Avaya Solution & Interoperability Test Lab

Application Notes for Configuring with the Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Acme Packet Net-Net 3800 Session Border Controller Release 6.2 with TELUS SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe a solution comprised of the Avaya Communication Server 1000 release 7.5 and the TELUS SIP Trunking. During the interoperability testing, Avaya Communication Server 1000 was able to interoperate with the TELUS Communication NSN HiQ via SIP trunking. This test was performed to verify SIP trunk features including basic call, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls are placed in both directions with various set types.

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.

©2011 Avaya Inc. All Rights Reserved.

Table of Contents

©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.

List of Figures

©2011 Avaya Inc. All Rights Reserved.

©2011 Avaya Inc. All Rights Reserved.

Introduction

This document provides a typical network configuration deployment of the Avaya Communication Server 1000 (hereafter referred to as CS1K) and the TELUS SIP Trunking (hereafter referred to as TELUS system). During the interoperability testing, all SIP trunk applicable feature test cases were executed to ensure the interoperability between the TELUS system and the Avaya CS1K 7.5, Avaya Aura® Session Manager Release 6.1 and Acme Packet Net-Net 3800 Session Border Controller Release 6.2 system.
The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 2:1**. Avaya uses a combination of FQDNs and IP addresses, the TELUS network is IP address based.
For confidentiality purposes, the IP addresses in these Application notes have been modified to show 111.x.x.x for Avaya internal addresses, 222.x.x.x for Avaya external address and 333.x.x.x for TELUS external address. TELUS customers will use their own FQDNs and IP addresses as required.

1. General Test Approach and Test Results

The CS1K system release 7.5 was connected to an Acme Session Border Controller (hereafter referred to as Acme SBC) via SIP trunks to the Avaya Aura® Session Manager. The Acme SBC was connected to the TELUS system via SIP trunk. Various call types were made from the CS1K to the TELUS system and vice versa to ensure the interoperability between the CS1K and the TELUS system.

1.1. Interoperability Compliance Testing

The focus of this testing is to verify that CS1K release 7.5 can interoperate with the TELUS system. The following interoperability areas were covered.

- General call processing between CS1K and TELUS systems including:
  - Codec (G.711 u-law/ G.729/ ptime 20ms, VAD disabled)
  - Hold/Retrieve on both ends
  - Music On Hold
  - CLID displays
  - Ring-back tone
  - Speech paths
  - 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
- RFC2833/DTMF on both direction
- SIP Transport UDP
- Thru dialing via PBX Call Pilot
- Voice Mail Server CallPilot (hosted on the Avaya CS1Ksystem)

©2011 Avaya Inc. All Rights Reserved.

- Early Media Transmission

1.2. Test Results

The objectives outlined in **Section 1.1** were verified. All the applicable test cases were executed. However, the following observations were noted during the compliance testing.

1.2.1. Blind Transfer

In the default configuration, the CS1K will not allow a blind transfer to be executed if the parties involved do not support the SIP UPDATE method. With the installation of plugin 501 on the CS1K, the blind transfer will be allowed and the call will be completed. The limitation of this plugin is that no ringback is provided to the originator of the call for the duration that the destination set is ringing. There are certain devices within the TELUS network that this situation would apply to and hence the originator of a call that is blind transferred will not hear ringback. In addition to plugin 501, it is required that VTRK SU version "cs1000-vtrk-7.50.17.16-15.i386.000.ntl" or higher be used on all SSG signaling servers to ensure proper operation of the blind transfer feature. The use of plugin 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPATE method, but rather extend support to those parties that do not.

1.2.2. reINVITE without SDP "slow-start"

There are certain systems within the TELUS network that currently do not support reINVITE without SDP. In order to provide transfer capabilities to systems components that do not support reINVITE without SDP "called slow-start", the SBC must be configured to insert a dummy SDP onto reINVITES and the SBC must also anchor all media.

The side effect of anchoring the media is an increase of network traffic on the customer's network in situations where external callers are connected together. For example, in normal conditions if an external call enters the customer's network and is transferred back out to another external set, the media would be connected directly between the external sets and not use resources on the customer's network. When media anchoring is used, the external media stream of each call leg still travels into the customer's network where it is anchored or linked together on the SBC.

There is no real measureable limitation of inserting an SDP onto reINVITE that did not originally include one. The inserted SDP is a copy of one previously used in the current call leg and the o= sequence number is not increased. The NSN HiQ in the TELUS network will not send this particular reINVITE further to other SIP nodes. The only possible implication that can be thought at this point is a time-out on calls that require several hops, but this has not been proven.

1.2.3. Diversion header added to call redirection

Calls that are redirected on the CS1K 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 CS1K does not support

©2011 Avaya Inc. All Rights Reserved.

Diversion headers. In order to provide this functionality the Acme Packet SBC will extract the user and host information from the History-Info header and create a Diversion header. There are certain voice mail systems that may not integrate properly when a Diversion header is used.

1.2.4. History-Info support

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 CS1K accomplishes this by using the Acme Packet SBC to extract the user and host information from the History-Info header and create P-Asserted-Identity header. The limitations of the using a P-Asserted-Identity header are discussed in the Caller ID and Privacy section.

1.2.5. Caller ID

Caller ID works properly between the CS1K and the TELUS network when there is no call redirection involved in the call flow. However, when a call is redirected on the CS1K the caller ID will not properly reflect the originator of the call. In normal conditions if a set is programmed to call forward calls to a different terminating set, the caller ID displayed on the terminating set will be that or the originator of the call and not the caller ID of the set that is doing the call forward. On the TELUS network the PAI header is used to authenticate the call during call redirection scenarios. When a call is redirected the PAI header will be populated with the information of the set that is doing the call redirection. The limitation of this approach on the TELUS network is that the caller ID displayed on the terminating set is that of the redirecting set and not the caller ID of the originator of the call.

1.2.6. Privacy

The privacy issue is linked to the caller ID issue above, in that the incorrect caller ID is displayed on the terminating set when a call redirection takes place. In normal conditions the privacy information of the originator of the call is carried forward through call redirection to the terminating set. This case is still true for the current TELUS setup, that the privacy of the originator of the call is protected in redirection scenarios. However, if privacy is configured on the set doing the redirection then the privacy of this set will be compromised. As mentioned in the Caller ID section, the caller ID displayed on the terminating set is that of the set doing the redirection, this is a limitation of using the P-Asserted-Identity header for call redirection. Because the CS1K will use the privacy setting of the originator of the call, the privacy setting of the set doing the redirection is ignored. As a result the caller ID of the redirecting set will always be displayed on the terminating set is call redirection scenarios, regardless of the privacy setting of the redirecting set.

©2011 Avaya Inc. All Rights Reserved.

1.2.7. Hold/Resume

When a call is placed on hold and no music on hold is configured, the CS1K will send an INVITE with SDP to the set on hold so it will no longer listen to the other party. This is normally accomplished on the CS1K by setting c=0.0.0.0 and a=inactive in the SDP. For the TELUS configuration and to align with RFC 3264, the SBC is configured to change the 0.0.0.0 to a valid IP address, in this case the IP address of the external interface of the SBC, and change the stream to a=sendonly.

1.2.8. SIP Header Optimization

SIP header rules were implemented in the SBC to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X_nt_e_164_clid, Alert_Info and Route. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-epid-frag and x-nt-inforeq/8000, was stripped out. These particular headers and MIME have no real use in the service provider network, in this case the TELUS network. If an issue is being investigated on the service provider network, the presence of these headers may add unnecessary confusion.

1.3. Support

For technical support on the TELUS system, please contact your TELUS Account Executive or visit TELUS.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the Support Contact Options link followed by Maintenance Support provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

©2011 Avaya Inc. All Rights Reserved.

2. Reference Configuration

Figure 2:1 illustrates the test configuration used during the compliance testing event between the CS1K and TELUS system.

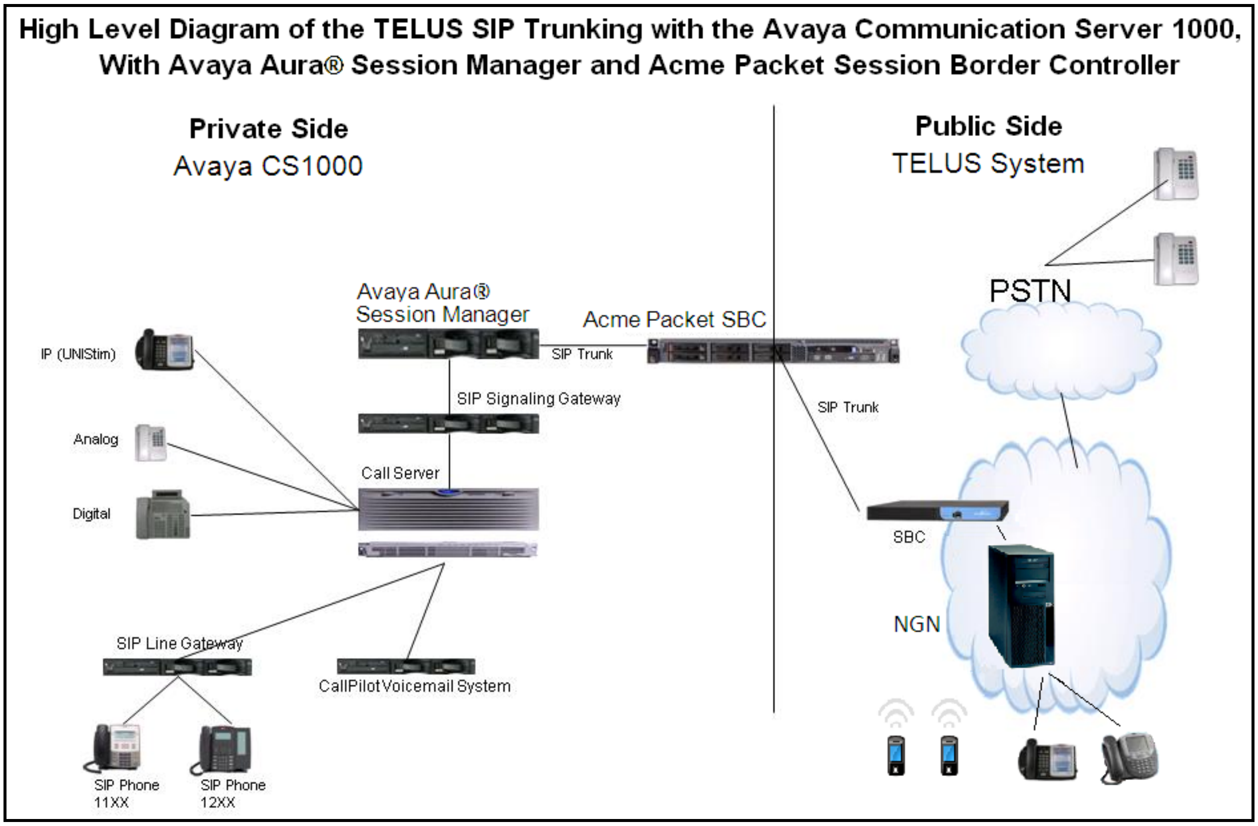

Figure 2:1 Network Diagram for Avaya CS1K – TELUS system

The following assumptions were made for this lab test configuration:

1. CS1K R7.5, Session Manager 6.1 and Acme Packet 6.2 software implemented with all the latest patches
2. TELUS provides support to setup, configure, and troubleshoot on the carrier switch for the duration of the testing.

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, name and redirection information both prior to answer and after call establishment.

©2011 Avaya Inc. All Rights Reserved.

6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window were open during the test cases execution for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path and display checked before and after calls were put on/off hold from each end.
9. Applicable files were screened on an hourly basis during the testing for message that may indicate technical issues. This refers to Avaya PBX 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.

3. Equipment and Software Validated

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

Avaya system:

System	Software/Loadware version
Avaya CS1K 7.5 (CPPM)	• Call Server: 7.50 Q GA • SSG Server: 7.50.17 GA • SLG Server: 7.50.17 GA
Avaya Aura ® Session Manager	• 6.1.0.0.610023
Avaya phones	• 2001 p2: 0604DCN (UNIStim) • 2004 p1: 0602B76 (UNIStim) • M3904: Core 2.4, Flash 9.4 P0 L1.8
Acme Packet Net-Net 3800	• Firmware SCX6.2.0 MR-4 Patch 3 (Build 754)

TELUS system:

System	Software/Loadware version
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 – Issue: 01 Release: x2107.50, 2011-07-19 11:40:08 (est)
SSG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17.16-1.i386.000.ntl
SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17.16-1.i386.000.ntl

Note: It is required that VTRK SU version "cs1000-vtrk-7.50.17.16-15.i386.000.ntl" or higher be used on all SSG signaling servers to ensure proper operation of the blind transfer feature. The pstat command shown below can be used to verify what version of VTRK SU is installed. If a new version is required, download the newest Linux 7.50 Service Pack and install using the standard patch process (not described in this document).

