Border Rules	57
6.3.3.	Create Media Rules	58
6.3.4.	Create Security Rules.....	59
6.3.5.	Create Signaling Rules.....	60
6.3.6.	Create Time of Day Rules.....	62
6.3.7.	Create Endpoint Policy Groups	63
6.4.	Device Specific Settings.....	64
6.4.1.	Manage Network Settings.....	65
6.4.2.	Create Media Interfaces	66

6.4.3.	Create Signaling Interfaces	66
6.4.4.	Configuration Server Flows	67
7.	Verification Steps.....	68
7.1.	General	68
7.2.	Verification of an Active Call on Call Server	68
7.3.	Protocol Trace	70
8.	Conclusion	71
9.	Additional References.....	72

1. Introduction

These Application Notes illustrate a sample configuration using Communication Server 1000 Release 7.5, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 4.0.5 with the TELUS system. The TELUS Service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

2. General Test Approach and Test Results

The Communication Server 1000 connects to the Avaya SBCE using a SIP connection. Then the Avaya SBCE connects to the TELUS system using SIP signaling. Various call types were made from Communication Server 1000 to and from the TELUS system to verify the interoperability.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- General call processing between Communication Server 1000 and TELUS 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 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)
- TELUS Derived Voice (DV) Endpoints
- TELUS Mobility Endpoints

The following assumptions were made for this lab test configuration:

1. Communication Server 1000 R7.5 software and implementation of latest patches
2. TELUS 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 messages that may indicate technical issues. This refers to 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 **Section 2.1** were verified. All the applicable test cases were executed. However, the following observations were noted during the compliance testing:

1. 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.
2. 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 Communication Server 1000, but the PSTN-to-SIP gateway that TELUS uses for this Interop testing does not support the UPDATE. In order to make the blind transfer work, make sure to enable plug-in 501 on Communication Server 1000 to allow blind transfer to work without the UPDATE method. The limitation of this plug-in is that no ring-back tone is provided to the originator of the call for the duration that the destination set is ringing.
3. Calls that are redirected on the Communication Server 1000 require a SIP Diversion header to be added so the calls can be handled properly on the TELUS network. The Diversion header is needed to fix billing situations within the TELUS network on the NSN HiQ where calls are forwarded or transferred to external sets. The NSN HiQ requires Diversion headers if the outgoing call contains a different number in the From and PAI headers, which is the case on redirected calls. The Diversion header ensures that

the proper party is billed for the call. The Communication Server 1000 does not support Diversion headers. In order to provide this functionality, the Avaya Session Border Controller will extract the user and host information from the History-Info header and create a Diversion header (Refer to section 6.2.9)

4. The TELUS network does not support SIP History-Info headers as these headers are primarily used for inter-SIP PBX communication. Instead, the TELUS network requires that a SIP P-Asserted-Identity header be sent for redirected calls. The Communication Server 1000 accomplishes this by using the Avaya SBCE to extract the user and host information from the History Info and create P-Asserted-Identity header (Refer to section 6.2.9)

It was agreed with TELUS 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 TELUS system, please contact TELUS technical support at:

<http://www.TELUS.com>

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between Communication Server 1000 and TELUS 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.

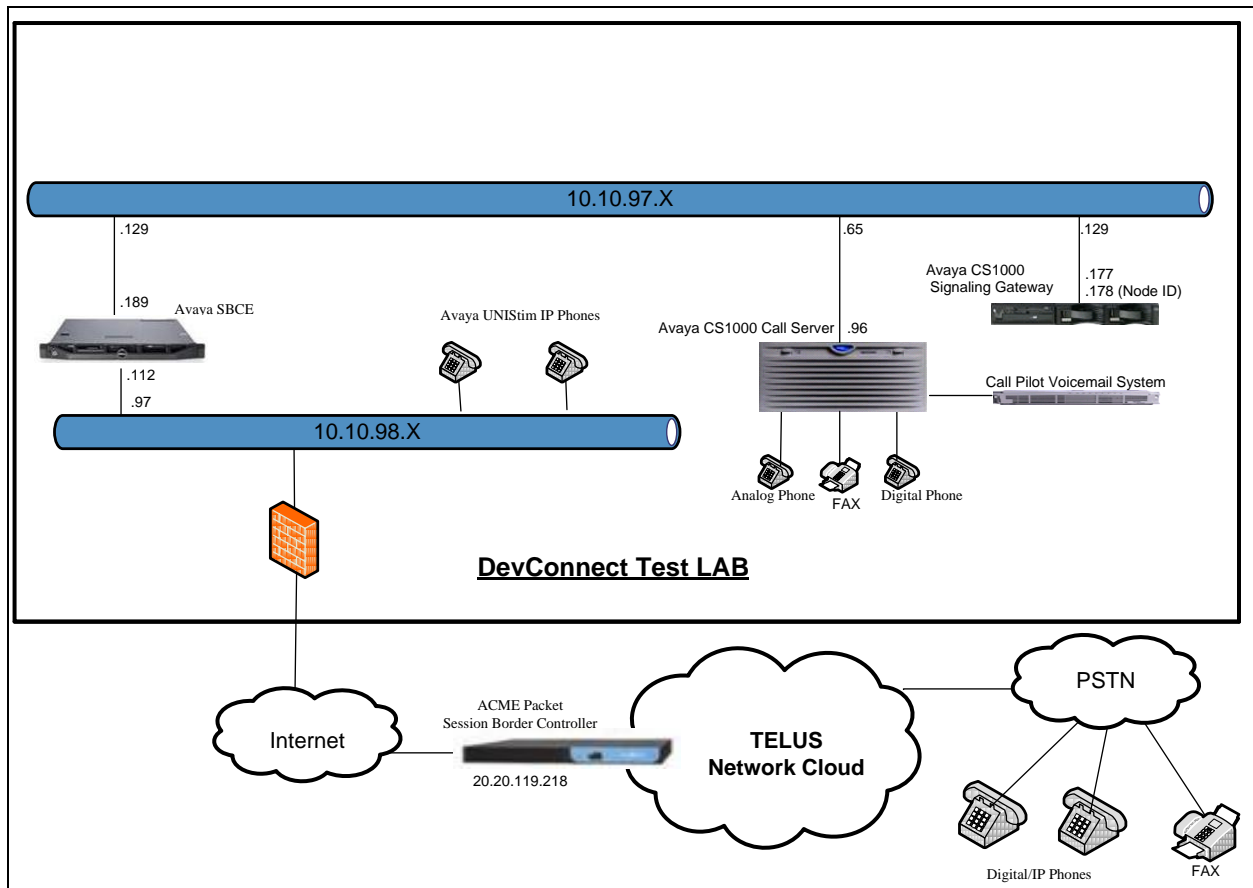


Figure 1- Network diagram for Avaya and TELUS Systems

4. Equipment and Software Validated

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

Avaya system:

System	Software
Avaya Communication Server 1000 (CPPM)	Call Server: 750 Q+ GA Signaling Server: 7.50.17 GA SIP Line Server: 7.50.17 GA
Avaya Session Border Controller for Enterprise	4.0.5 Q09
Avaya UNISTim Phone	2002 p2: 0604DCN 1140: 0625C8D 1120: 0624C8D 2007: 0621C8D
Avaya 3904 Digital Phone	N/A
Analog Phone	N/A
HP Officejet 4500 Fax	N/A

TELUS system:

System	Software
Acme Packet Net-Net 4250 Session Border Controller	6.1m7p5
Nokia Siemens Networks HiQ 4200	Version 14.0

Additional software and patch lineup for the configuration and active patch list 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_20120713.ntl

Avaya SBCE: 4.0.5 Q09 plus the patch - HistInfo-mvista-load-Q09.rpm

5. Configure Communication Server 1000

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 Communication Server 1000, over the TELUS SIP trunk to PSTN.

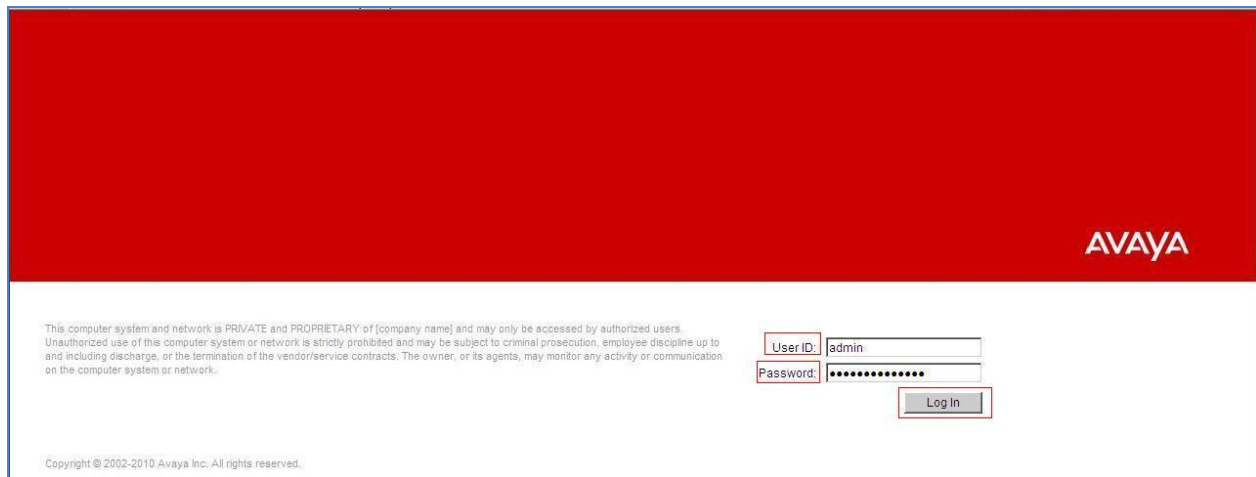
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult the references in **Section 9**.

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

5.1. Log in to Communication Server 1000 System

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

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**.



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.

User ID: admin

Password:

Log In

Copyright © 2002-2010 Avaya Inc. All rights reserved.

Figure 2 – Login Unified Communications Management

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

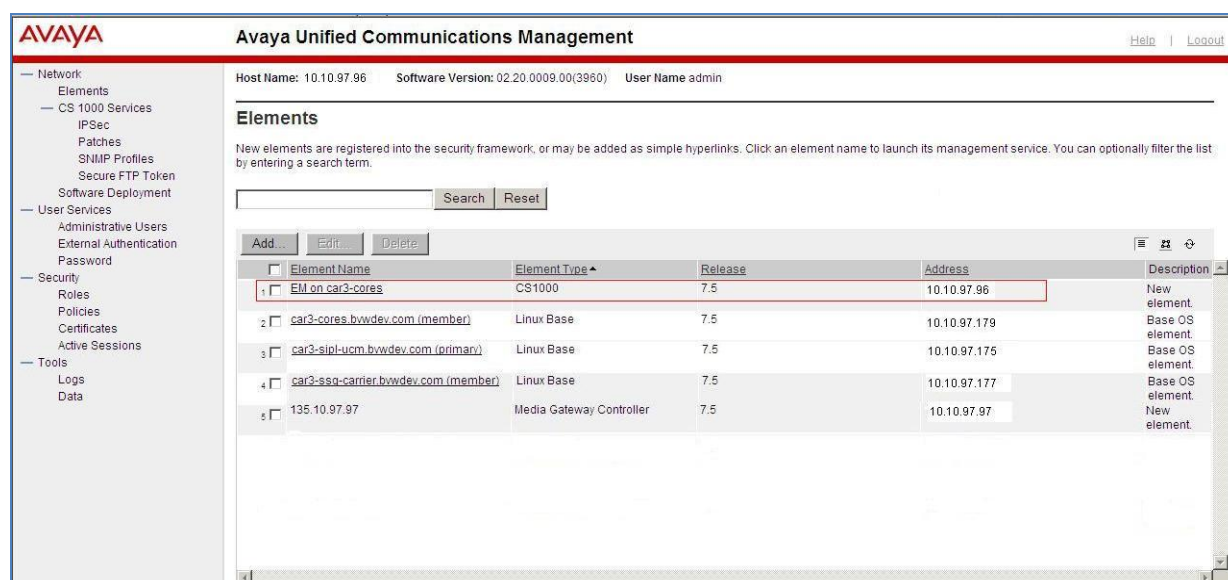


Figure 3 – Unified Communications Management

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+

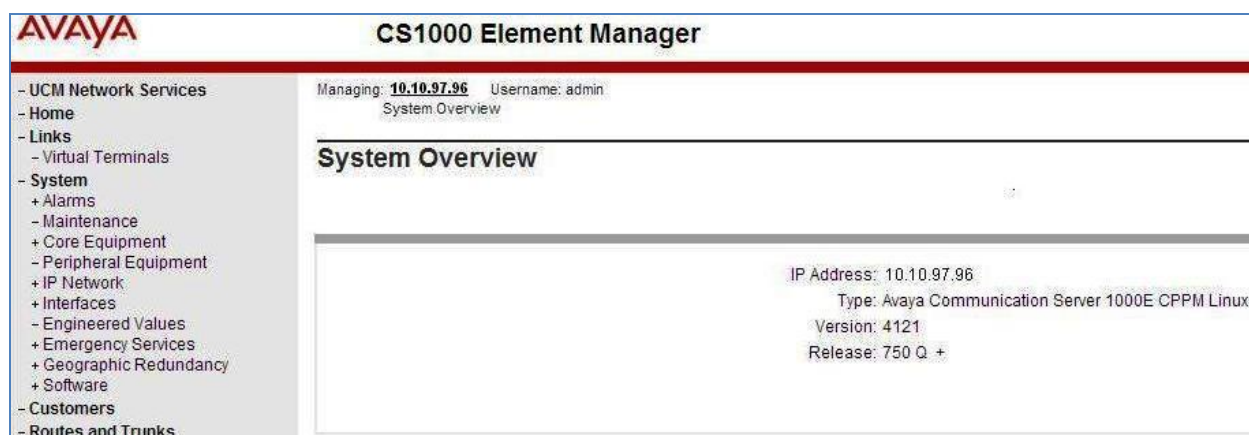


Figure 4 – Element Manager System Overview

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: Wed August 22 11:42:05 2012 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 11:43 08/22/2012
```