The output of "**dstat**" command on Call Server:

©2011 Avaya Inc. All Rights Reserved.

```
pdt> dstat
Call Server:
------------
DepList name: core
        Filename: /var/opt/nortel/cs/fs/u/patch/deplist/mcore_01.cpl
        Issue   :  01
        Release :  x2107.50
        Created :  2011-07-19 11:40:08 (est)
        Number of patches: 60
        Patches Loaded: 60
        Patches In-service: 60
```

The output of "**pstat**" command on SSG Server:

```
[admin@car1-sps-ucm ~]$ pstat
Product Release: 7.50.17.00
In system patches: 0

In System service updates: 12
PATCH#  IN_SERVICE   DATE      SPECINS   REMOVABLE   NAME
0       Yes          27/04/11   NO       YES         cs1000-sps-7.50.17-01.i386.000
1       Yes          27/04/11   NO       YES         cs1000-baseWeb-7.50.17.01-1.i386.000
2       Yes          27/04/11   NO       YES         cs1000-shared-pbx-7.50.17-01.i386.000
3       Yes          27/04/11   NO       YES         cs1000-dbcom-7.50.17-02.i386.000
4       Yes          29/08/11   NO       YES         cs1000-vtrk-7.50.17.16-15.i386.000
11      Yes          25/08/11   NO       YES         cs1000-linuxbase-7.50.17.16-1.i386.000
12      Yes          25/08/11   NO       YES         cs1000-dmWeb-7.50.17.16-1.i386.000
13      Yes          25/08/11   NO       YES         cs1000-emWeb_6-0-7.50.17.16-6.i386.000
14      Yes          25/08/11   NO       YES         cs1000-tps-7.50.17.16-4.i386.000
15      Yes          25/08/11   YES      YES         cs1000-Jboss-Quantum-7.50.17.16-4.i386.000
16      Yes          25/08/11   NO       YES         cs1000-patchWeb-7.50.17.16-1.i386.000
17      Yes          25/08/11   NO       YES         cs1000-bcc-7.50.17.16-13.i386.000
```

The plug-in list can be displayed with the plp (plug-in print) command as shown below. Plug-ins come preinstalled and are delivered with every software load. If plug-in 501 is not activated, it can be enabled using the ple command, also shown below.

©2011 Avaya Inc. All Rights Reserved.

```
>
PDT login on /pty/ptty00.S
Username: admin
Password:

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

pdt> plp

0  TO 43  - DISABLED
44  TO 46  - NOT SUPPORTED
47  TO 48  - DISABLED
49  - NOT SUPPORTED
50  - DISABLED
51  TO 52  - NOT SUPPORTED
53  - DISABLED
54  - NOT SUPPORTED
55  TO 62  - DISABLED
63  - NOT SUPPORTED
64  - DISABLED
65  - NOT SUPPORTED
66  - DISABLED
67  - NOT SUPPORTED
68  TO 70  - DISABLED
71  - NOT SUPPORTED
72  TO 74  - DISABLED
75  TO 200  - NOT SUPPORTED
201  - ENABLED
202  TO 203  - DISABLED
204  - NOT SUPPORTED
205  TO 226  - DISABLED
227  - NOT SUPPORTED
228  - DISABLED
229  - NOT SUPPORTED
230  TO 233  - DISABLED
234  - NOT SUPPORTED
235  - DISABLED
236  TO 499  - NOT SUPPORTED
500  TO 501  - DISABLED
502  TO 503  - NOT SUPPORTED
504  TO 505  - DISABLED
506  TO 511  - NOT SUPPORTED

pdt> ple 501

PLUG-IN 501  IS ENABLED

pdt>
```

4. Avaya Communication Server 1000 Configuration

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

The below procedures describe the configuration details of CS1K with a SIP trunk to TELUS system.

4.1. Login to CS1K System

4.1.1. Login Unified Communications Management and Element Manager

a) Open an instance of a web browser and connect to the Unified Communications Management (UCM) GUI at the following address: http://<UCM IP address> as shown in **Figure 4:1**. Log in using an appropriate Username and Password.

Figure 4:1 Login Unified Communications Management

b) The **Unified Communications Management** screen is displayed. Click on the **Element Name** of the CS1K Element as highlighted in red box as shown in **Figure 4:2**.

©2011 Avaya Inc. All Rights Reserved.

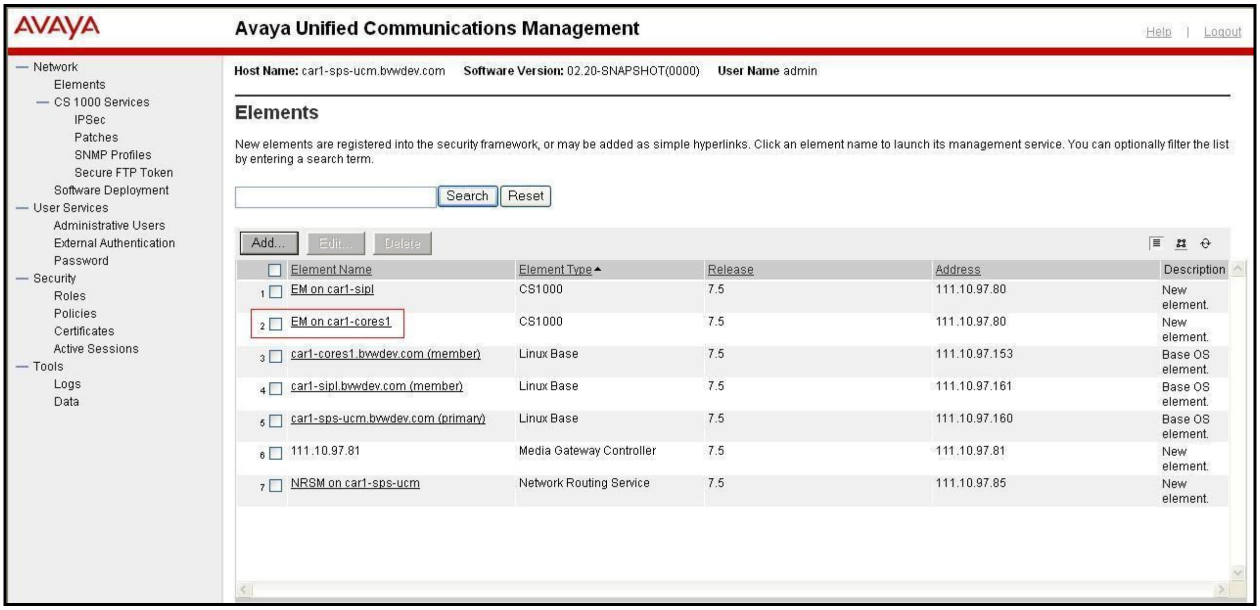

Figure 4:2 Unified Communications Management

c) The CS1K Element Manager (EM) **System Overview** page is displayed as shown in **Figure 4:3**, this is the main Element Manager screen from which all other menus can be launched.

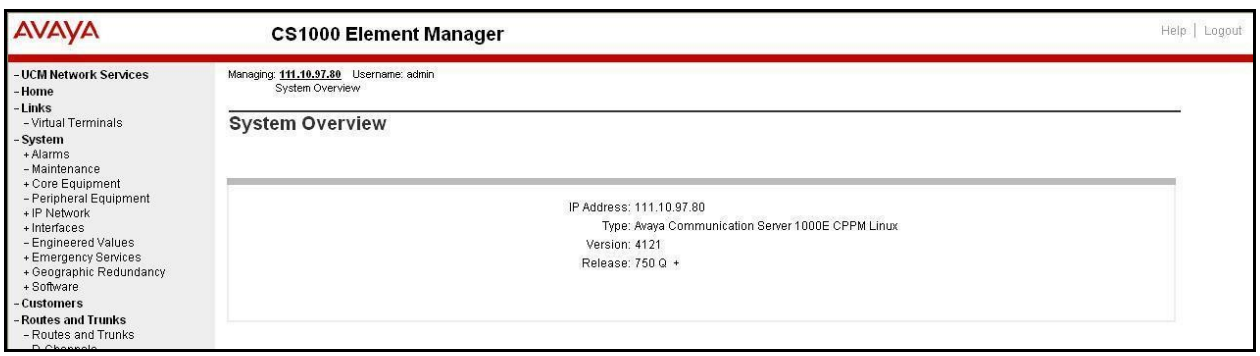

Figure 4:3 Element Manager System Overview

4.1.2. Login to Call Server Command Line Interface (CLI)

a) Using Putty, SSH to IP address of SSG Server with the admin account.
b) Run the command "cslogin" and login with the appropriate admin account and password.

©2011 Avaya Inc. All Rights Reserved.

```
login as: admin

            Avaya Inc. Linux Base  7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.
admin@135.10.97.80's password:
Last login: Mon Jul 18 11:01:44 2011 from 135.20.233.246
[admin@car1-cores1 ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authenticating

TTY 09 SCH MTC BUG   11:38
OVL111 IDLE   0
>login admin
PASS?
.
TTY #09 LOGGED IN ADMIN 11:3
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
9  18/7/2011

>
SRPT4619 WARNING: Last Archive Procedure had failed
       No archives were completed since May 13 14:59:00 2011


OVL000
>
```

4.2. Administer a Node IP Telephony

This section describes how to configure a Node IP Telephony on the CS1K.

4.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 1000) in CS1K IP network to work with the TELUS system. For further information on Avaya Communications Server 1000, please consult reference in Additional References.

a) Select **System -> IP Network -> Nodes: Servers, Media Cards. Figure 4:4** displays **IP Telephony Nodes** page. Then click on the Node ID of your CS1K Element (e.g. **1000**).

©2011 Avaya Inc. All Rights Reserved.

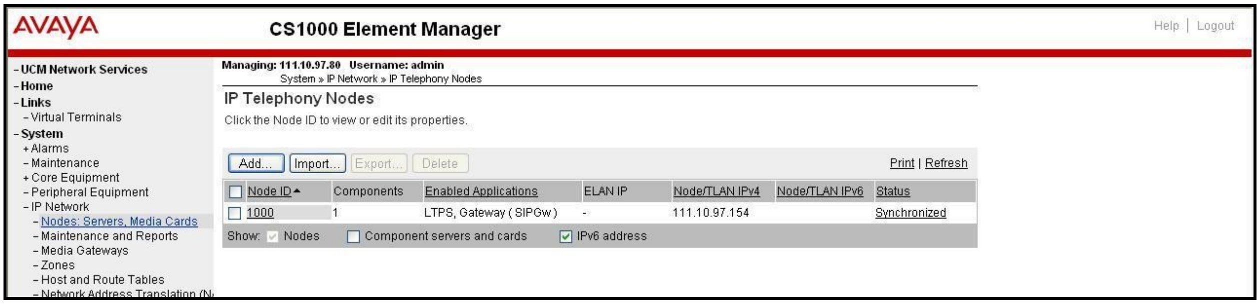

Figure 4:4 IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 4:5** with the IP address of the CS1K node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components to process the SIP call.

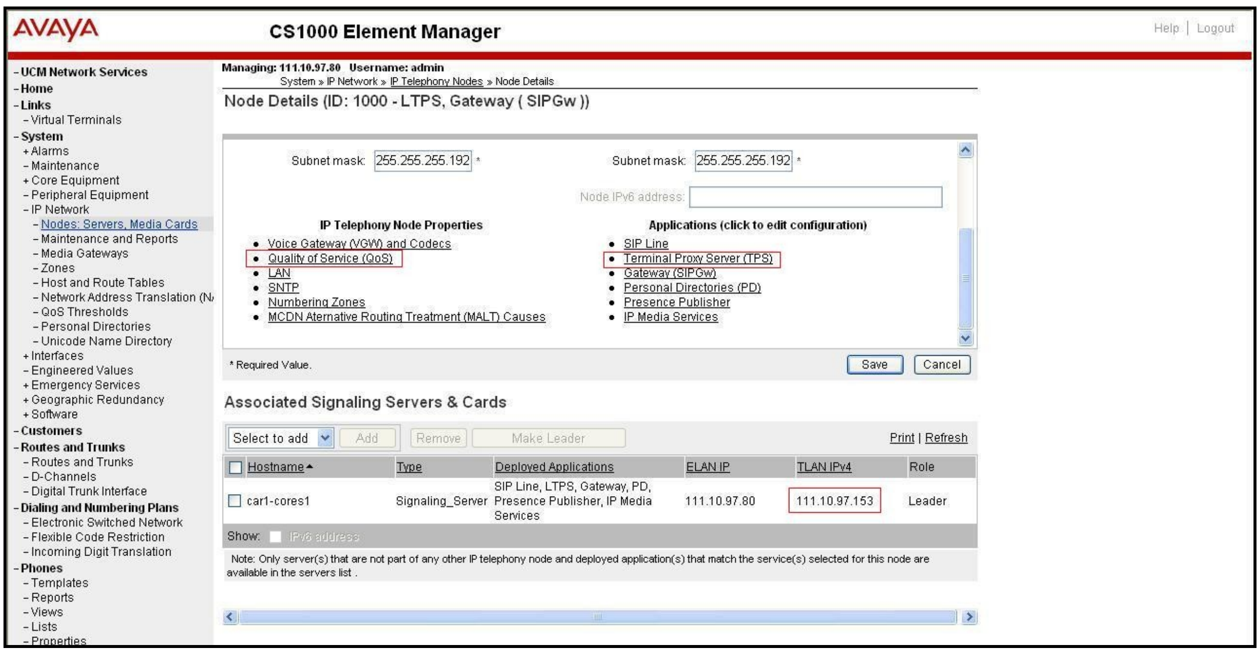

Figure 4:5 Node Details

4.2.2. Administer TPS

c) Continue from **Section 4.2.1**. On the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link as shown in **Figure 4:6.**

d) Check the **UNIStim Line Terminal Proxy Server** check box and then click **Save** as shown in **Figure 4:6**.

©2011 Avaya Inc. All Rights Reserved.

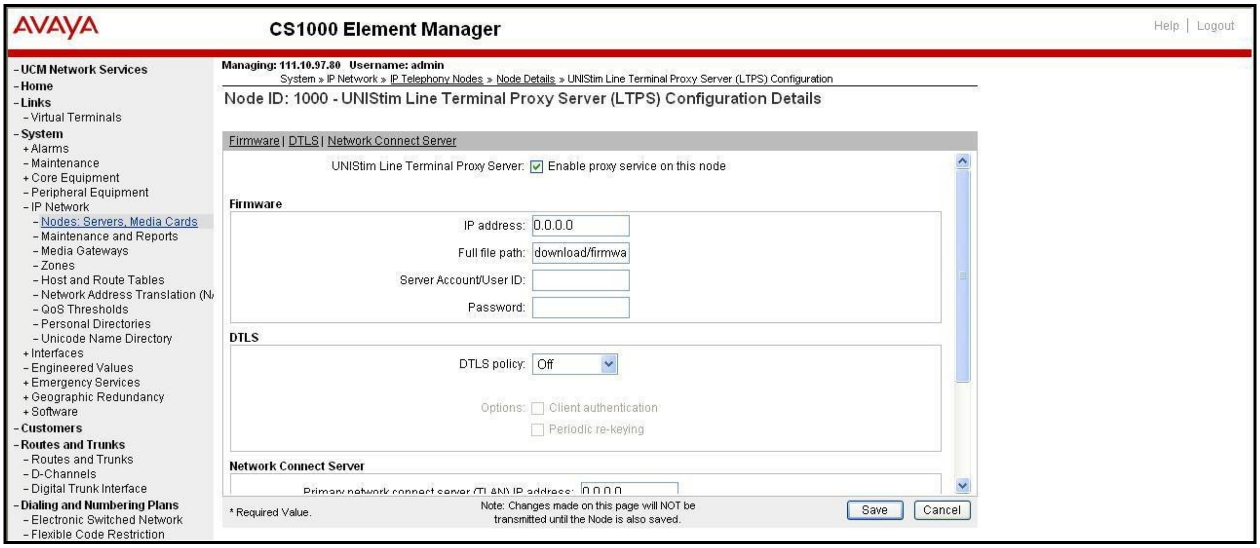

Figure 4:6 TPS Configuration Details

4.2.3. Administer Quality of Service (QoS)

e) Continue from **Section 4.2.1**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 4:5**.

f) The default Diffserv values are as shown in **Figure 4:7**. Click the **Save** button.

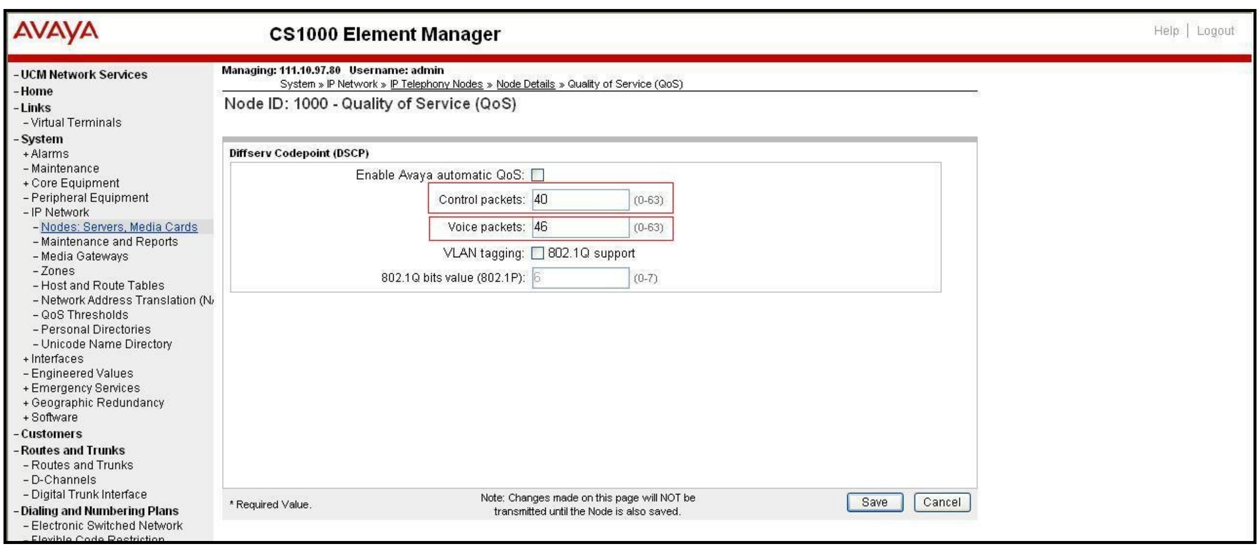

Figure 4:7 QoS Configuration Details

4.2.4. Synchronize the New Configuration

g) Continue from **Section 4.2.3**, return to the **Node Details** page in **Figure 4:5** and click on the **Save** button.

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

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

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

4.3. Administer Voice Codec

4.3.1. Enable Voice Codec, Node IP Telephony.

a) Select **IP Network** -> **Nodes: Servers, Media Cards** -> Configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1K system. The **Node Details** screen is displayed. (See in **Section 4.2.1** for more detail).
b) On the **Node Details** page as shown in **Figure 4:5**, click on **Voice Gateway (VGW) and Codec.**
c) The TELUS SIP Trunk supports voice codec G.711 and G.729, payload size 20 ms, with VAD disabled. **Figure 4:8** and **Figure 4:9** show voice codec profile configured on CS1K with G.729 and G.711, payload size 20ms and VAD disabled.

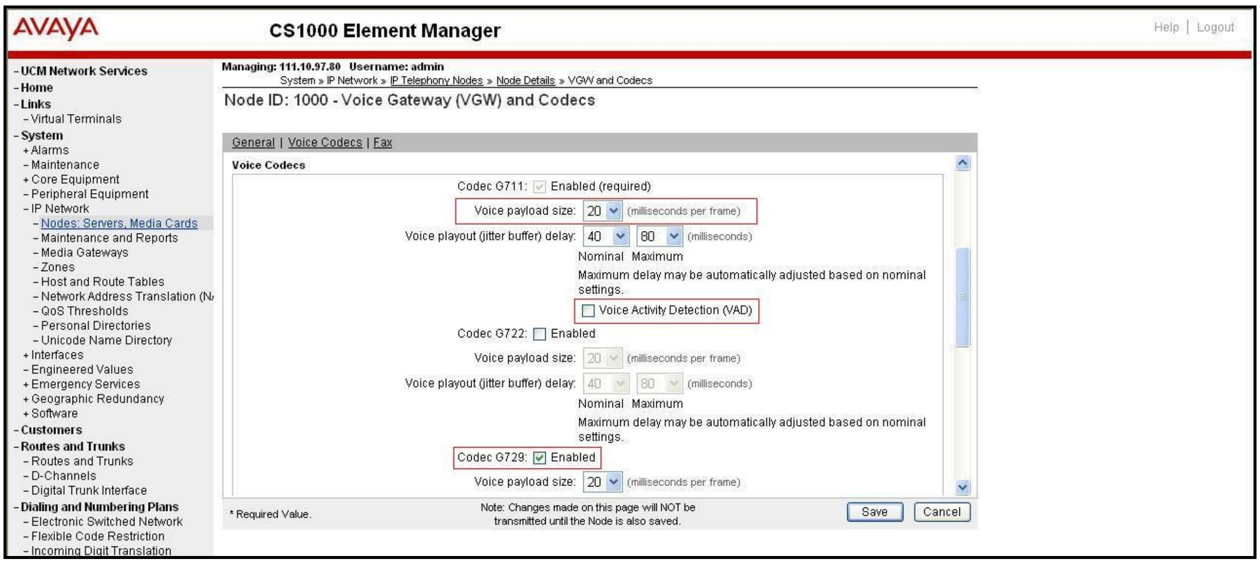

Figure 4:8 Voice Codec G.711 Configuration Details

©2011 Avaya Inc. All Rights Reserved.

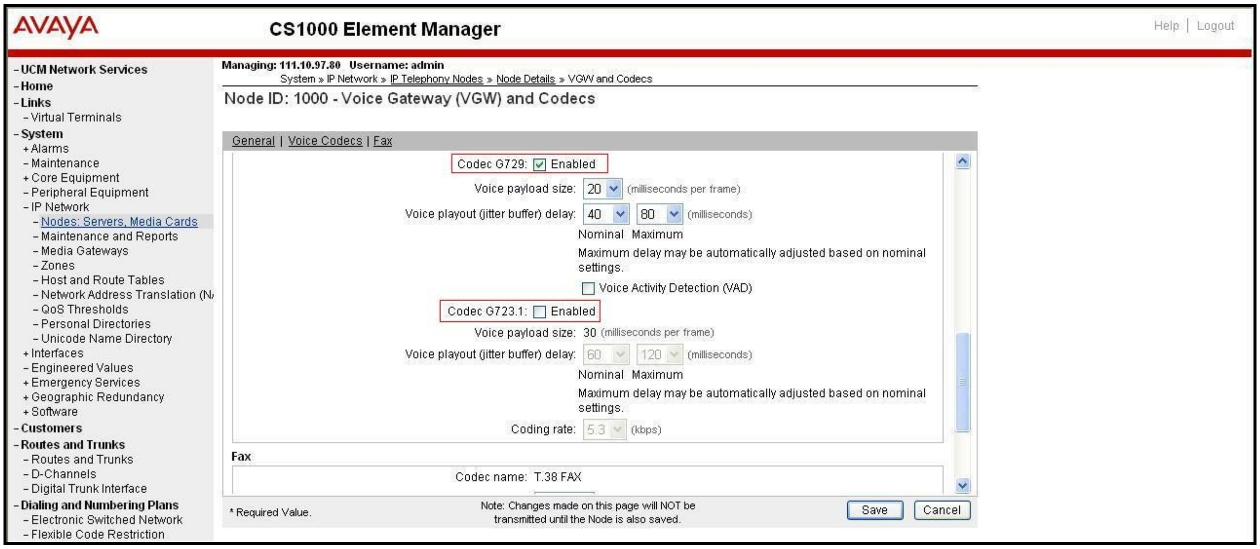

Figure 4:9 Voice Codec G.729 Configuration Details

d) For Fax over IP, TELUS supports T.38 as default and G.711 as fallback. **Figure 4:10** shows T.38 with payload size 30ms was chosen as default codec for fax.

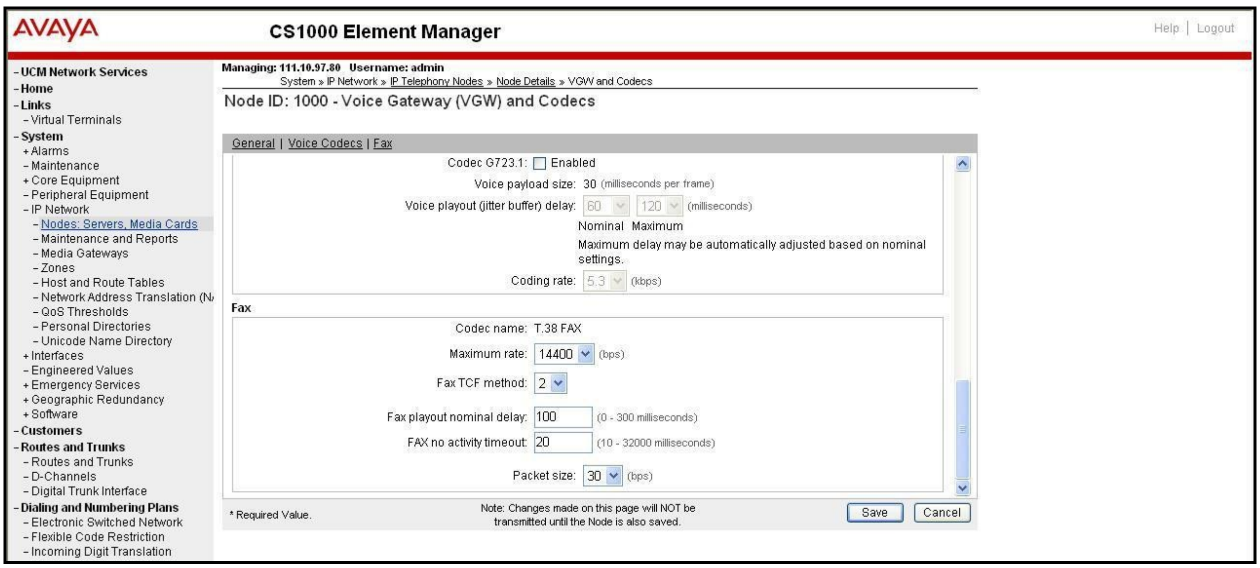

Figure 4:10 Fax Codec T.38 Configuration Details

Figure 4:11 shows **Modem Pass Through** was selected; this configuration enables G.711 as fallback codec for fax.