```
>
```

5.2. Administer an IP Telephony Node

This section describes how to configure an IP Telephony Node 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 TELUS system. For further information on Avaya Communications Server 1000, please consult the references in **Section 9**.

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

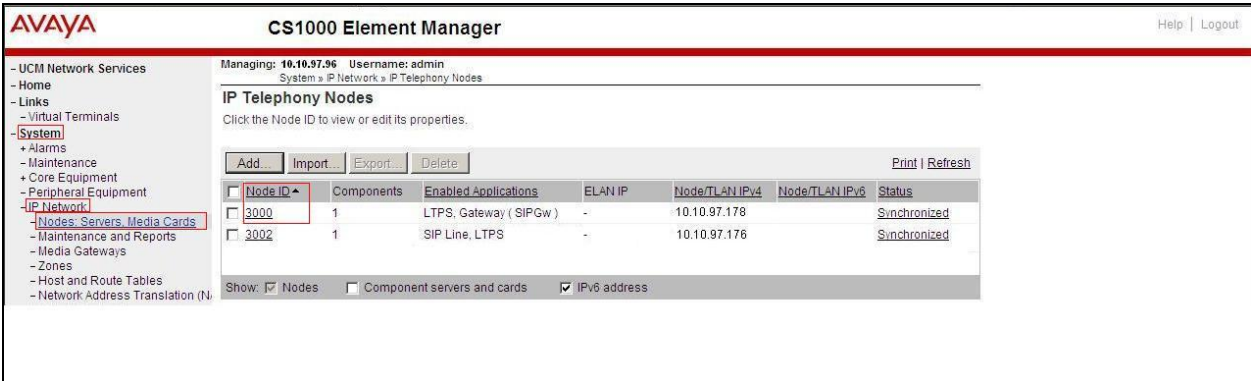


Figure 5 – IP Telephony Nodes

The **Node Details** screen is displayed in **Figure 6** and **Figure 7** with the IP address of the Communication Server 1000 node. The **Node IPv4 Address 10.10.97.178** is a virtual address which corresponds to the TLAN IP address **10.10.97.177** of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP Address to communicate with other components to process the SIP call.

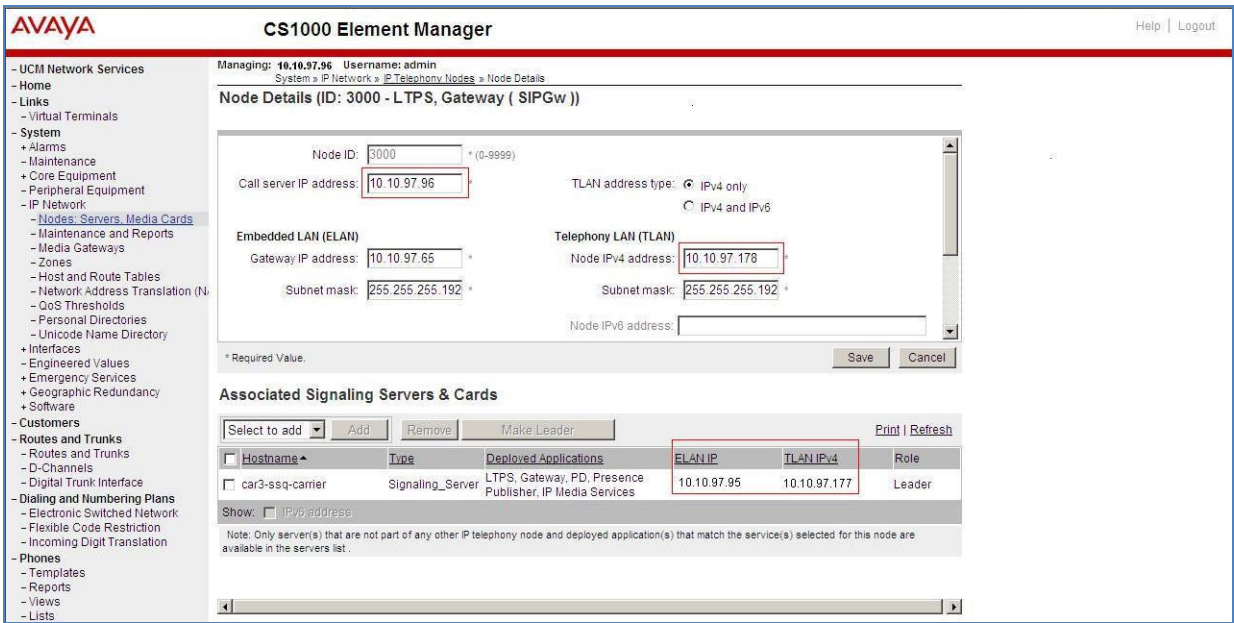


Figure 6 –Node Details

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 (V/GW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

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

* Required Value.

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)

Continue from **Section 5.2.1**. On the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 7**.

Check the **UNISlim Line Terminal Proxy Server** check box to enable proxy service on this node and then click the **Save** button as shown in **Figure 8**.

The screenshot displays the 'UNISlim Line Terminal Proxy Server (LTPS) Configuration Details' for Node ID: 3000. The interface includes a left-hand navigation menu with categories like UCM Network Services, Links, System, and Customers. The main content area shows configuration options for the LTPS. The 'Enable proxy service on this node' checkbox is checked. The 'Firmware' section contains fields for IP address (0.0.0.0), Full file path (download/firmwa), and Server Account/User ID. The 'DTLS' section shows the DTLS policy set to 'Off' and options for Client authentication and Periodic re-keying. The 'Network Connect Server' section is empty. A 'Save' button is highlighted at the bottom right.

Figure 8 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

Continue from **Section 5.2.1**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 7**.

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

The screenshot displays the 'Quality of Service (QoS)' configuration details for Node ID: 3000. The interface includes a left-hand navigation menu with categories like UCM Network Services, Links, System, and Customers. The main content area shows configuration options for QoS. The 'Enable Avaya automatic QoS' checkbox is unchecked. The 'DiffServ Codepoint (DSCP)' section shows Control packets: 40 (0-63), Voice packets: 40 (0-63), and 802.1Q bits value (802.1P): 5 (0-7). A 'Save' button is highlighted at the bottom right.

Figure 9 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

Continue from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button.

The **Node Saved** screen is displayed. Click on **Transfer Now** (not shown).

The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box and click on **Start Sync** (not shown).

When the synchronization completes, check the Signaling Server check box and click on **Restart Applications** (not shown).

5.3. Administer Voice Codec

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

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 TELUS system supports **G.711/time 20ms** and **G.729/time 20ms** with **VAD** unchecked. 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, System, Interfaces, and Customers. 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 codes. The first code is 'Codec G711: [x] Enabled (required)'. Below it, 'Voice payload size' is set to '20' (milliseconds per frame). 'Voice playback (jitter buffer) delay' is set to '40' (Nominal) and '80' (Maximum) milliseconds. There is a note: 'Maximum delay may be automatically adjusted based on nominal settings.' Below this, 'Voice Activity Detection (VAD)' is unchecked. The second code is 'Codec G722: [] Enabled', with 'Voice payload size' set to '20' ms. The third code is 'Codec G729: [x] Enabled', with 'Voice payload size' set to '20' ms. At the bottom, there is a 'Save' button and a 'Cancel' button. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

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 **G.711** and **Codec G.729** and uncheck **VAD** as shown in **Figure 11**.

Scroll down to the bottom of the page and click on the **Save** button (not shown)

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like 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 (selected), 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, and Login Options. The main content area is titled 'VGW and IP phone codec profile'. It contains a list of settings for the 'G.711' codec, which is currently selected. The settings include checkboxes for 'Enable echo canceller', 'Enable dynamic attenuation', 'R factor calculation', 'DTMF tone detection', 'Enable low latency mode', 'Remove DTMF delay (squell DTMF from TDM to IP)', 'Enable modem/fax pass through mode', 'Enable V.21 FAX tone detection', and 'VAD' (which is unchecked). There are also input fields for 'Echo canceller tail delay' (128 ms), 'Voice activity detection threshold' (1), 'Idle noise level' (0), 'Fax TCF method' (2), 'Fax maximum rate' (9600 bps), 'FAX playback nominal delay' (100 ms), 'FAX no activity timeout' (20 ms), 'FAX packet size' (30), 'Voice payload size' (20 ms/frame), 'Voice playback (jitter buffer) nominal delay' (40 ms), and 'Voice playback (jitter buffer) maximum delay' (80 ms). Below the 'G.711' section, the 'G.729A' section is also visible, showing 'Codec name G729A' and 'Voice payload size' (20 ms/frame). The bottom of the page shows the copyright notice: 'Copyright © 2002-2011 Avaya Inc. All rights reserved.'

Figure 11 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

This section describes the steps to create 2 zones: zone 10 for VGW and IP phones, 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 phones for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.

Select **IP Network** → **Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown in **Figure 12**.

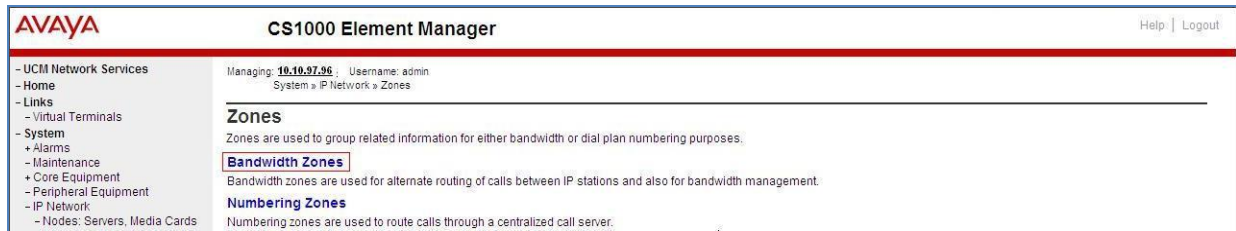


Figure 12 – Zones Page

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

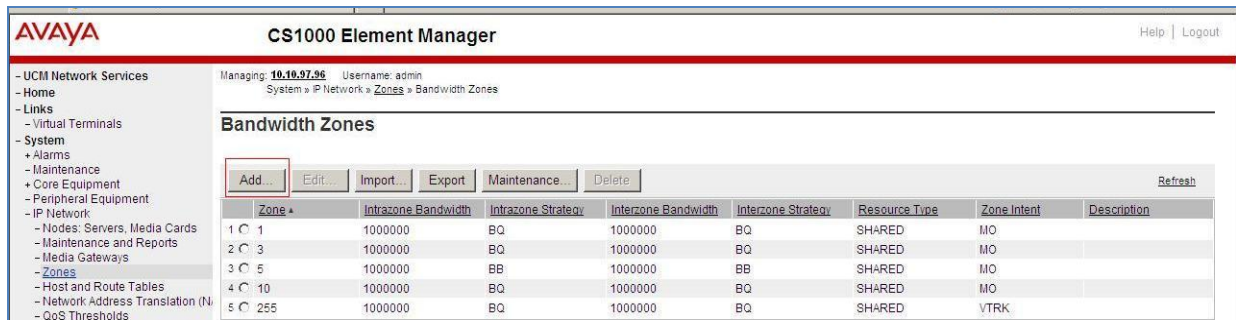


Figure 13 – Bandwidth Zones

- 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 and VTRK: is used for virtual trunk.

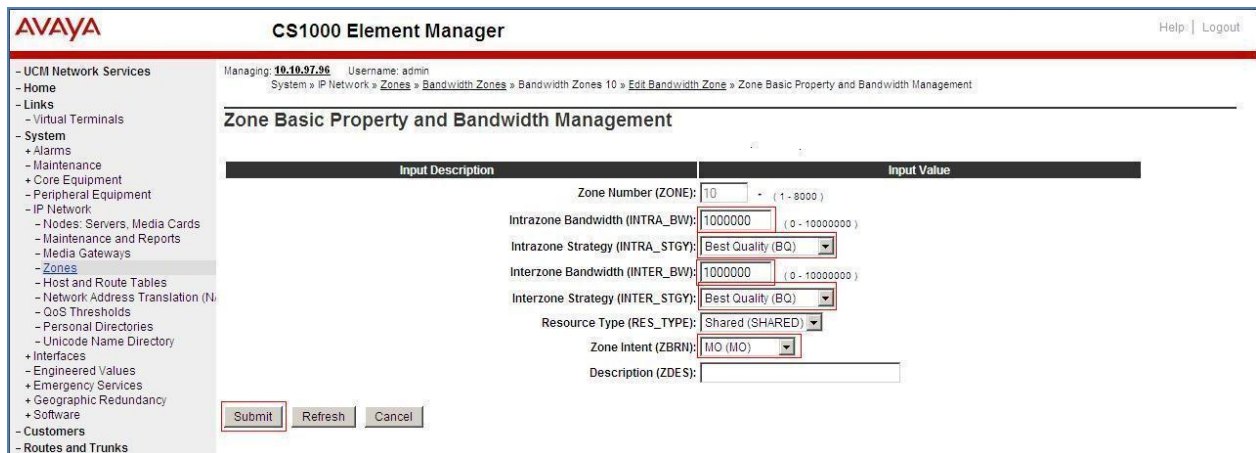


Figure 14 –Bandwidth Management Configuration Details – IP phone

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

Follow **Section 5.4.1** to create a zone for the virtual trunk. The difference is in **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk as shown in **Figure 15** and then click on the **Submit** button.

The screenshot shows the 'Zone Basic Property and Bandwidth Management' page in the CS1000 Element Manager. The left sidebar contains a tree view with categories like UCM Network Services, Links, System, and Customers. The main area displays configuration fields for Zone 255. The 'Zone Number (ZONE)' is set to 255. 'Intrazone Bandwidth (INTRA_BW)' and 'Interzone Bandwidth (INTER_BW)' are both set to 1000000. 'Intrazone Strategy (INTRA_STGY)' and 'Interzone Strategy (INTER_STGY)' are both set to 'Best Quality (BQ)'. 'Resource Type (RES_TYPE)' is set to 'Shared (SHARED)'. 'Zone Intent (ZBRN)' is set to 'VTRK (VTRK)'. The 'Description (ZDES)' field is empty. At the bottom, there are 'Submit', 'Refresh', and 'Cancel' buttons.

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):	

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 Session Border Controller For Enterprise.

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 to list all feature packages (not shown). Select **Integrated Services Digital Network** to edit its parameters (not all parameters shown in **Figure 16** below). 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).

The screenshot shows the 'Integrated Services Digital Network' configuration page for Package 145. The left sidebar is the same as in Figure 15. The main area displays configuration fields for the ISDN. The 'Integrated Services Digital Network' checkbox is checked. 'Virtual private network identifier' is set to 1. 'Private network identifier' is set to 1. 'Node DN' is empty. 'Multi-location business group' is set to 0. 'Business sub group consult-only' is set to 65535. At the bottom, there are 'Submit', 'Refresh', and 'Cancel' buttons.

Integrated Services Digital Network:	<input checked="" type="checkbox"/>
Virtual private network identifier:	1 (1 - 10383)
Private network identifier:	1 (1 - 10383)
Node DN:	
Multi-location business group:	0 (0 - 65535)
Business sub group consult-only:	65535 (0 - 65535)

Figure 16 –Customer – ISDN Configuration

5.5.2. Administer SIP Trunk Gateway to Avaya SBCE

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 the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 17**. The parameters (highlighted in red boxes) are filled in.

The screenshot shows the Avaya CS1000 Element Manager interface. The left pane contains a navigation tree with categories like UCM Network Services, System, and Customers. The main pane displays the 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details' screen. The 'General' tab is active, showing fields for 'Vtrk gateway application' (SIP Gateway (SIPGw)), 'SIP domain name' (bwdev7.com), 'Local SIP port' (5060), 'Gateway endpoint name' (car3-ssg-carrier), 'Gateway password', 'Application node ID' (3000), and 'Enable failsafe NRS'. The 'Virtual Trunk Network Health Monitor' section is also visible, with a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor addresses'. The 'SIP ANAT' is set to IPv4. The bottom of the screen shows a note: 'Changes made on this page will NOT be transmitted until the Node is also saved.' and 'Save' and 'Cancel' buttons.