©2011 Avaya Inc. All Rights Reserved.

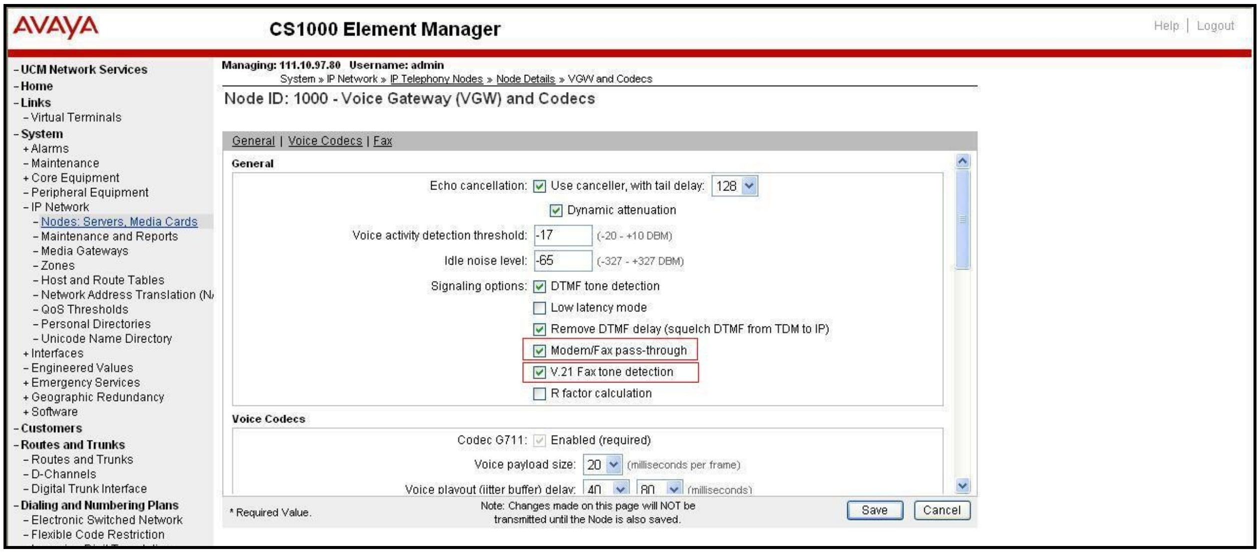

Figure 4:11 Fax Codec G.711 Configuration Details

e) Click **Save**.
f) Synchronize the new configuration (please refer to **Section 4.2.4** for more detail)

4.3.2. Enable Voice Codec on Media Gateways.

CS1K uses Media Gateways to support traditional analog/ digital phones can make voice call over SIP Trunk. Media Gateways is also needed to support analog terminal to send fax over IP.

a) From the left menu of the Element Manager page in **Figure 4:12**, select **IP Network** -> **Media Gateways** menu item. The Media Gateways page will appear. Click on the corresponding **IPMG** located on the left of the page.

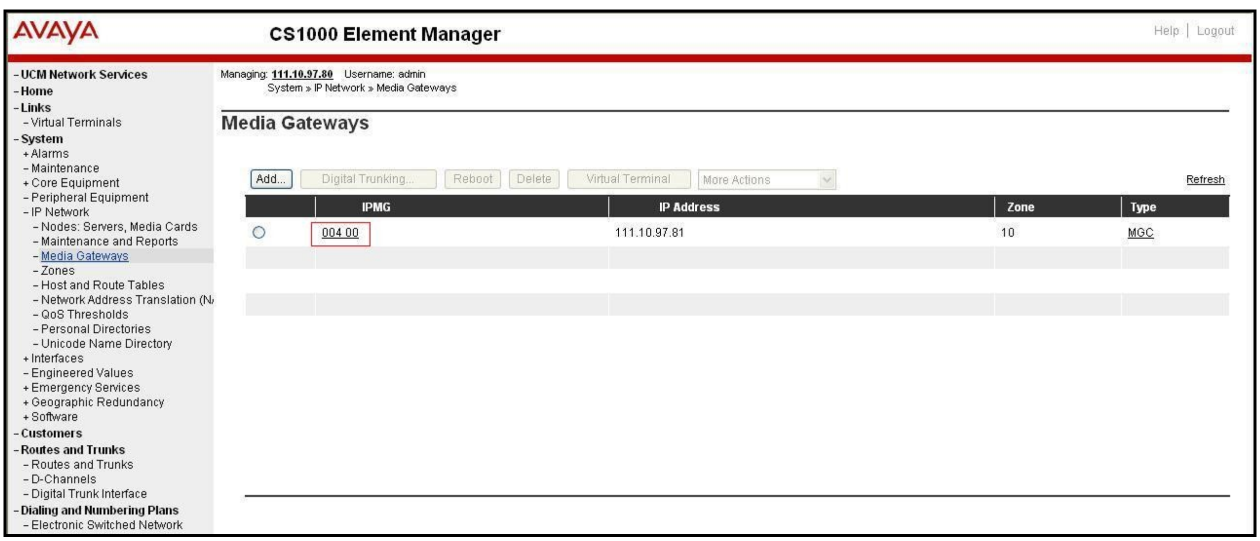

Figure 4:12 Media Gateways Screen

©2011 Avaya Inc. All Rights Reserved.

b) The IPMG Property Configuration page displays basic configuration setting for the Media Gateway. Click on the “Next” at the lower right of the page to proceed to the codec settings.

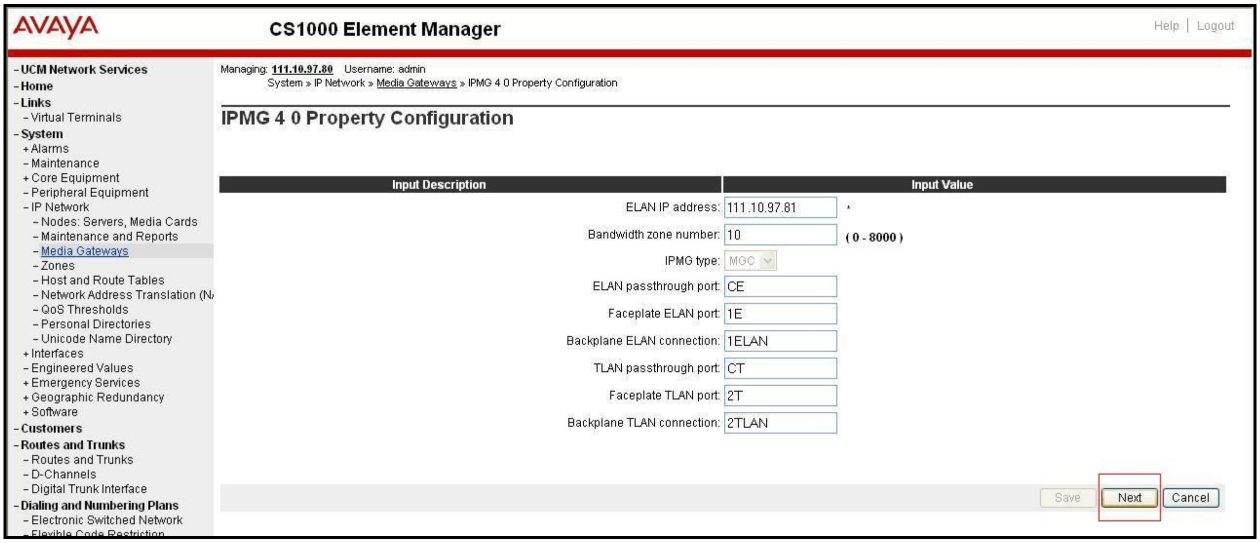

Figure 4:13 IPMG Property Configuration Page

c) The TELUS SIP Trunk supports voice codecs G.711 and G.729, payload size 20 ms, with VAD disabled**. Figure 4:14** shows configuration for voice codec profile; codec **G711, Voice payload size** 20 and uncheck **VAD**; then check Codec **G729A** checkbox, select **Voice payload size** 20 and uncheck **VAD.**

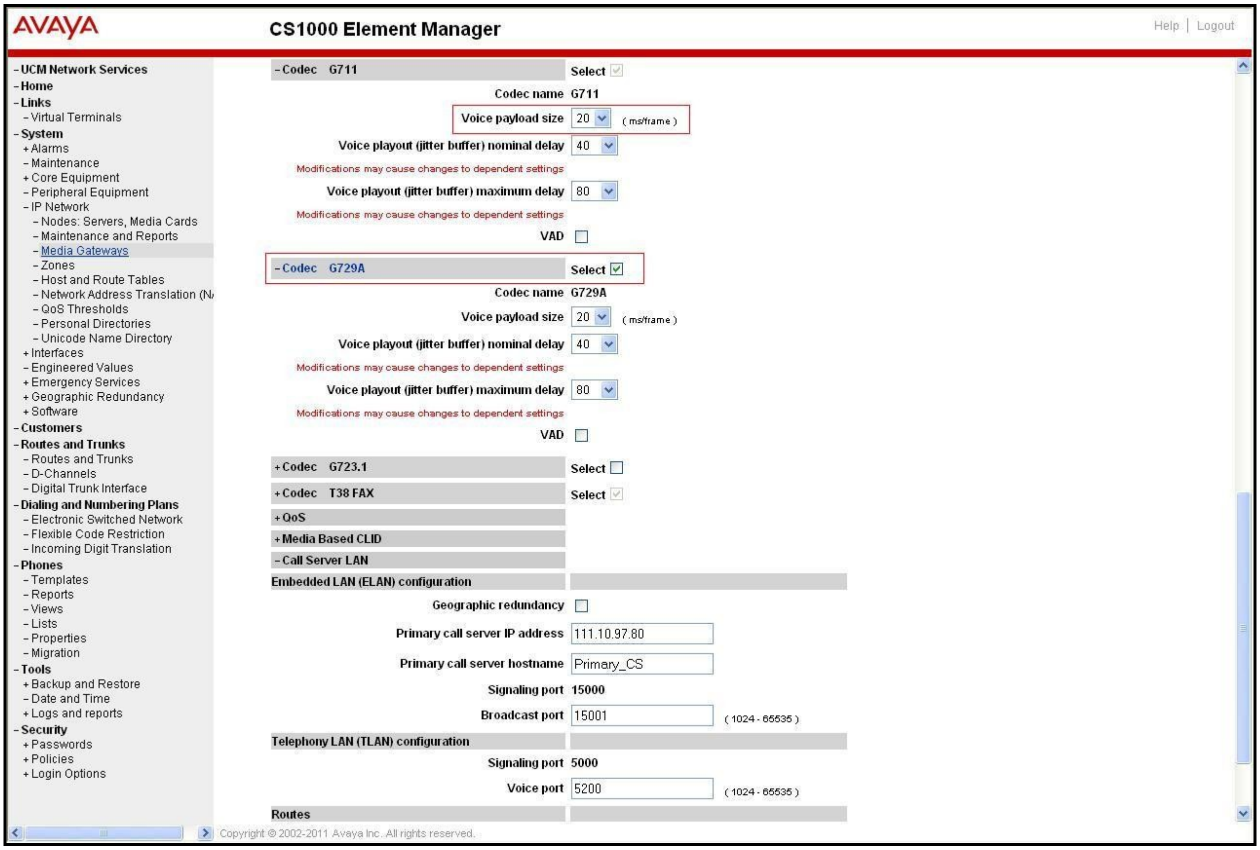

Figure 4:14 Media Gateways G.729 and G.711 Configuration Details

©2011 Avaya Inc. All Rights Reserved.

d) For Fax over IP, TELUS supports T.38 as default and G.711 as fallback. **Figure 4:15** shows T.38 with payload size 30ms was chosen as default codec, and Modem Pass Through was enabled, this configuration enables G.711 as fallback codec for fax.

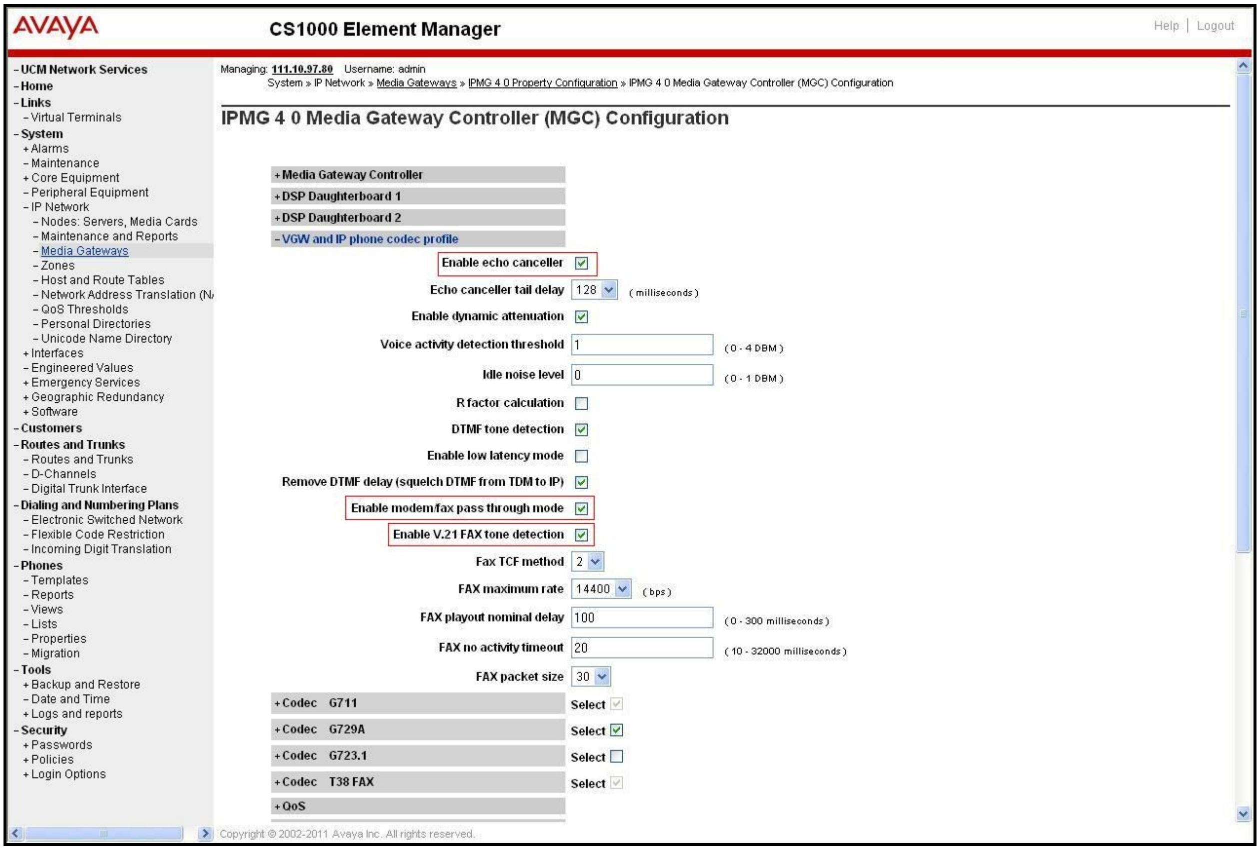

Figure 4:15 Media Gateways T.38 and ModemPassThrough(G.711) Configuration Details

4.4. Administer Zones and Bandwidth

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

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

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

a) Select **IP Network** -> **Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown in **Figure 4:16**.

©2011 Avaya Inc. All Rights Reserved.

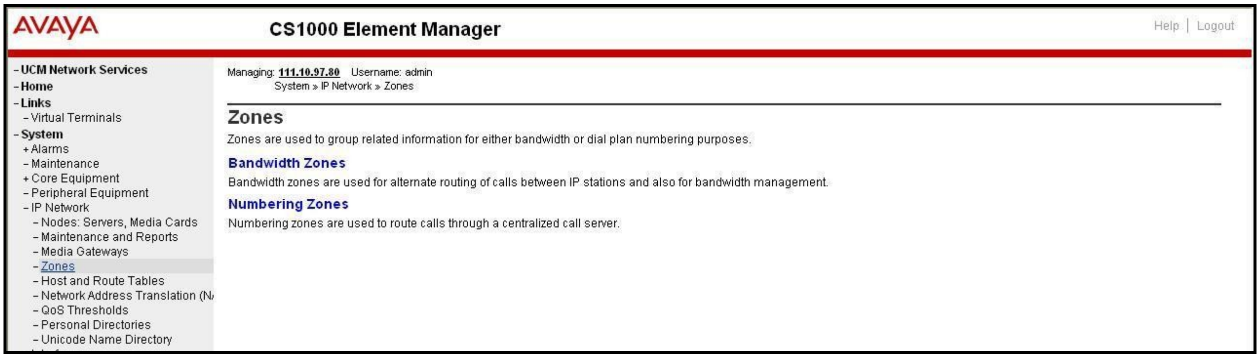

Figure 4:16 Zones Page

b) The **Bandwidth Zones** screen is displayed as shown in **Figure 4:17**. Click **Add**.

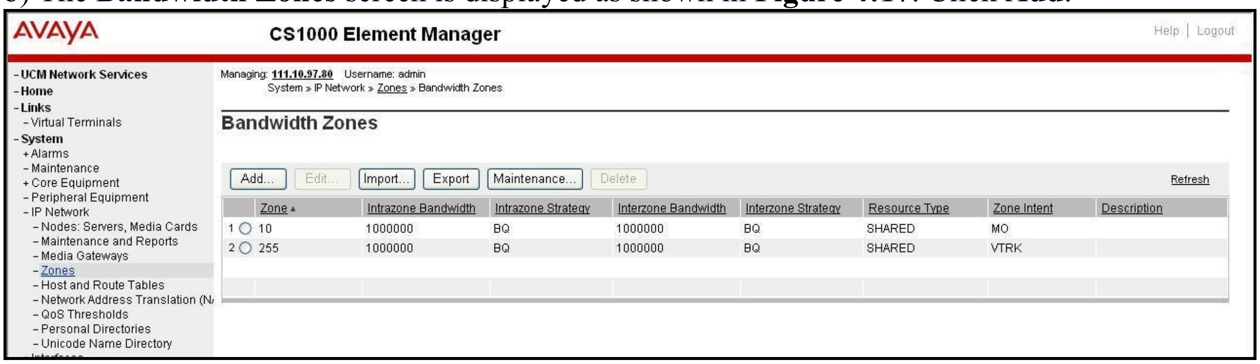

Figure 4:17 Bandwidth Zones

c) Then in the **Add Bandwidth Zone** screen (not shown), click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in **Figure 4:18** and click on the **Submit** button.

- **INTRA_STGY**: bandwidth configuration for local calls.
- **INTER_STGY**: bandwidth 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
- **VTRK**: is used for virtual trunk.

The TELUS SIP Trunk support is set for G.711 for the initial setup, with G.729 used when necessary for low bandwidth test cases. So the **MO** Zone 10 was configured with **Strategy Best Quality (BQ)**.

©2011 Avaya Inc. All Rights Reserved.

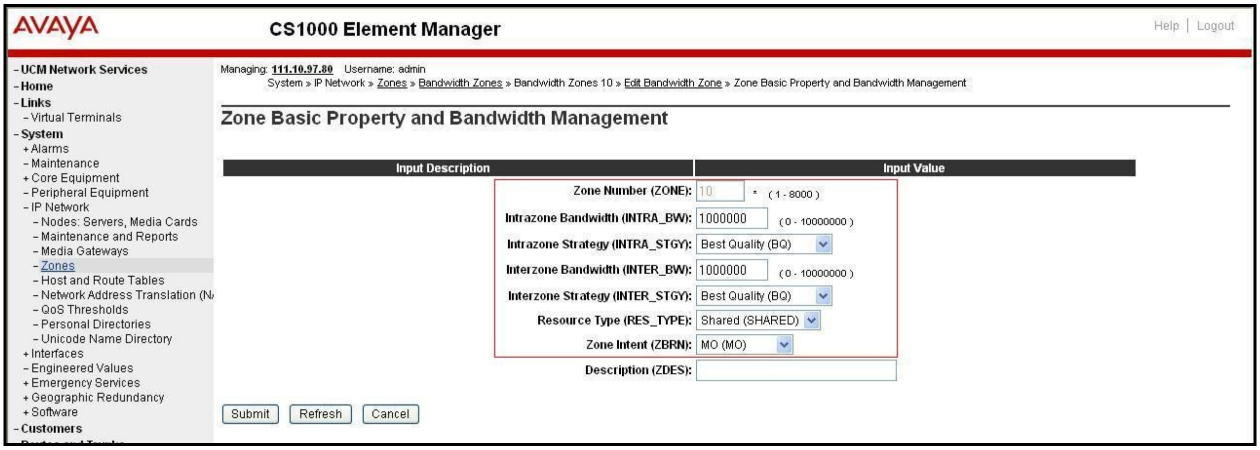

Figure 4:18 Bandwidth Management Configuration Details– IP phone

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

Follow **Section 4.4.1** 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 4:19** and then click on the **Submit** button.

The TELUS SIP Trunk support G.729 as the first choice, G.711 as fallback. So the **VTRK** Zone 255 was configured with **Strategy Best Quality (BQ)**.

Figure 4:19 Bandwidth Management Configuration Details– Virtual Trunk

©2011 Avaya Inc. All Rights Reserved.

4.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between the SIP Signalling Gateway (SSG) and the Session Manager (SM).

4.5.1. Integrated Services Digital Network (ISDN)

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.

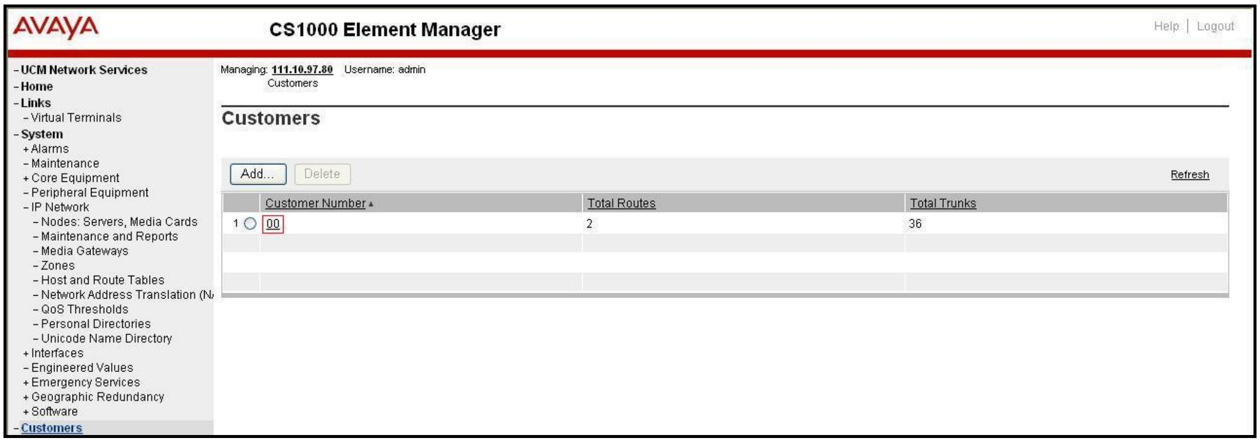

Figure 4:20 Customer Page

b) The **Customer 00 Edit** page will appear. Select the **Feature Packages** option from this page.

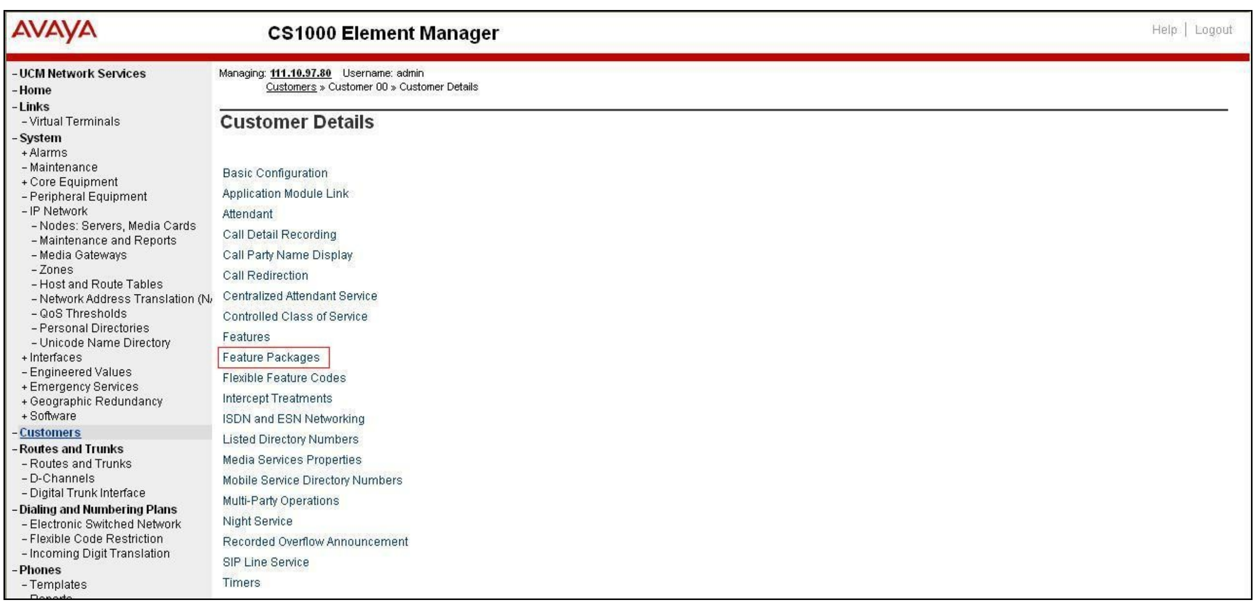

Figure 4:21 Customer Details Page

c) The screen is updated with a list of F**eature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below

©2011 Avaya Inc. All Rights Reserved.