Figure 17 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 18**. Enter **Primary TLAN IP address** as the IP address of Avaya SBCE internal interface. Enter **Port: 5060** and **Transport protocol: UDP**. Uncheck **Support registration**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like 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, and Dialing and Numbering Plans. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. It has tabs for 'General', 'SIP Gateway Settings', and 'SIP Gateway Services'. The 'SIP Gateway Settings' tab is selected, showing the 'Proxy Or Redirect Server' configuration. Under 'Proxy Server Route 1:', there are fields for 'Primary TLAN IP address' (10.10.97.189), 'Port' (5060), and 'Transport protocol' (UDP). Below these are checkboxes for 'Support registration' (unchecked) and 'Primary CDS proxy' (unchecked). A 'Secondary TLAN IP address' field is also present with a value of 0.0.0.0. At the bottom, there are 'Save' and 'Cancel' buttons, and a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

Figure 18 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 18**, scroll down the parameters box to the **SIP URI Map** section.

Under the **Public E.164 Domain Names**, for:

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

Under the **Private domain names**, for:

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

The remaining fields can be left at their default values as shown in **Figure 19**. Then click on the **Save** button.

Figure 19 – Virtual Trunk Gateway Configuration Details

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

5.5.3. Administer Virtual D-Channel

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 and type DCH as shown in **Figure 20**. Click the **to Add** button.

Figure 20 – D-Channels

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
- **User:** Integrated Services Signaling Link Dedicated (ISLD)
- **Interface type for D-channel (IFC):** Meridian Meridian1 (SL1)
- **Meridian 1 node type:** Slave to the controller (USR)
- **Release ID of the switch at the far end (RLS):** 25

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.

AVAYA CS1000 Element Manager

Help | Logout

- Basic Configuration

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

Submit Refresh Delete Cancel

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

Figure 21 – D-Channels Configuration Details

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

- Basic options (BSCOPT)

Action Device And Number (ADAN): DCH

D channel Card Type: DCIP

Designator: VoIP

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (ISLD)

Interface type for D-channel: Meridian Meridian1 (SL1)

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRI loop number:

Primary Rate Interface: more PRI

Secondary PRI2 loops:

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

Release ID of the switch at the far end: 25

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

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

Signalling server resource capacity: 1800 Range: 0 - 3700

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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

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

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

- Remote Capabilities: Edit

- B channel Service messaging: ☐

+ 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 (DV1)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3)	<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 MSML 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

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

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

5.5.4. Administer Virtual Super-Loop

Select **System** → **Core 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

[Add](#) [Delete](#) [Refresh](#)

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

Figure 24 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

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**.

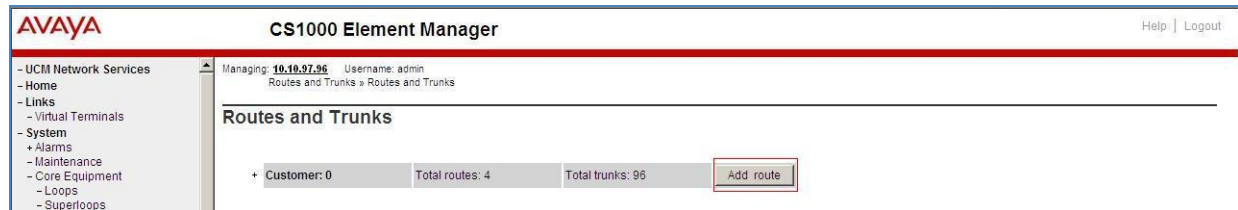


Figure 25 – Add route

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 (example: route 100).
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk Type (TKTP):** TIE trunk data block (TIE)
- **Incoming and Outgoing trunk (ICOG):** Incoming and Outgoing (IAO)
- **Access Code for the trunk route (ACOD):** An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 5.4.2**).
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number 3000 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
 - **Mode of operation (MODE):** Route uses ISDN Signalling Link (ISLD)
 - **D channel number (DCH):** D-Channel number 100 (created in **Section 5.5.3**)
 - **Network calling name allowed (NCNA):** Check the field.
 - **Network call redirection (NCRD):** Check the field.
 - **Insert ESN access code (INAC):** Check the field.

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.10.97.36** 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): ☒

- 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 DT12 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**.
- Click on the **Submit** button

AVAYA CS1000 Element Manager

Help | Logout

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

- Basic Route Options

Attendant announcement (ATAN): No Attendant Announcement (NO)
 Billing number required (BLN): ☐
 Call detail recording (CDR): ☒
 - CDR records generated on incoming calls (INC): ☒
 - CDR record printing content option for redirected calls (LAST): ☒
 - Time to answer output in CDR (TTA): ☐
 - CDR ACD Q initial connection records to be generated (QREC): ☒
 - CDR on outgoing calls (OAL): ☒
 - CDR on outgoing toll calls (OTL): ☐
 - Answered call identification allowed (ALA): ☒
 - 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

5.5.6. Administer Virtual Trunks

From the EM, select **Routes and Trunks** → **Route and Trunks** (not shown). The Route list is now updated with the newly added route. In the example, the Route 100 was added. Click on the **Add trunk** button as shown in **Figure 28**.

AVAYA CS1000 Element Manager

Help | Logout

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

Routes and Trunks

Customer	Route	Type	Description	Actions
0				Add route
11		TIE	SIPL	Edit Add trunk
100		TIE	100	Edit Add trunk

Figure 28 – Route and Trunks Page

The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service**

(CLS) at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 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

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin

Routes and Trunks » Routes and Trunks » Customer 0, Route 100, Trunk 1 Property Configuration

Customer 0, Route 100, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

+ Advanced Trunk Configurations

Figure 29 – New Trunk Configuration Details

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)

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

Return Class of Service Cancel

Figure 30 – Class of Service Configuration Details Page

5.5.7. Administer Calling Line Identification Entries

Select **Customers** → **00** → **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in **Figure 31**

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin

Customers > Customer 00 > Customer Details > ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code: (0 - 9999)

Code for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks

☒ Connection of supervised external trunks

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-DID users: ☐ Coordinated dialing plan

☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Size: (0 - 4000)

Country code: (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Figure 31 – ISDN and ESN Networking

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

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin

Customers > Customer 00 > Customer Details > ISDN and ESN Networking > Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range:

End range:

End range should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add Delete

Refresh

Figure 32 – Calling Line Identification Entries

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

- **National Code:** input prefix digits assigned by Service Provider, in this case it is 3 digits – 403.

- **Local Code:** input prefix digits assigned by Service Provider, in this case it is 3 digits – 692. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 403692. 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 - 403692. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Calling Party Name Display:** Uncheck for **Roman characters**.

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

AVAYA CS1000 Element Manager Help | Logout

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

Edit Calling Line Identification 0

General Properties

National Code: 403 (0 - 999999)
Code for national home number

Local Code: 692 (1-12 digits)
Code for home local number or listed DN

Home Location Code: 403692 (1-7 digits)

Local Steering Code: 403692 (1-7 digits)

Use DN as DID: YES

Emergency Services Access

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

Emergency Options: ☐ Home national number for emergency services access calls
☒ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☐

CPND Name: (first name, last name)

Expected Length: (dropdown menu)

Display Format: First name, Last name (dropdown menu)

Save Cancel

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.

- Login Call Server Overlay CLI (please refer to **Section 5.1.2** for more detail).
- 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)

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**.

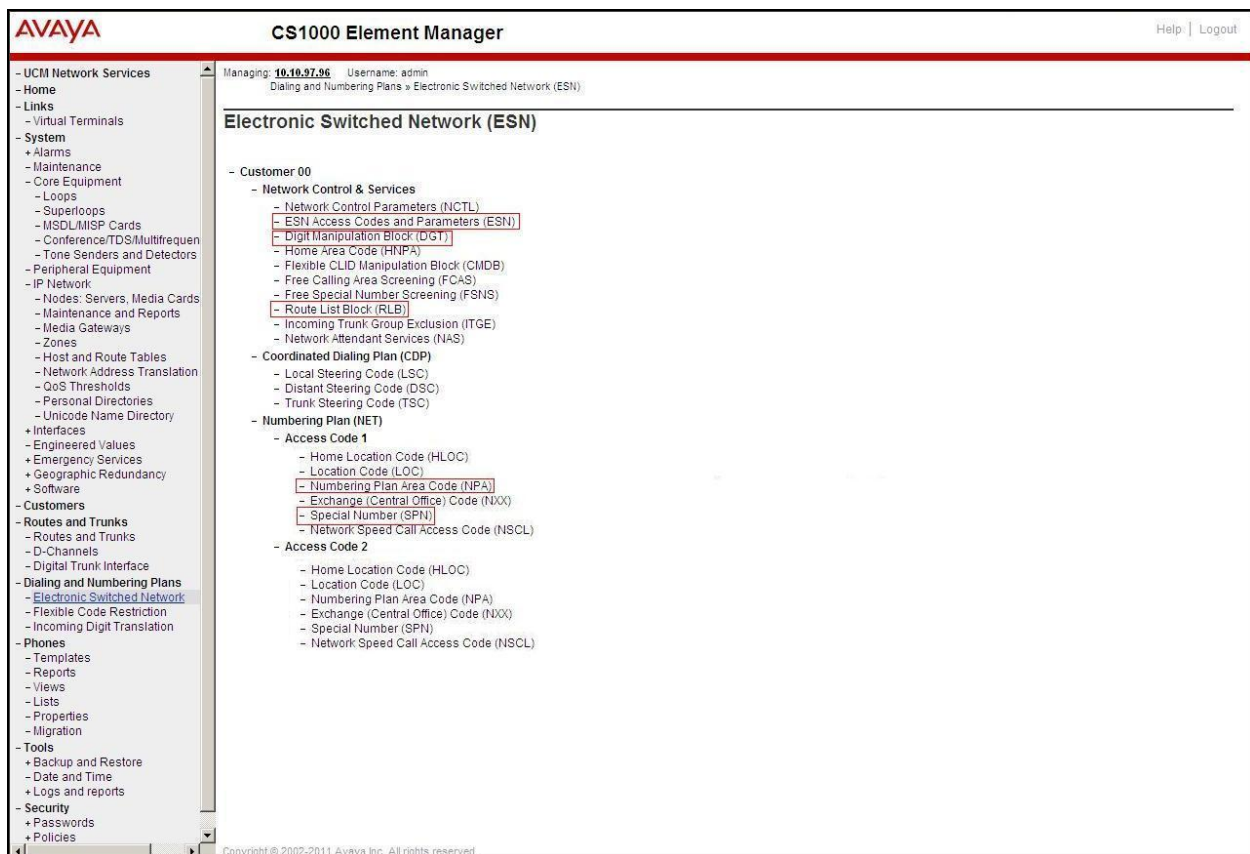


Figure 34 –ESN Configuration Details

In the **ESN Access Codes and Basic Parameters** page, define **NARS Access Code 1** as shown in **Figure 35**.
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 1

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
AC2 xNPA xSPN   ----- > (Set NPA, SPN not to associate to ESN Access Code 2)
FNP
CLID
...
```