Integrated Services Digital Network. Check the **Integrated Services Digital Network** (ISDN) checkbox, and retain the default values for all remaining fields as shown in **Figure 4:22**. Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

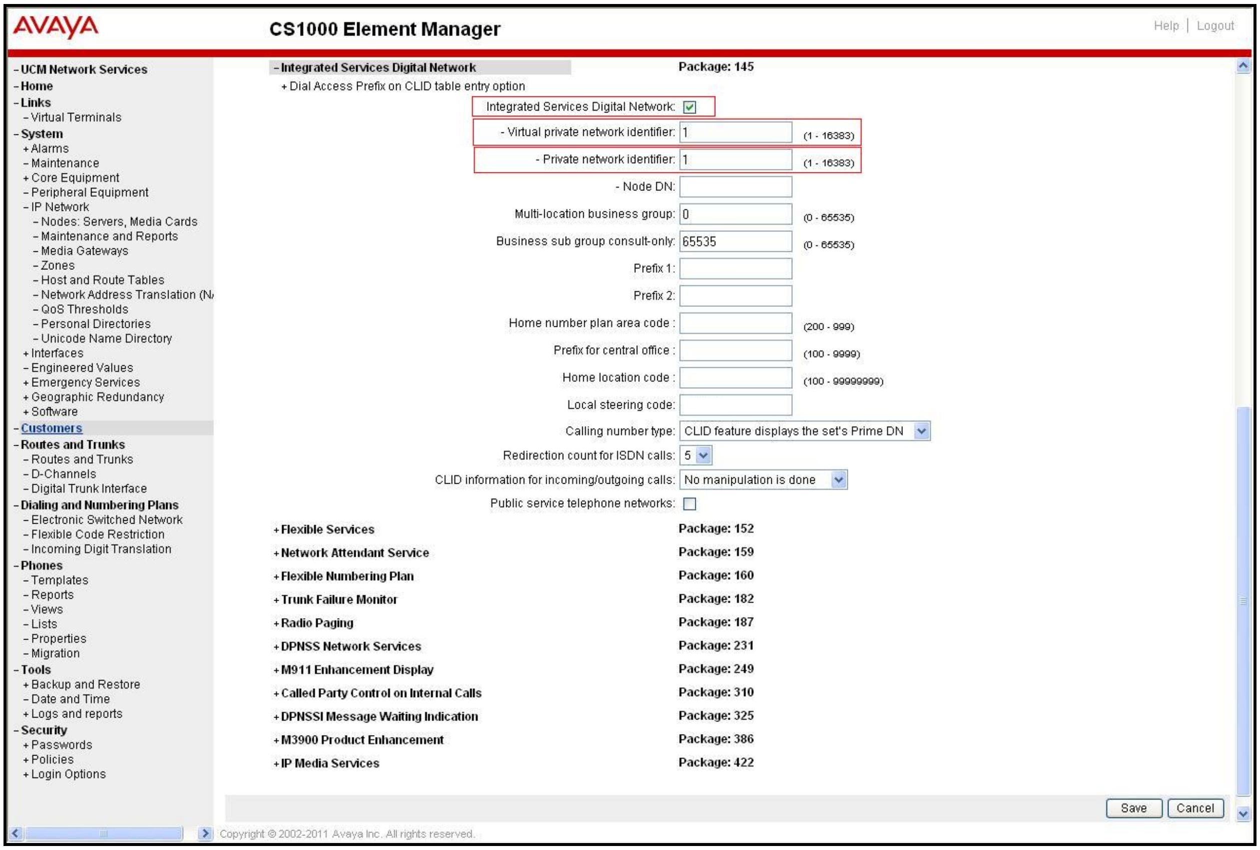

Figure 4:22 Customer – ISDN Configurations

4.5.2. Administer SIP Trunk Gateway to SM

a) Select **IP Network** -> **Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this CS1K system. The **Node Details** screen is displayed as shown in **Figure 4:5, Section 4.2.1.**

b) On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

c) Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following testing values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 4:23**. The parameters (highlighted in red boxes) are filled in, which were obtained when user creates a SIP profile in SM (these are shown in **Section 5.4**).

- **Vtrk gateway application**: **SIP Gateway (SIPGw)**
- **SIP domain name**: TELUS.com
- **Local SIP port**: 5060
- **Gateway endpoint name**: car1-cores1 (the FQDN of the CS1K)
- **Application node ID**: 1000 (this should match the Node ID configured in Section 4.2.1)

©2011 Avaya Inc. All Rights Reserved.

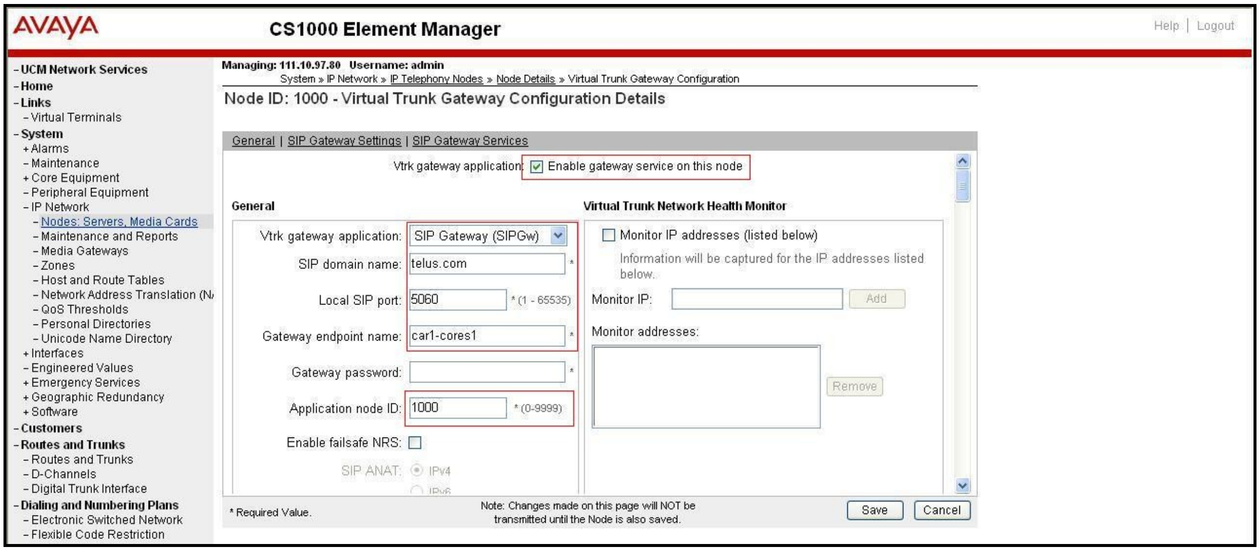

Figure 4:23 Virtual Trunk Gateway Configuration Details Page 1

d) Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 4:24**.

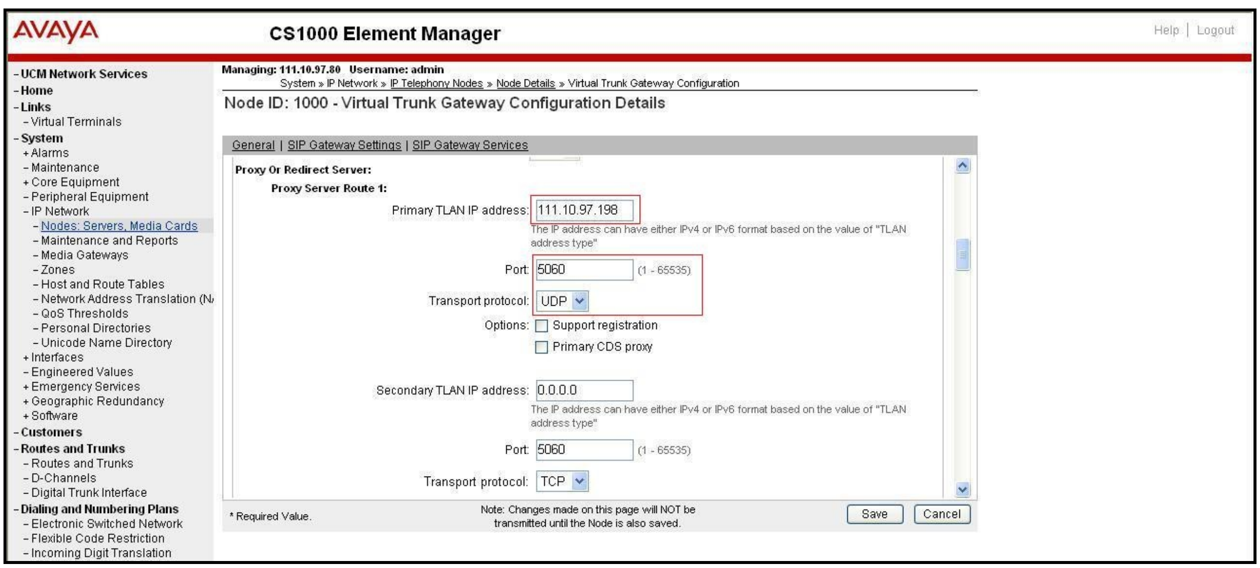

Figure 4:24 Virtual Trunk Gateway Configuration Details Page 2

e) On the same page as shown in **Figure 4:25**, scroll down to the **SIP URI Map** section (**Figure 18**).

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

©2011 Avaya Inc. All Rights Reserved.

Under the **Private E.164 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

Note: These fields are blank in correspondence with the Avaya DevConnect lab configuration, it is possible that customer installations will have domains names configured here.

Then click on the **Save** button.

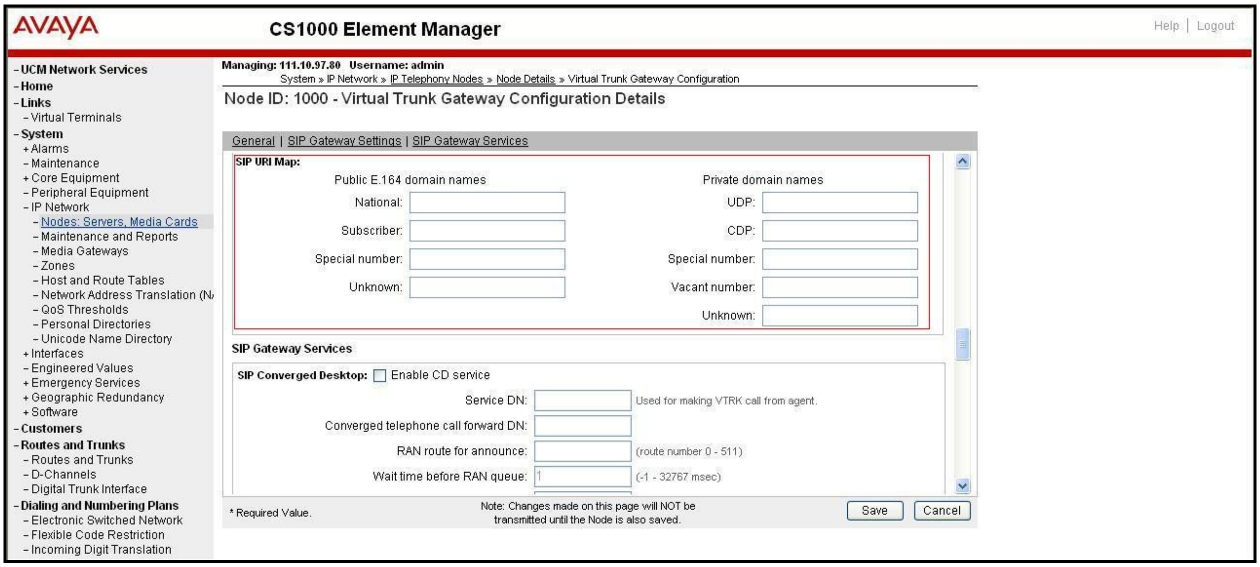

Figure 4:25 Virtual Trunk Gateway Configuration Details Page 3

©2011 Avaya Inc. All Rights Reserved.

4.5.3. Administer Virtual D-Channel

a) Select **Routes and Trunks** -> **D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown in **Figure 4:26**. Click on **to Add** button**.**

Figure 4:26 D-Channels

b)

©2011 Avaya Inc. All Rights Reserved.