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

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1 INTL NPA SPN NXX LOC ----- > (NPA, SPN are associated to ESN Access Code 1)
AC2
FNP YES
...
```

5.6.3. Digit Manipulation Block (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 **Figure 37, Figure 38**).

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)**.

In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click on **to Add** button as shown in **Figure 36**.



Figure 36 – Add a DMI

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**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with categories like 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, and Zones. The main content area is titled 'Digit Manipulation Block' and contains the following fields:

- Digit Manipulation Index numbers: 14
- Number of leading digits to be deleted: 0 (0 - 19)
- Insert: [Empty text box]
- IP Special Number: [Empty checkbox]
- Call Type to be used by the manipulated digits: NPA (NPA)

At the bottom right of the main content area, there are four buttons: Submit, Refresh, Delete, and Cancel. The Submit button is highlighted with a red box.

Figure 37 – DMI_14 Configuration Details

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**.

The screenshot shows the AVAYA CS1000 Element Manager interface, similar to Figure 37. The left sidebar and main content area are the same. The configuration fields for DMI_15 are:

- Digit Manipulation Index numbers: 15
- Number of leading digits to be deleted: 1 (0 - 19)
- Insert: [Empty text box]
- IP Special Number: [Empty checkbox]
- Call Type to be used by the manipulated digits: NPA (NPA)

At the bottom right of the main content area, there are four buttons: Submit, Refresh, Delete, and Cancel. The Submit button is highlighted with a red box.

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**. 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**.

Select an available value in the textbox for the **route list index** (in this case is 14) and click on **Add** button as shown in **Figure 39**.

Figure 39 – Add a Route List Block.

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)

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**.

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**.

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**)

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left-hand navigation pane shows a tree structure with categories like 'UCM Network Services', 'Links', 'System', 'Interfaces', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' as the selected option. The main content area is titled 'Data Entry of a Route List Block' and shows the configuration for 'Route List Block Index: 15'. The 'General Properties' section includes a text box for 'Entry Number for the Route List' set to 0. The 'Indexes' section contains several dropdown menus and checkboxes: 'Time of Day Schedule' (0), 'Facility Restriction Level' (0), 'Digit Manipulation Index' (15), 'ISL D-Channel Down Digit Manipulation Index' (0), 'Free Calling Area Screening Index' (0), 'Free Special Number Screening Index' (0), 'Business Network Extension Route' (unchecked), and 'Incoming CLID Table' (0). The 'Options' section includes checkboxes for 'Local Termination entry' (unchecked), 'Skip Conventional Signaling' (unchecked), 'Use Tone Detector' (unchecked), 'Conversion to LDN' (unchecked), 'Expensive Route' (unchecked), 'Strategy on Congestion' (No Reroute (NRR)), 'QSIG Alternate Routing Causes' (QSIG Alternate Routing Cause 1), 'Preferred Routing' (Preferred Route 1), 'ISDN Drop Back Busy' (Drop Back Disabled (DBD)), 'ISDN Off-Hook Queuing Option' (unchecked), and 'Off-Hook Queuing Allowed' (unchecked). The bottom of the page shows a copyright notice: 'Copyright © 2002-2011 Avaya Inc. All rights reserved.'

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 TELUS system. 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**.

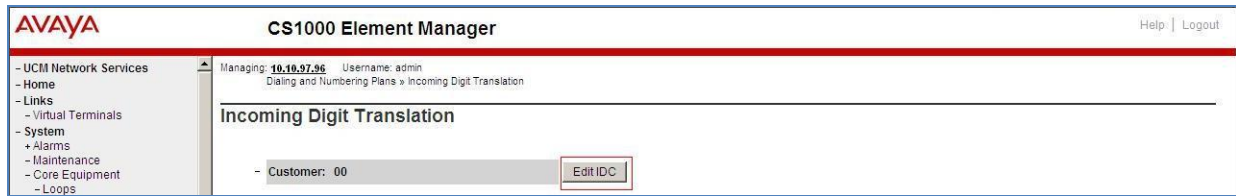


Figure 42 – Incoming Digit Translation

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

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 **DCNO** 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 403692xxxx will be translated to DN xxxx. The DID number 4036929470 is translated to 1700 for Voicemail accessing purpose.

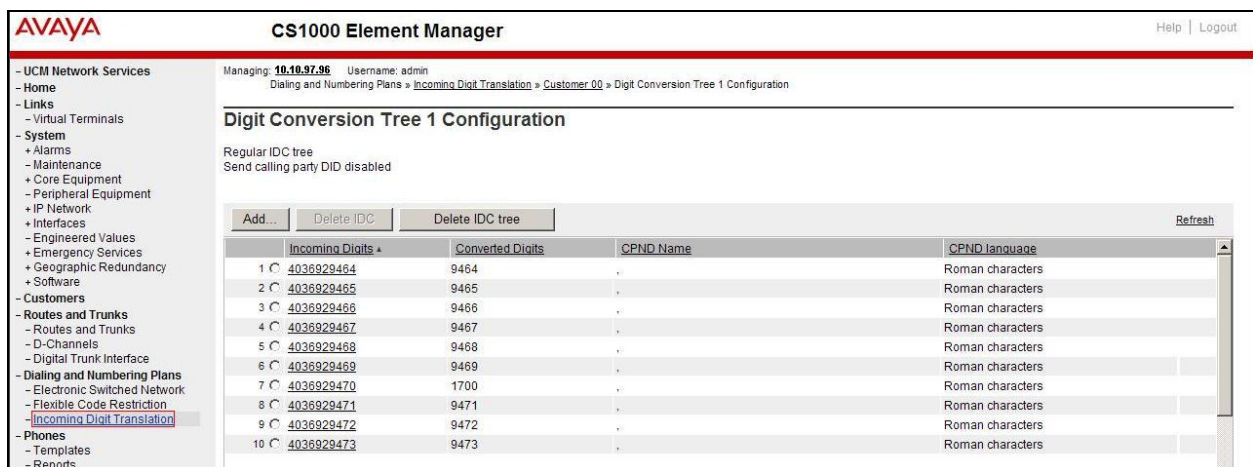


Figure 44 – Digit Conversion Tree

5.6.8. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 011, 411, 911 and so on.

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**.

Enter SPN number and then click on **to Add** button. **Figure 45** shows all the special number used for this testing.

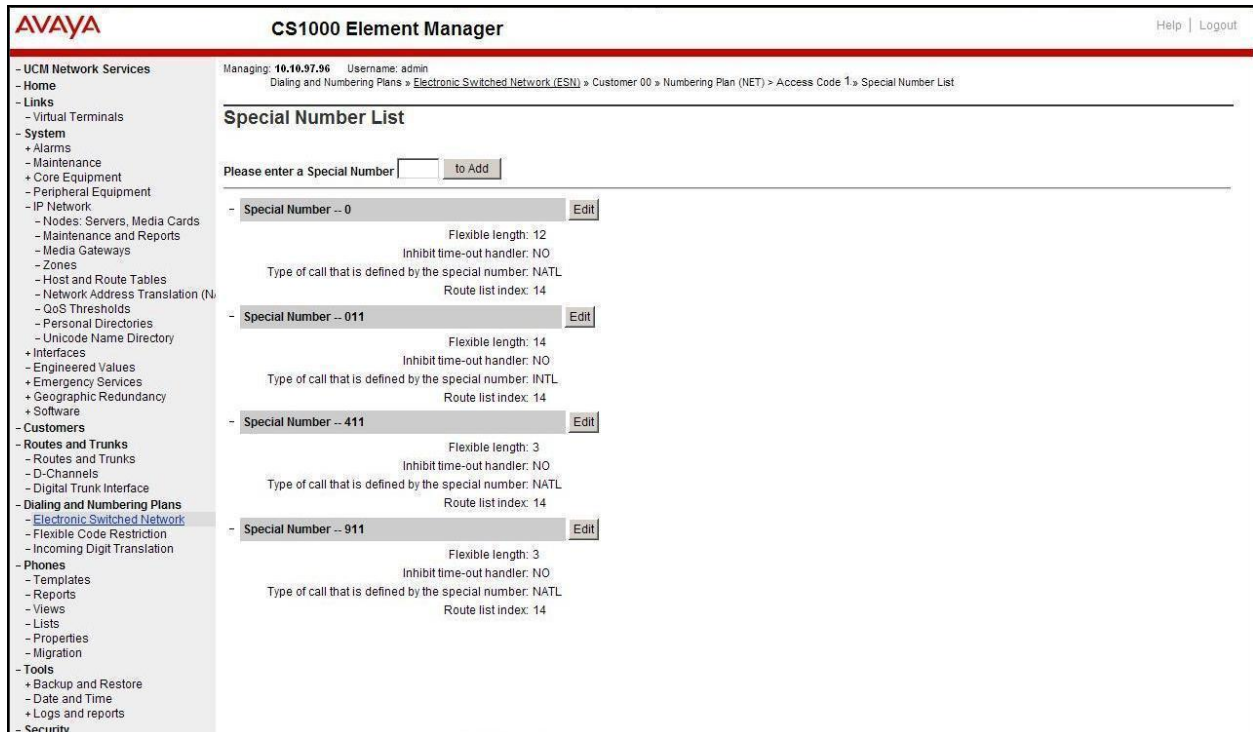


Figure 45 – Add a SPN.

5.6.9. Outbound Call - Numbering Plan Area (NPA)

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

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 1403, 1416, 1604, 1613, 1647, 1780 and 1800 area codes were used in this configuration as shown in **Figure 46**.

AVAYA

CS1000 Element Manager

[Help](#) | [Logout](#)

- 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

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

Numbering Plan Area Code List

Please enter an area code to Add

- Numbering Plan Area Code -- 1403	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1416	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1604	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1613	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1647	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1780	Edit
Route List Index: 14	
Incoming Trunk group Exclusion Index: NONE	
- Numbering Plan Area Code -- 1800	Edit
Route List Index: 14	
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 phones.

Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phones.

Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail).

Create an IP phone by using **LD 11**.

```

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 HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
 DRDD EXR0
 USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
 FSD 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 9464 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.

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
...
```

To allow the 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. 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**
- Click **Save** to save the configuration.

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: ☐

Save Cancel

Figure 47 – Call Redirection

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 616139675205.

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

DES 2007
TN 96 0 00 04 VIRTUAL
TYPE 2007
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
```

```
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDA CDMA LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXA ARHD CLTD ASCD
```

```
...
19 CFW 16 616139675205
```

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 **HUNT**. Following is the configuration of a phone has **CFB** enabled with forward number is 616139675205.

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

DES 2007
TN 96 0 00 04 VIRTUAL
TYPE 2007
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
...
FDN 616139675205
HUNT 616139675205
```

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 616139675205.

```
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 616139675205
HUNT 616139675205
```

```

...
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 the Call Waiting feature at the phone level.

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail), configure the Call Waiting feature for the 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 9464 0  MARP
  CPND
  CPND_LANG ROMAN
  NAME Carrier1
  XPLN 13
  DISPLAY_FMT FIRST, LAST
    01 WT
...

```


6. Configure Avaya SBCE

This section describes the configuration of the Avaya SBCE necessary for interoperability with TELUS systems.

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

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 9** of these Application Notes.

6.1. Log in Avaya SBCE

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

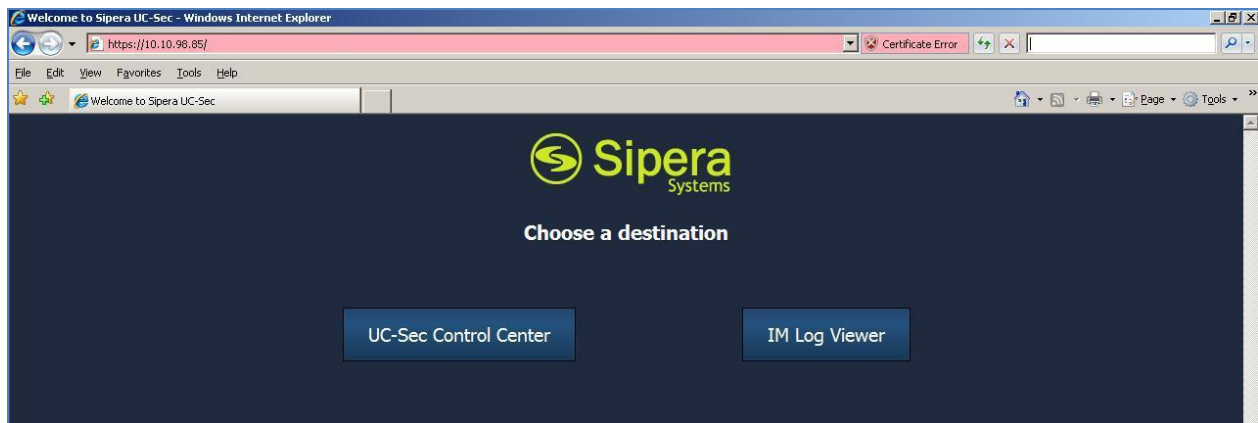
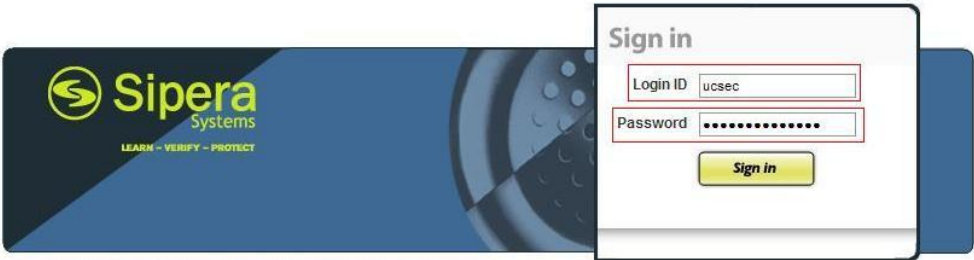


Figure 48: Avaya SBCE Web Interface

Select **UC-Sec Control Center** and enter the **Login ID** and **Password**



The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

Figure 49: Avaya SBCE Login

6.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

6.2.1. Configure Server Interworking - Avaya Side

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

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

Select **Add Profile**, enter **Profile name** as **CS1K_Car3**.

- Check **Hold Support** as **RFC2543**.
- Check **Diversion Header Support** as **Yes**.
- All other options on the General Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs, all options can be left at default. Click Finish (not shown).

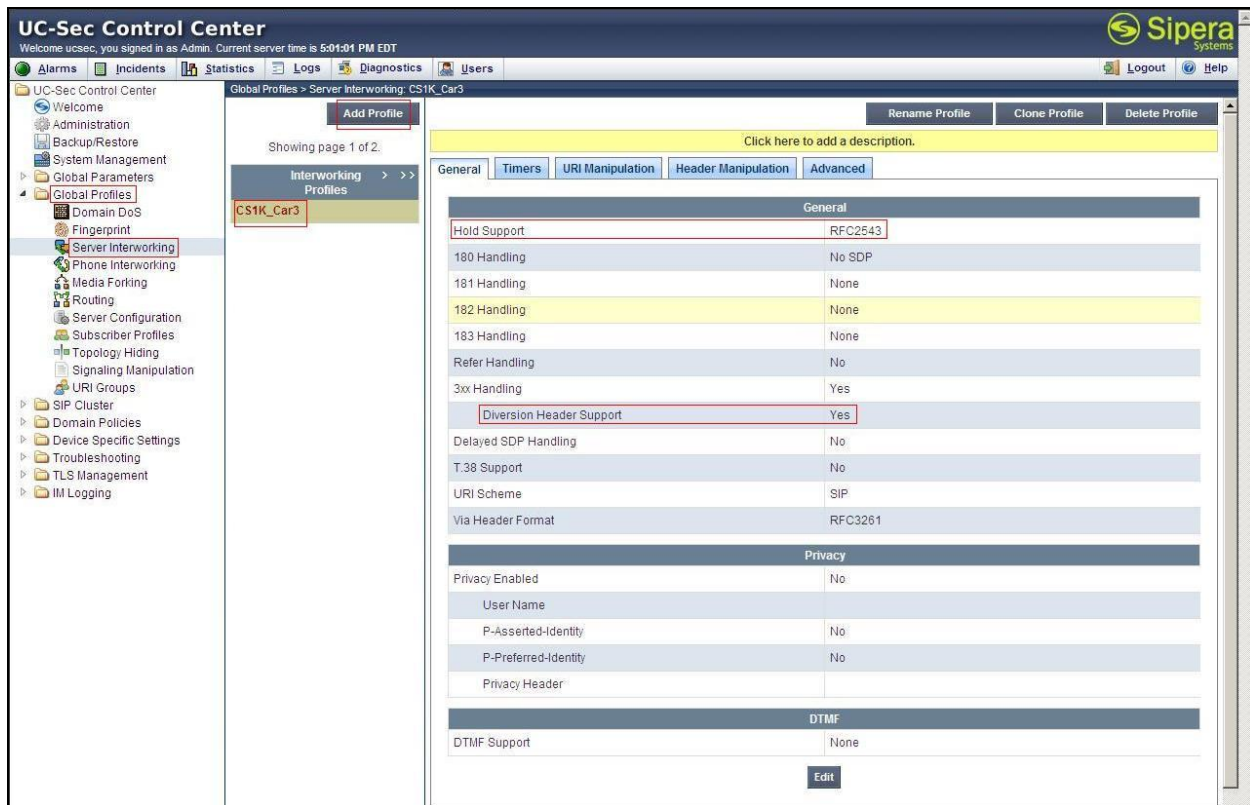


Figure 50: Server Interworking – Avaya Side

6.2.2. Configure Server Interworking – TELUS side

From the menu on the left-hand side, select **Global Profiles** → **Server Internetworking**. Select **Add Profile**, enter **Profile name** as **TELUS**.

- Check **Hold Support** as **RFC2543**.
- Check **Diversion Header Support** as **Yes**.
- All other options on the General Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs, all options can be left at default. Click Finish (not shown).

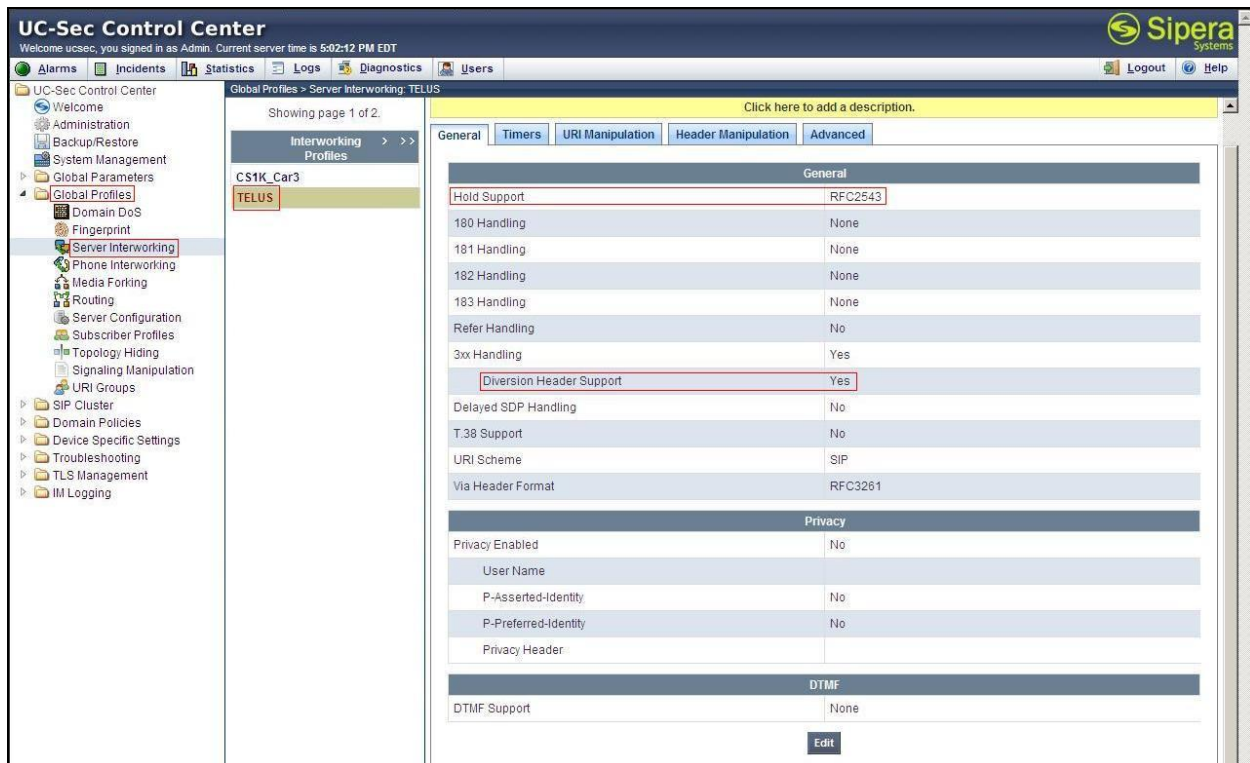


Figure 51: Server Interworking – TELUS Side

6.2.3. Configure Routing – Avaya side

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

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

Select **Add Profile**, enter Profile Name: **TELUS_To_CS1K75**.

- **URI Group: ***
- **Next Hop Server 1: 10.10.97.178 (Communication Server IP address)**
- **Check Next Hop Priority.**
- **Outgoing Transport: UDP**
- **Click Finish (not shown).**



Figure 52: Routing To Avaya

6.2.4. Configure Routing - TELUS side

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

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

Select **Add Profile**, enter Profile Name: **CS1K75_To_TELUS**.

- **URI Group: ***
- **Next Hop Server 1: 20.20.119.218** (IP Address provided by Customer)
- Check **Next Hop Priority**
- **Outgoing Transport as UDP**
- Click Finish (not shown)



Figure 53: Routing To TELUS

6.2.5. Configure Server – Communication Server 1000

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

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

Select **Add Profile**, enter Profile Name as **CS1K_Car3**.

On General tab (**Figure 54**):

- Select **Server Type: Call Server**

- **IP Address: 10.10.97.178 (Communication Server IP Address)**
- **Supported Transports: Check UDP**
- **UDP Port: 5060**



Figure 54: Communication Server Configuration 1

- On the **Advanced** Tab (Figure 55), select **CS1K_Car3** for **Interworking Profile**.
- Click **Finish** (not shown).



Figure 55: Communication Server Configuration 2

6.2.6. Configure Server – TELUS ACME packet SBC

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

Select **Add Profile**, enter Profile Name as **TELUS**.

On General tab (Figure 56):

- Select **Server Type: Trunk Server**
- **IP Address: 20.20.119.218 (TELUS Trunk Server)**
- **Supported Transports: Check UDP**
- **UDP Port: 5060**



Figure 56: TELUS Server Configuration

On the **Advanced** Tab (Figure 57):

- Select **TELUS** for **Interworking Profile**
- Select **Signaling Manipulation Script: For TELUS**



Figure 57: TELUS Server Advanced Configuration

On the **Heartbeat** Tab (Figure 58):

- Check on **Enable Heartbeat**.
- Select **Method** as **OPTIONS** (TELUS requires).
- **Frequency:** 60 seconds
- **From URI:** ping@bvwddev7.com
- **To URI:** ping@20.20.119.218
- Check **TCP Probe**, **TCP Probe Frequency:** 10 seconds
- Click **Finish** (not shown).

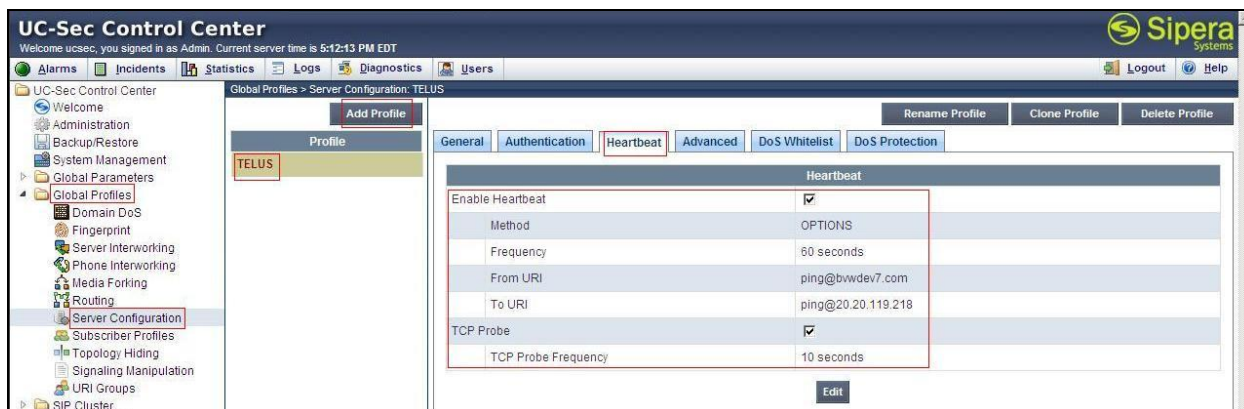


Figure 58: TELUS Server Heartbeat Configuration

6.2.7. Configure Topology Hiding – Avaya side

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

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

Select **Add Profile**, enter Profile Name as **TELUS_To_CS1K75**.

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



Figure 59: Topology Hiding Communication Server

6.2.8. Configure Topology Hiding – TELUS side

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.