The D-Channels 100 Property Configuration screen is displayed next as shown in **Figure 4:27**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type (CTYP): D-Channel is over IP (DCIP)**
- **Designator (DES)**: A descriptive name
- **Interface type for D-channel (IFC): Meridian Meridian1 (SL1)**
- **Meridian 1 node type: Slave to the controller (USR)**
- **Release ID of the switch at the far end (RLS): 25**
- **Advanced options (ADVOPT):** check on **Network Attendant Service Allowed**

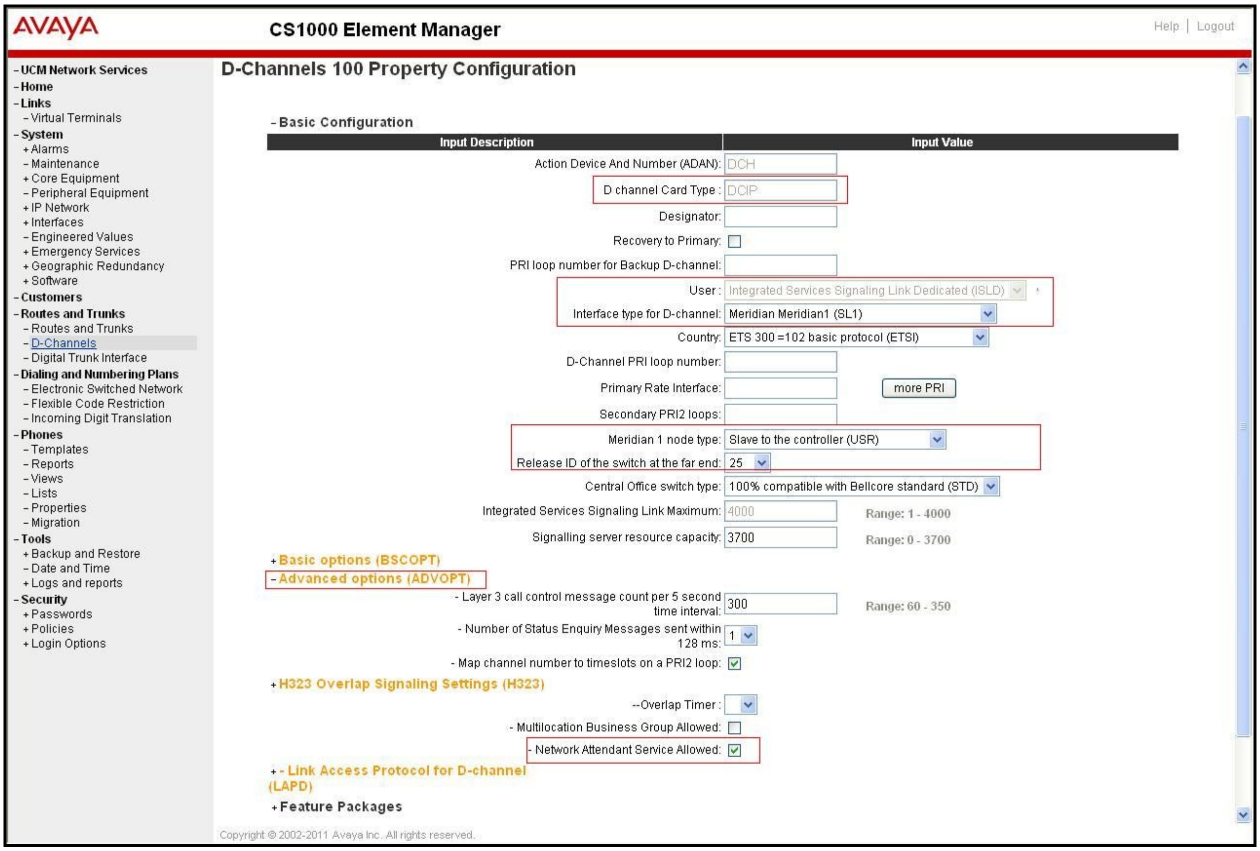

Figure 4:27 D-Channels Configuration Details

c) Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities** (**RCAP**) attribute as shown in **Figure 4:28**. The **Remote Capabilities Configuration** page will appear. Then check on the **ND2** and the **MWI** (if PSTN mailboxes are present on the CS1K Call Pilot) checkboxes as shown in **Figure 4:29**.

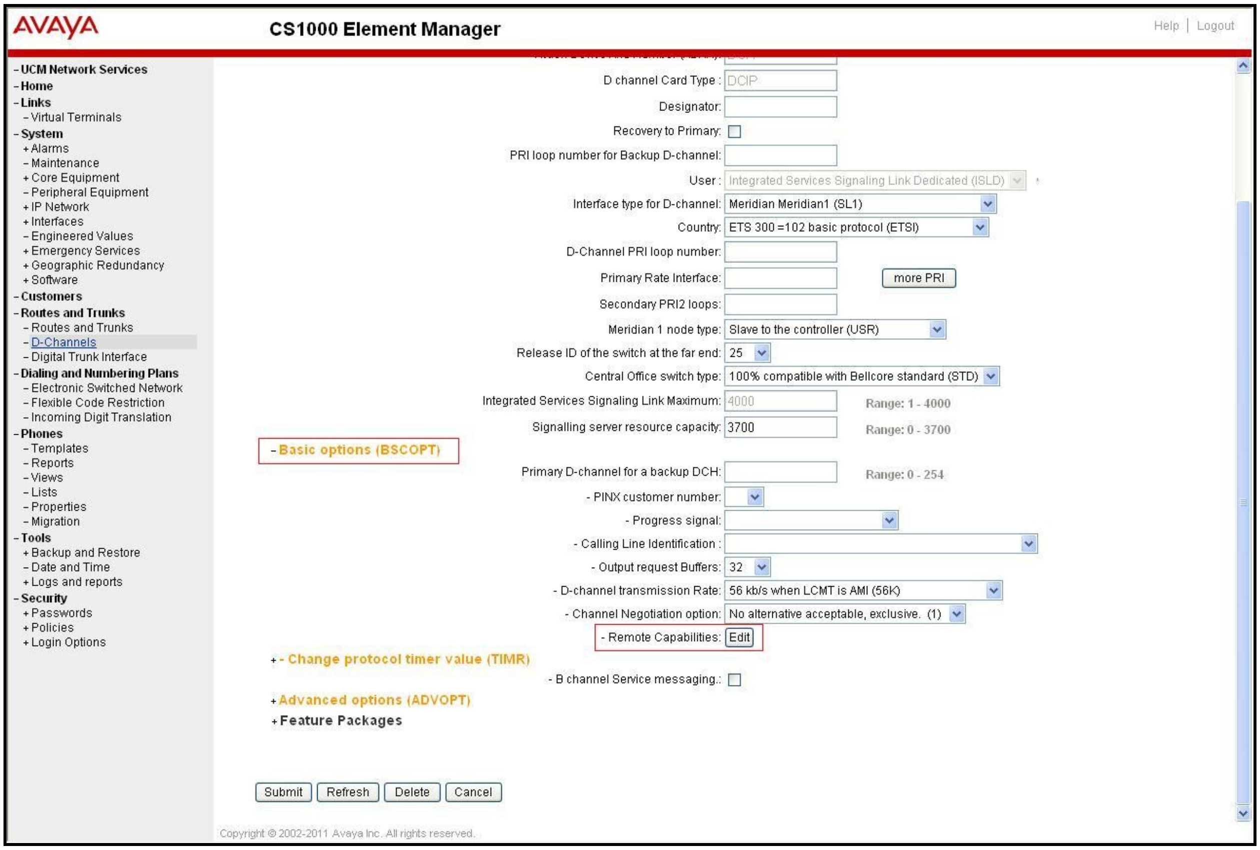

Figure 4:28 D-Channels Configuration Details

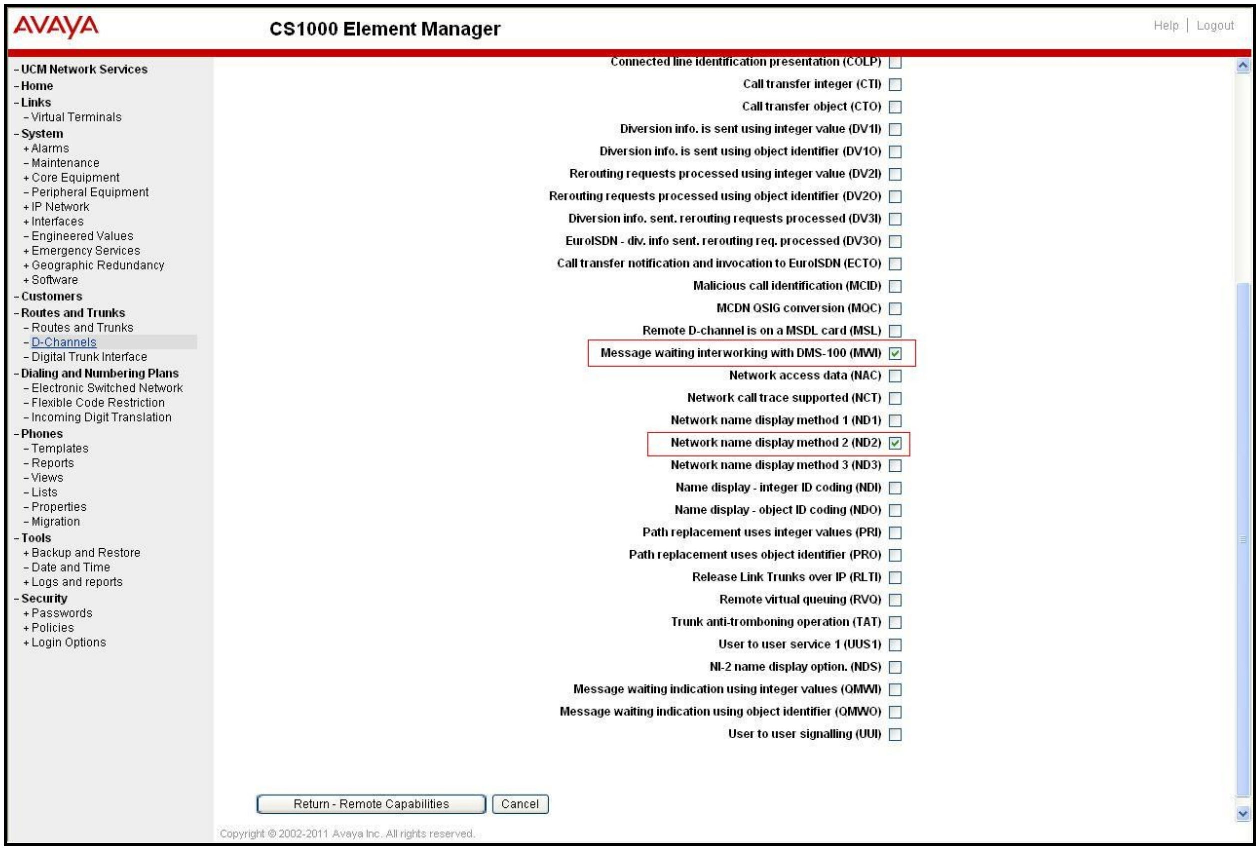

Figure 4:29 Remote Capabilities Configuration Details

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

4.5.4. Administer Virtual Super-Loop

Select **System** -> **Core Equipments** -> **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click "**Add**" button to create a new one as shown in **Figure 4:30**. In this example, Superloop 100 is being added and used.

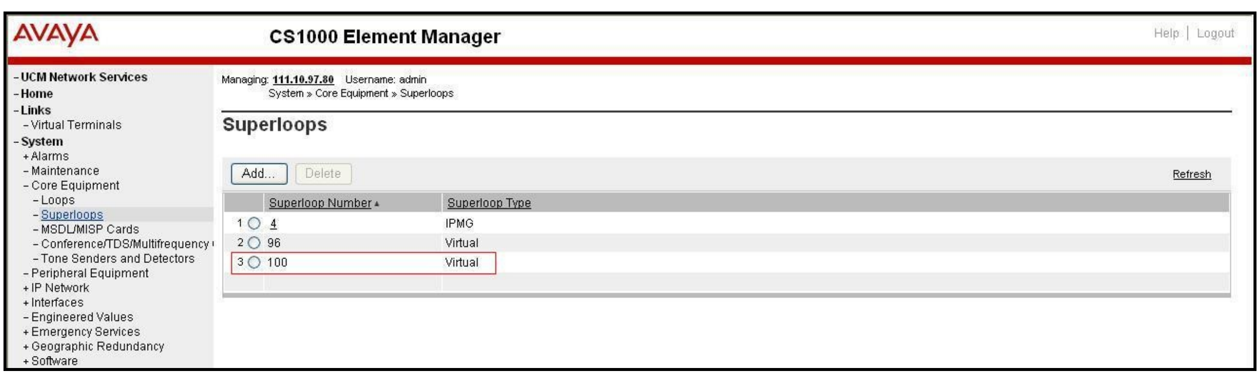

Figure 4:30 Administer Virtual Super-Loop

4.5.5. Enable Music for Customer Data Block

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options. The **Customer 00 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.
b) The screen is updated with a list of F**eature Packages** populated. Select **Enhanced Music** to edit its parameters. Check to enable music for Customer 00, define music route 1 as show in the redbox of **Figure 4:31**. The CS1K system has been pre-configured with music route 1.
c) Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