Select **Add Profile**, enter Profile Name as **CS1K75_To_TELUS**.

- For the Header **To**,
 - In the **Criteria** column, select **IP/Domain**.
 - In the **Replace Action** column, select **Overwrite**.
 - In the **Overwrite Value** column, select **20.20.119.218**.
- For the Header **Request-Line**,
 - In the **Criteria** column, select **IP/Domain**.
 - In the **Replace Action** column, select **Overwrite**.
 - In the **Overwrite Value** column, select **20.20.119.218**.



Figure 60: Topology Hiding TELUS

6.2.9. Configure Signaling Manipulation

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

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

Enter script Title: **For TELUS**

- Edit the script as shown in **Figure 61**
 - To replace the Request Line sip:domain from the body in the SIP message
 - To create Diversion Header using History Info Header information
 - To replace information of PAI field by information of History Info field
 - To remove History Info
- Click Save (not shown).

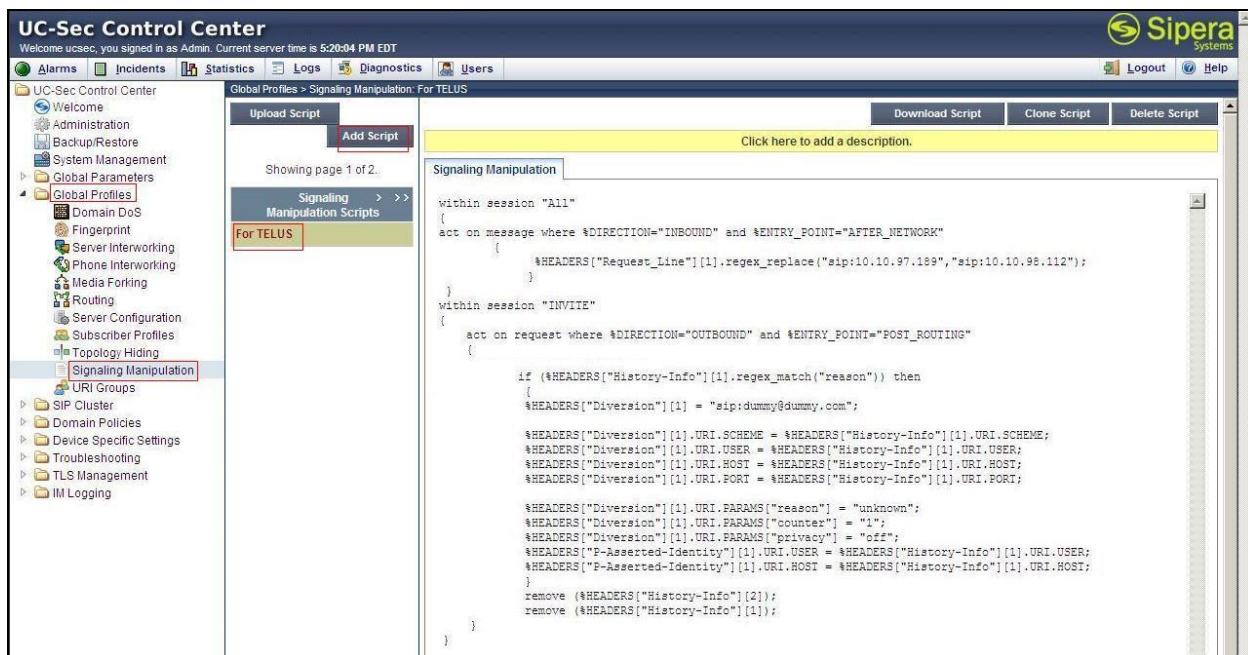


Figure 61: Signaling Manipulation

6.3. Domain Policies

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

6.3.1. Create Application Rules

Application Rules allow you to define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions your network will process in order to prevent resource exhaustion.

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

- Select the **default** rule.
- Select **Clone Rule** button.
 - Name: **CS1K_Car3_AppR**
 - Click Finish (not shown).

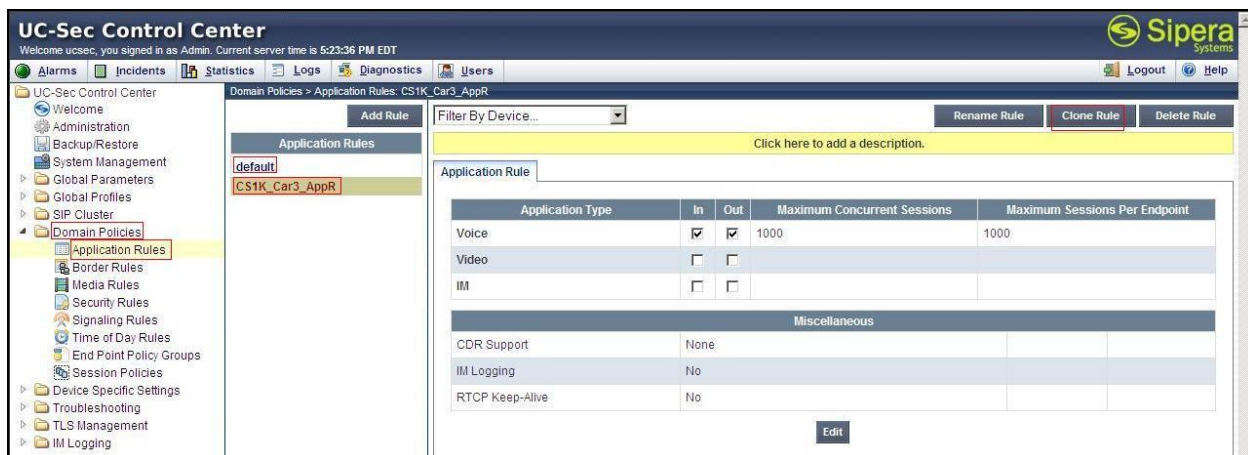


Figure 62: Communication Server Application Rule

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

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

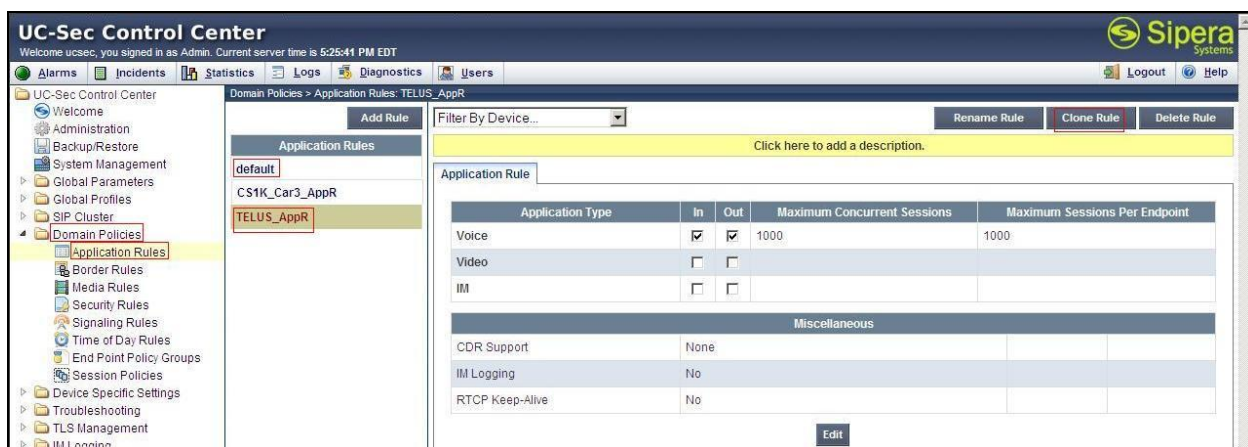


Figure 63: TELUS Application Rule

6.3.2. Create Border Rules

Border Rules allow you control NAT Traversal. The NAT Traversal feature allows you to determine whether or not call flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

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

- Select the **default** rule.
- Select **Clone Rule** button.
 - Enter Clone Name: **CS1K_Car3_BorderR**

- Click Finish (not shown).



Figure 64: Communication Server Border Rule

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

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

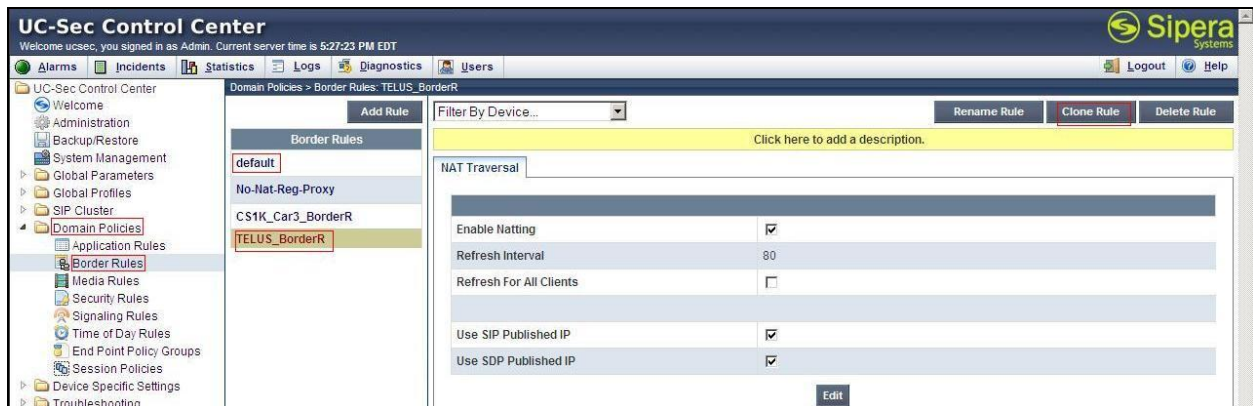


Figure 65: TELUS Border Rule

6.3.3. Create Media Rules

Media Rules allow you to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the UC-Sec security product.

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

- Select the **default-low-med** rule.
- Select **Clone Rule** button.

- Enter Clone Name: **CS1K_Car3_MediaR**
- Click Finish (not shown).



Figure 66: Communication Server Media Rule

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

- Select the **default-low-med** rule.
- Select **Clone Rule** button.
 - Enter Clone Name: **TELUS_MediaR**
 - Click Finish (not shown).



Figure 67: TELUS Media Rule

6.3.4. Create Security Rules

Security Rules allow you to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows you to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, you can also define the security feature profile so that the feature is applied in a specific manner to a specific situation.

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

- Select the **default-med** rule.
- Select **Clone Rule** button.
 - Enter Clone Name: **CS1K_Car3_SecurityR**
 - Click Finish (not shown).



Figure 68: Communication Server Security Rule

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

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



Figure 69: TELUS Security Rule

6.3.5. Create Signaling Rules

Signaling Rules allow you to define the action to be taken (*Allow*, *Block*, *Block with Response*, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching

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

- Select the **default** rule.
- Select **Clone Rule** button.
 - Enter Clone Name: **CS1K_Car3_SigR**
 - Click Finish (not shown).

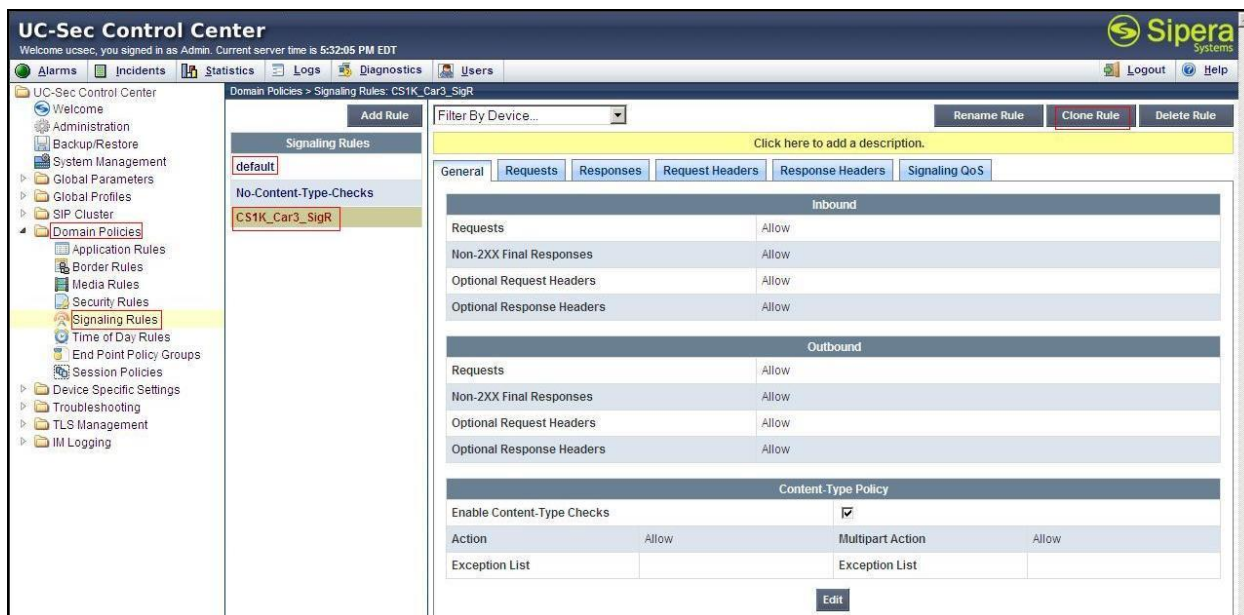


Figure 70: Communication Server Signaling Rule

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

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

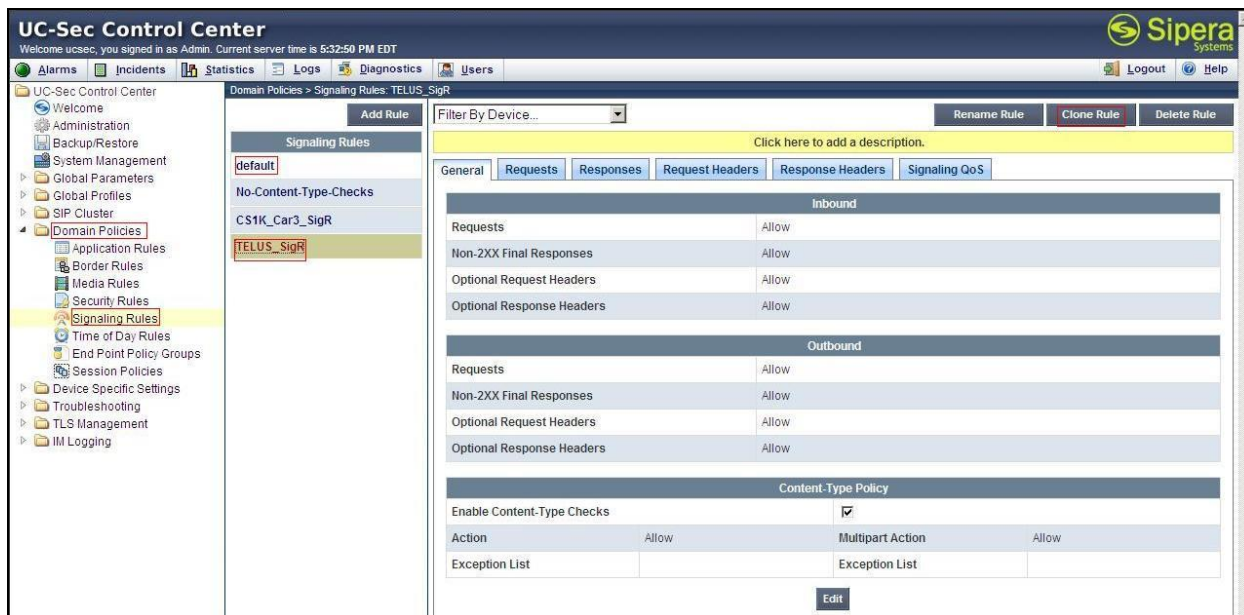


Figure 71: TELUS Signaling Rule 1

6.3.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows you to determine when the domain policy it is assigned to will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect

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

- Select the **default** rule.
- Select **Clone Rule** button.
 - Enter Clone Name: **CS1K_Car3_ToDR**
 - Click Finish (not shown).

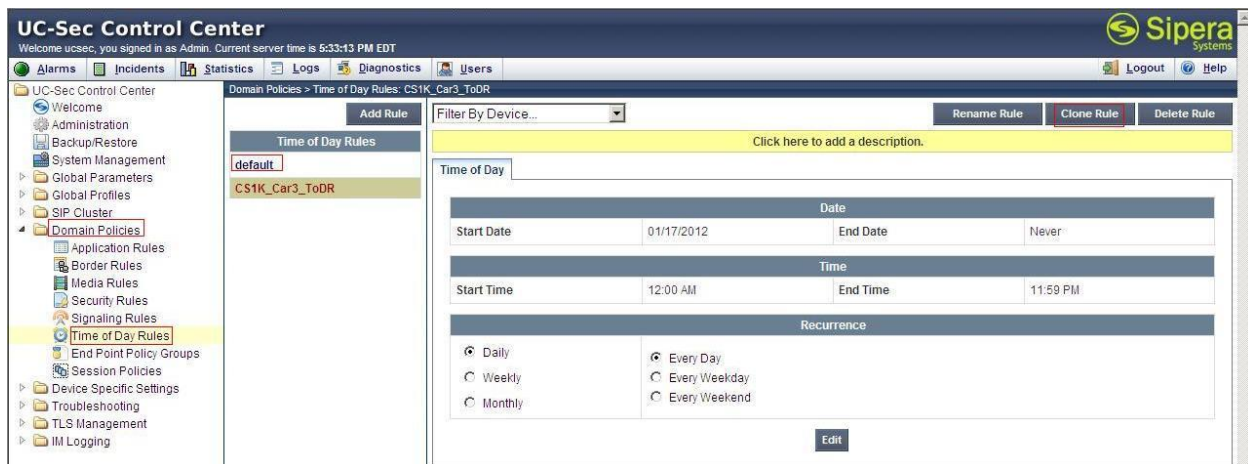


Figure 72: Communication Server Time of Day Rule

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

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

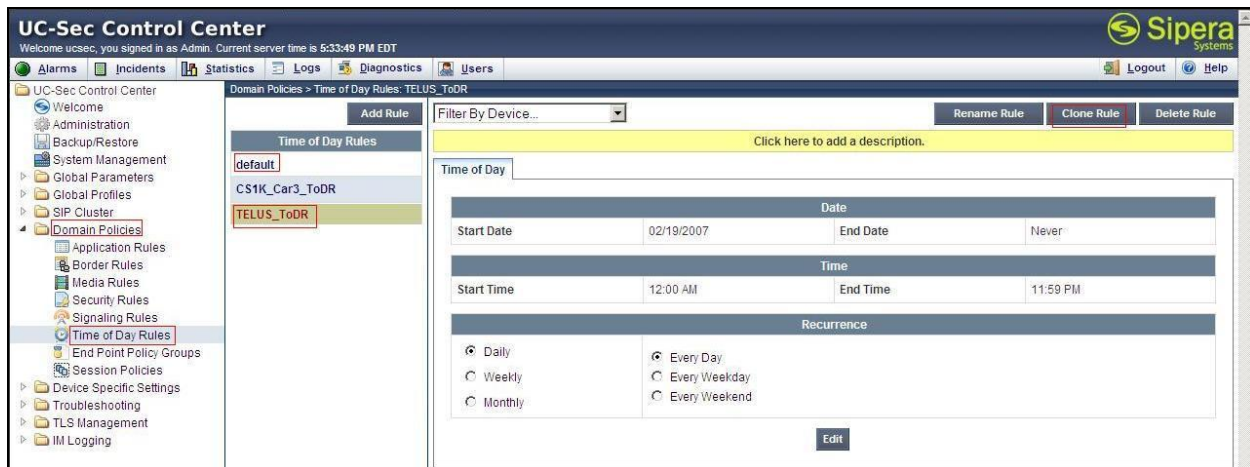


Figure 73: TELUS Time of Day Rule

6.3.7. Create Endpoint Policy Groups

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

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

- Select **Add Group**.
- Enter **Group Name: CS1K_Car3_PolicyG**
 - **Application Rule: CS1K_Car3_AppR**
 - **Border Rule: CS1K_Car3_BorderR**
 - **Media Rule: CS1K_Car3_MediaR**
 - **Security Rule: CS1K_Car3_SecurityR**
 - **Signaling Rule: CS1K_Car3_SigR**
 - **Time of Day: CS1K_Car3_ToDR**
- Select **Finish** (not shown).

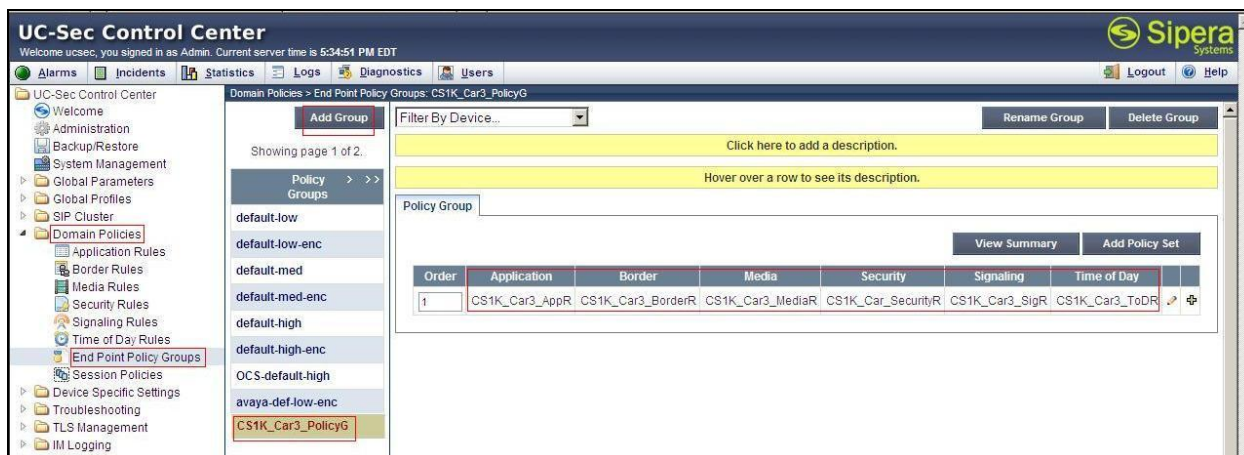


Figure 74: Communication Server End Point Policy Group

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

- Select **Add Group**.
- Enter **Group Name: TELUS_PolicyG**
 - **Application Rule: TELUS_AppR**
 - **Border Rule: TELUS_BorderR**
 - **Media Rule: TELUS_MediaR**
 - **Security Rule: TELUS_SecurityR**
 - **Signaling Rule: TELUS_SigR**
 - **Time of Day: TELUS_ToDR**
- Select **Finish** (not shown).

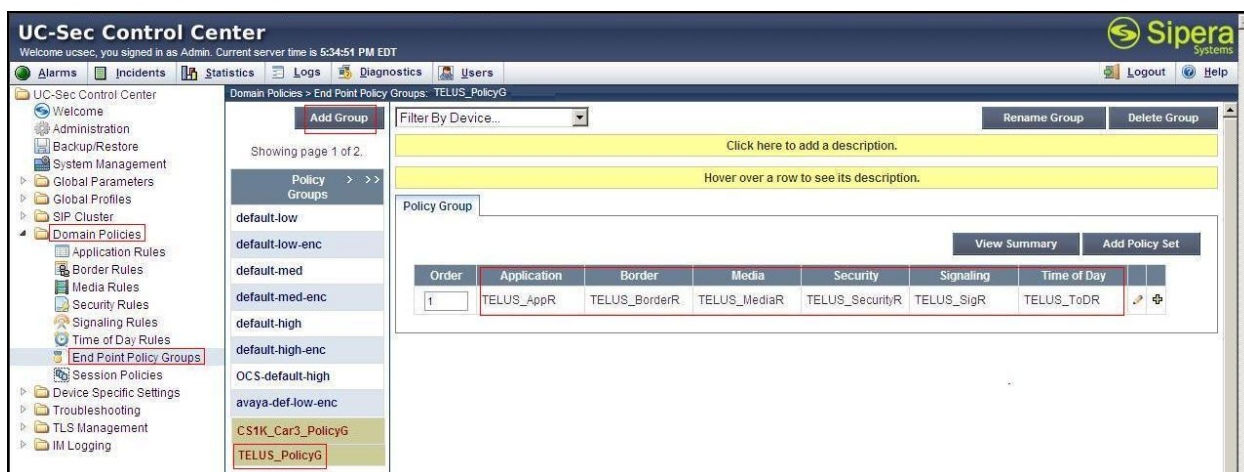


Figure 75: TELUS End Point Policy Group

6.4. Device Specific Settings

The Device Specific Settings feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will

function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, endpoint and session call flows and Network Management.

6.4.1. Manage Network Settings

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

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
 - **IP Address for Inside interface: 10.10.97.189; Gateway: 10.10.97.129**
 - **IP Address for Outside interface: 10.10.98.112; Gateway: 10.10.98.97**
- Select the physical interface used in the **Interface** column:
 - **Inside Interface: A1**
 - **Outside Interface: B1**

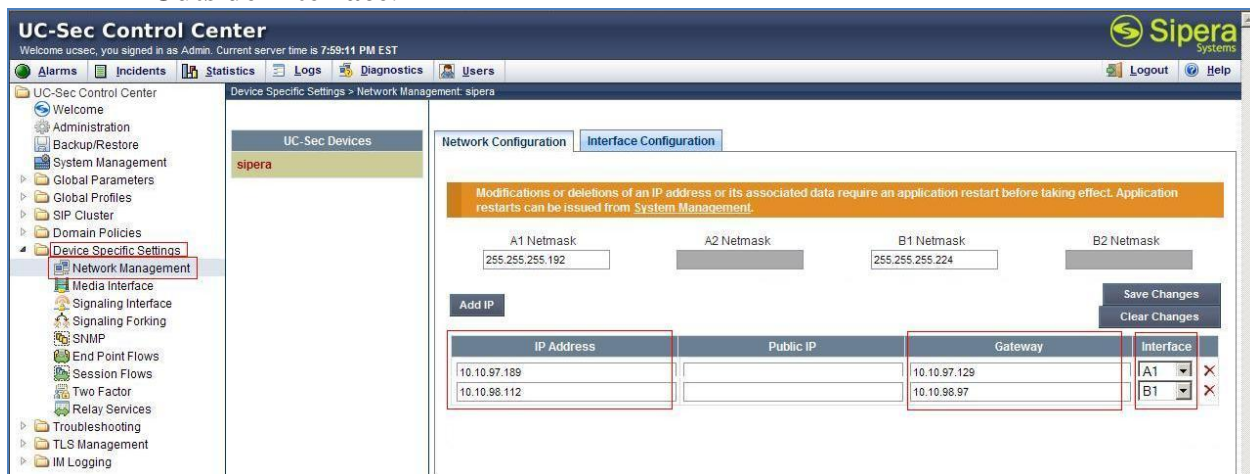


Figure 76: Network Management

- Select the **Interface Configuration** Tab.
- Enable the physical interfaces being used by clicking the **Toggle State** button.

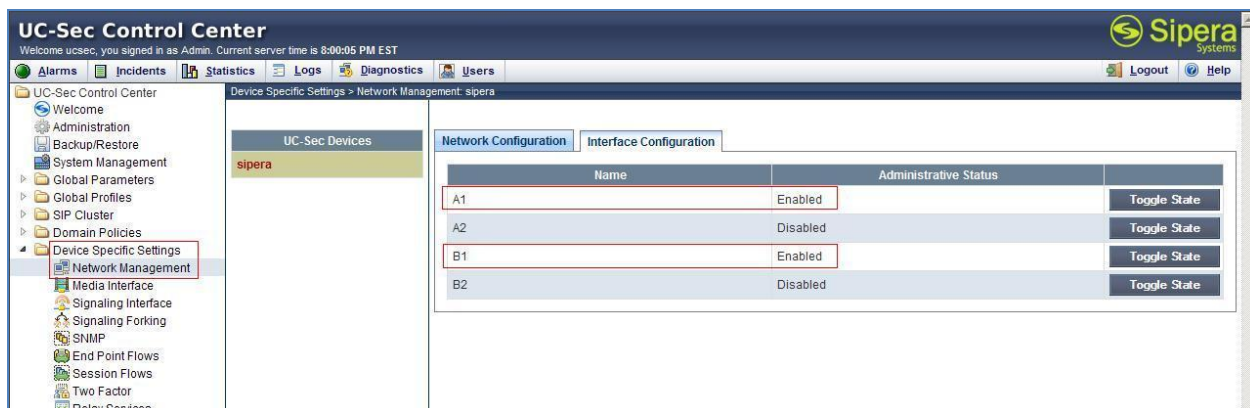


Figure 77: Network Interface Status

6.4.2. Create Media Interfaces

Media Interfaces (**Figure 78**) define the type of signaling on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

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

- Select **Add Media Interface**.
 - **Name: InsideMedia**
 - **Media IP: 10.10.97.189** (Internal Address toward **Communication Server**)
 - **Port Range: 35000 - 40000**
 - Click Finish (not shown).
- Select **Add Media Interface**.
 - **Name: OutsideMedia_SBCE**
 - **Media IP: 10.10.98.112** (External Internet Address toward TELUS trunk)
 - **Port Range: 35000 - 40000**
 - Click Finish (not shown).

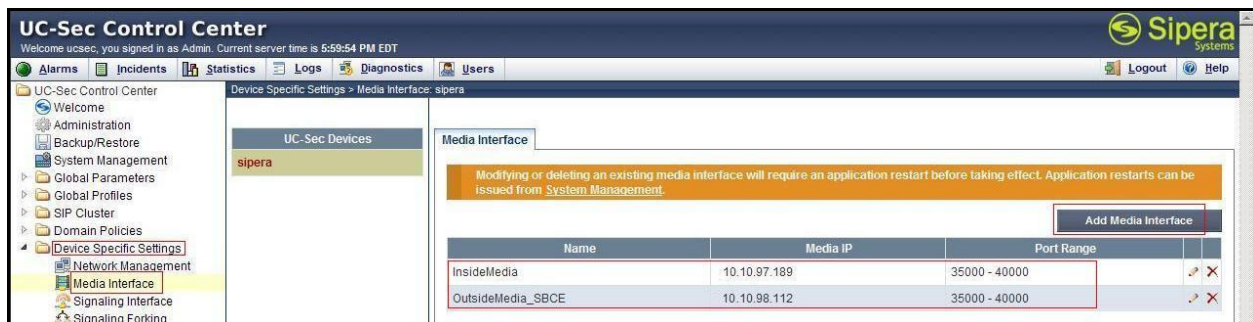


Figure 78: Media Interface

6.4.3. Create Signaling Interfaces

Signaling Interfaces (**Figure 79**) define the type of signaling on the ports.

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

- Select **Add Signaling Interface**.
 - **Name: InsideSIP**
 - **Media IP: 10.10.97.189** (Internal Address toward **Communication Server**)
 - **UDP Port: 5060**
 - Click Finish (not shown).

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

- Select **Add Signaling Interface**.
 - **Name: OutsideSIP_SBCE**
 - **Media IP: 10.10.98.112** (External Internet Address toward TELUS trunk)
 - **UDP Port: 5060**
 - Click Finish (not shown).



Figure 79: Signaling Interface

6.4.4. Configuration Server Flows

Server Flows (**Figure 80**) allow us to categorize trunk-side signaling and apply a policy.

6.4.4.1 Create End Point Flows – Communication Server

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

- Select the **Server Flows** Tab.
- Select **Add Flow**, enter **Flow Name: CS1K_CAR3**
 - **Server Configuration: CS1K_Car3**
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: OutsideSIP_SBCE**
 - **Signaling Interface: InsideSIP**
 - **Media Interface: InsideMedia**
 - **End Point Policy Group: CS1K_Car3_PolicyG**
 - **Routing Profile: CS1K75_To_TELUS**
 - **Topology Hiding Profile: TELUS_To_CS1K75**
 - **File Transfer Profile: None**
 - Click Finish (not shown).

6.4.4.2 Create End Point Flows – TELUS

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

- Select the **Server Flows** Tab.
- Select **Add Flow**, enter **Flow Name: TELUS**
 - **Server Configuration: TELUS**
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: InsideSIP**
 - **Signaling Interface: OutsideSIP_SBCE**
 - **Media Interface: OutsideMedia_SBCE**
 - **End Point Policy Group: TELUS_PolicyG**
 - **Routing Profile: TELUS_To_CS1K75**

- **Topology Hiding Profile: CS1K75_To_TELUS**
- **File Transfer Profile: None**
- Click Finish (not shown).

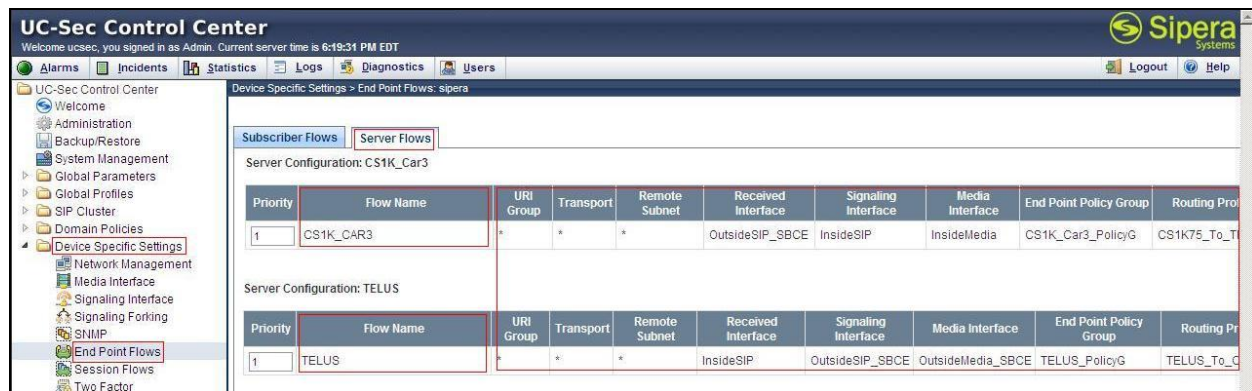


Figure 80: End Point Flows

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

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 4036929464.

- 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 9464**.
- After the call is released, issue command **trac 0 9464** 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 9464 is in call state:

```
>ld 80
```

```
.trac 0 9464
```

```
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: 20.20.119.218
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 9464 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 9464
MAIN_PM ESTD
TALKSLOT ORIG 20 TERM 25
EES_DATA:
NONE
QUEU NONE
CALL ID 501 76

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 484
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 16139675205 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
CALLED NO = 4036929464 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN

```

And this is the example after the call on 9464 is finished.

```

.trac 0 9464
IDLE VTN 96 0 00 02 MARP

```

SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675205) to an internal device (4036929464). 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.

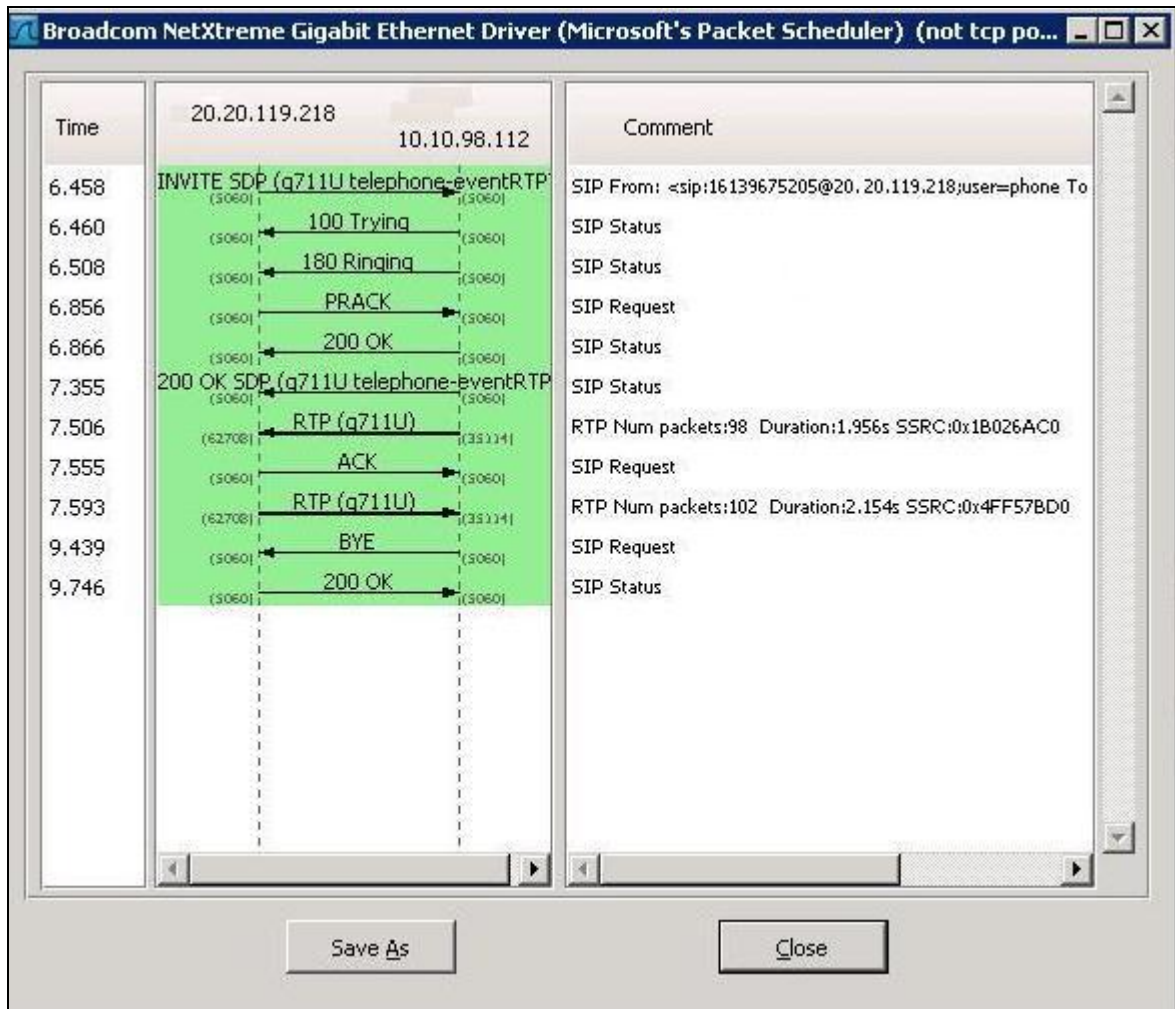
```

.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 the details of the INVITE message is being shown here.



```
Session Initiation Protocol
Request-Line: INVITE sip:4036929464@10.10.98.112:5060 SIP/2.0
Method: INVITE
Request-URI: sip:4036929464@10.10.98.112:5060
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 20.20.119.218:5060;branch=z9hG4bK610ek300e0jg2kc1e3c0.1
To: <sip:4036929464@10.10.98.112>
  SIP to address: sip:4036929464@10.10.98.112
  SIP to address User Part: 4036929464
  SIP to address Host Part: 10.10.98.112
From: <sip:16139675205@20.20.119.218;user=phone>;tag=sn1_0010398373_NSN_CLIENT
  SIP from address: sip:16139675205@20.20.119.218;user=phone
  SIP tag: sn1_0010398373_NSN_CLIENT
Call-ID: NSNSIP-e88b19ac-e98b19ac-1-11-1341866922-470108-1342337030
CSeq: 1235 INVITE
Contact: <sip:16139675205@20.20.119.218:5060;transport=udp>
Supported: 100rel
Supported: timer
Accept-Language: en;q=0.0
Allow: REGISTER, INVITE, ACK, BYE, CANCEL, NOTIFY, REFER, INFO, PRACK
Session-Expires: 1800;refresher=uac
Min-SE: 1800
Date: Mon, 09 Jul 2012 20:48:42 GMT
Max-Forwards: 68
Content-Type: application/sdp
Content-Length: 209
Message Body
Session Description Protocol
  Session Description Protocol Version (v): 0
  Owner/Creator, Session Id (o): PVG 1341866672580 1341866672580 IN IP4 20.20.119.218
  Session Name (s): -
  Phone Number (p): +1 6135555555
  Connection Information (c): IN IP4 20.20.119.218
  Time Description, active time (t): 0 0
  Media Description, name and address (m): audio 62708 RTP/AVP 0 101
```

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 TELUS system is considered **compliant** with Communication Server 1000 Release 7.5 and Avaya Session Border Controller for Enterprise Release 4.0.5 Q09.

9. Additional References

Product services for Avaya SBCE may be found at:

<http://www.sipera.com/products-services/esbc>

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 03.10, September 2011.*

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.09, October 2011*

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.05, October 2011*

[4] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.17, January 2012*

[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 05.03, December 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.