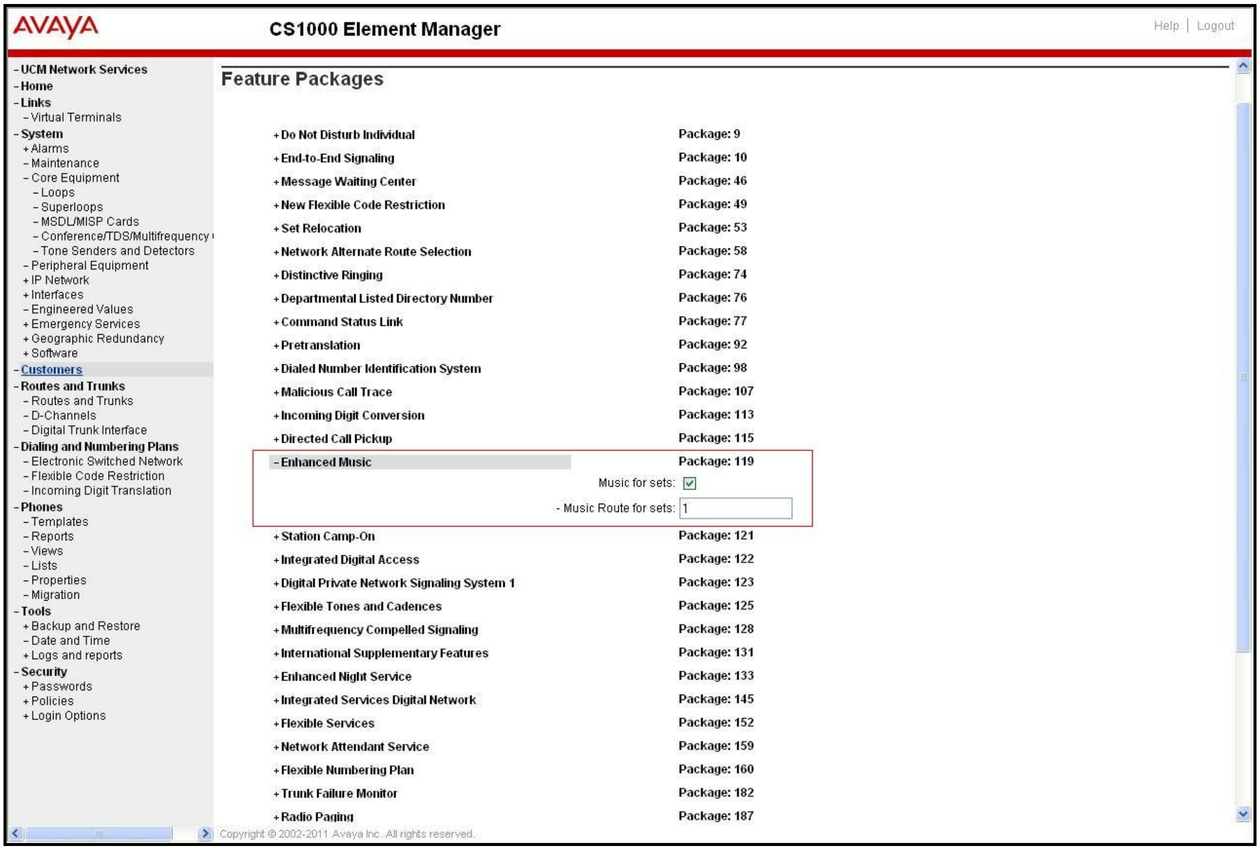

Figure 4:31 Enable Music for Customer 01

4.5.6. Administer Virtual SIP Routes

a) Select **Routes and Trunks** -> **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 4:32**.

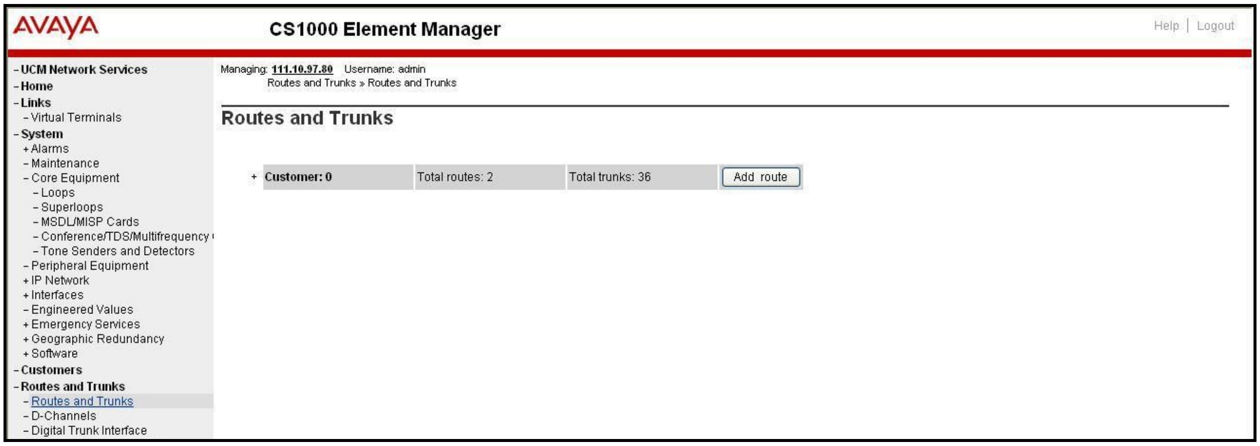

Figure 4:32 Add route

b) The **Customer 0**, New **Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 4:33**.

- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: **TIE trunk data block (TIE)**
- **Incoming and Outgoing trunk** (**ICOG**): **Incoming and Outgoing (IAO)**
- **Access Code for the trunk route (ACOD)**: An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 4.4.2**).
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number 1000 (created in **Section 4.2.1**).
- 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 4.5.3**)
    - **Network calling name allowed (NCNA)**: Check the field.
    - **Network call redirection (NCRD)**: Check the field.
    - **Insert ESN access code (INAC):** Check the field.

©2011 Avaya Inc. All Rights Reserved.

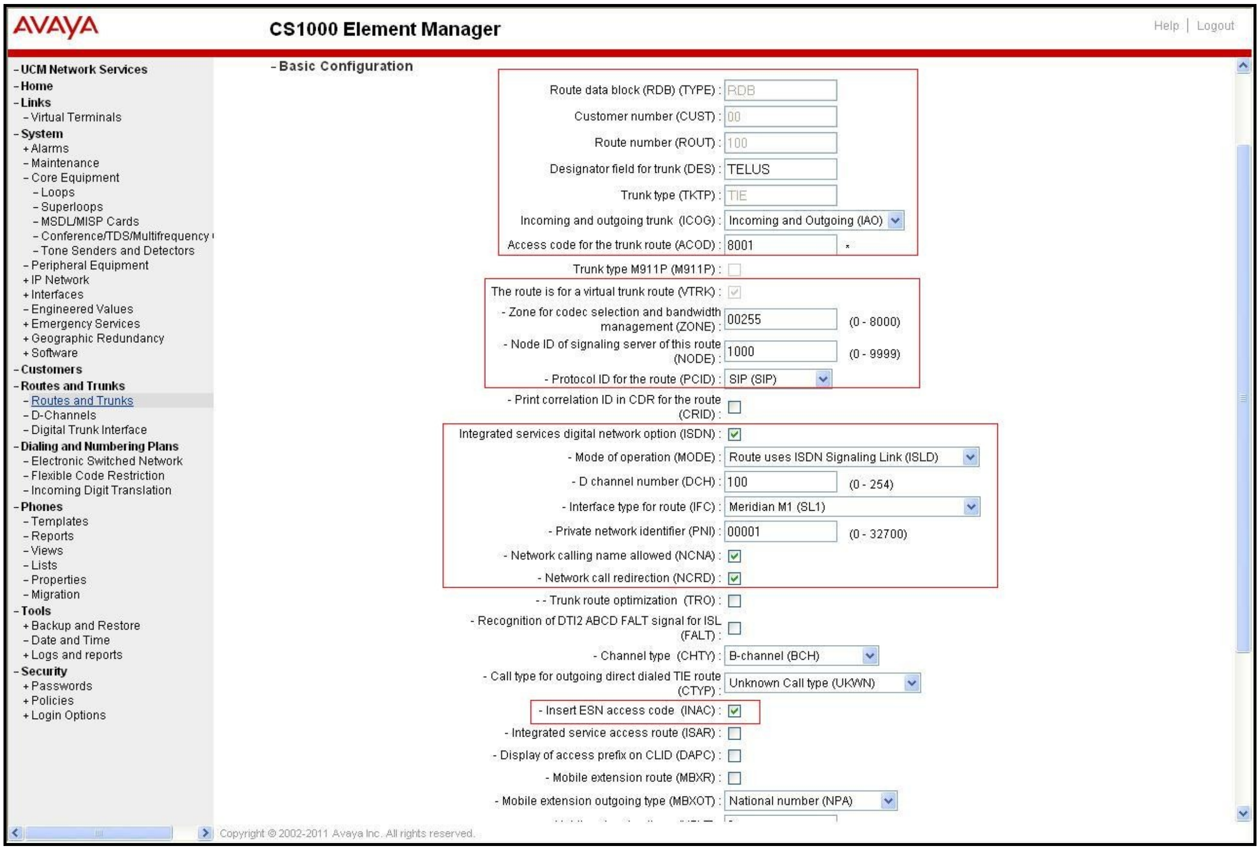

Figure 4:33 Route Configuration Details Pages 1

- 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 4:34**.

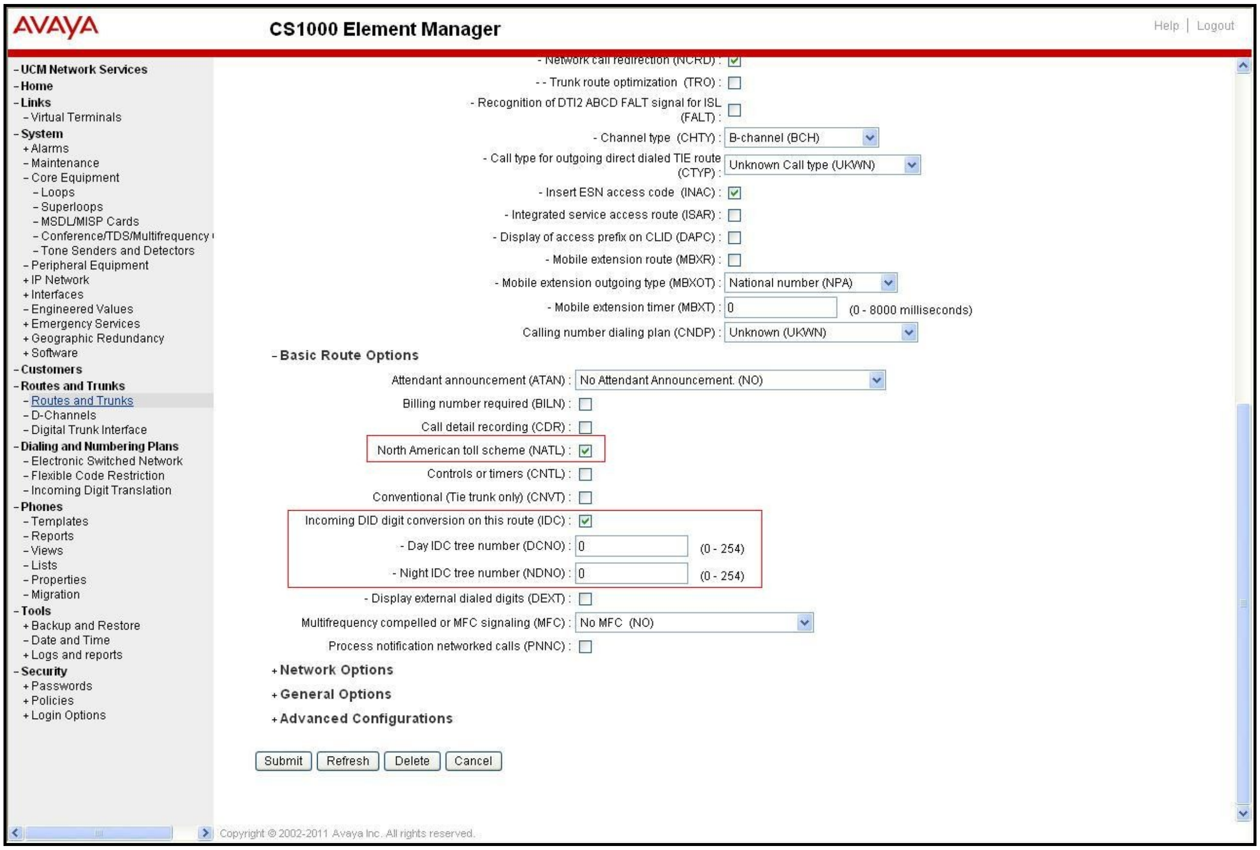

Figure 4:34 Route Configuration Details Pages 2

- Click on **Advance Configurations**; check **Music-on-hold** to enable music on hold on the route. Input music route 1 to the boxes as shown in **Figure 4:35**. The CS1K system has been pre-configured with route 1 as a music route.

©2011 Avaya Inc. All Rights Reserved.

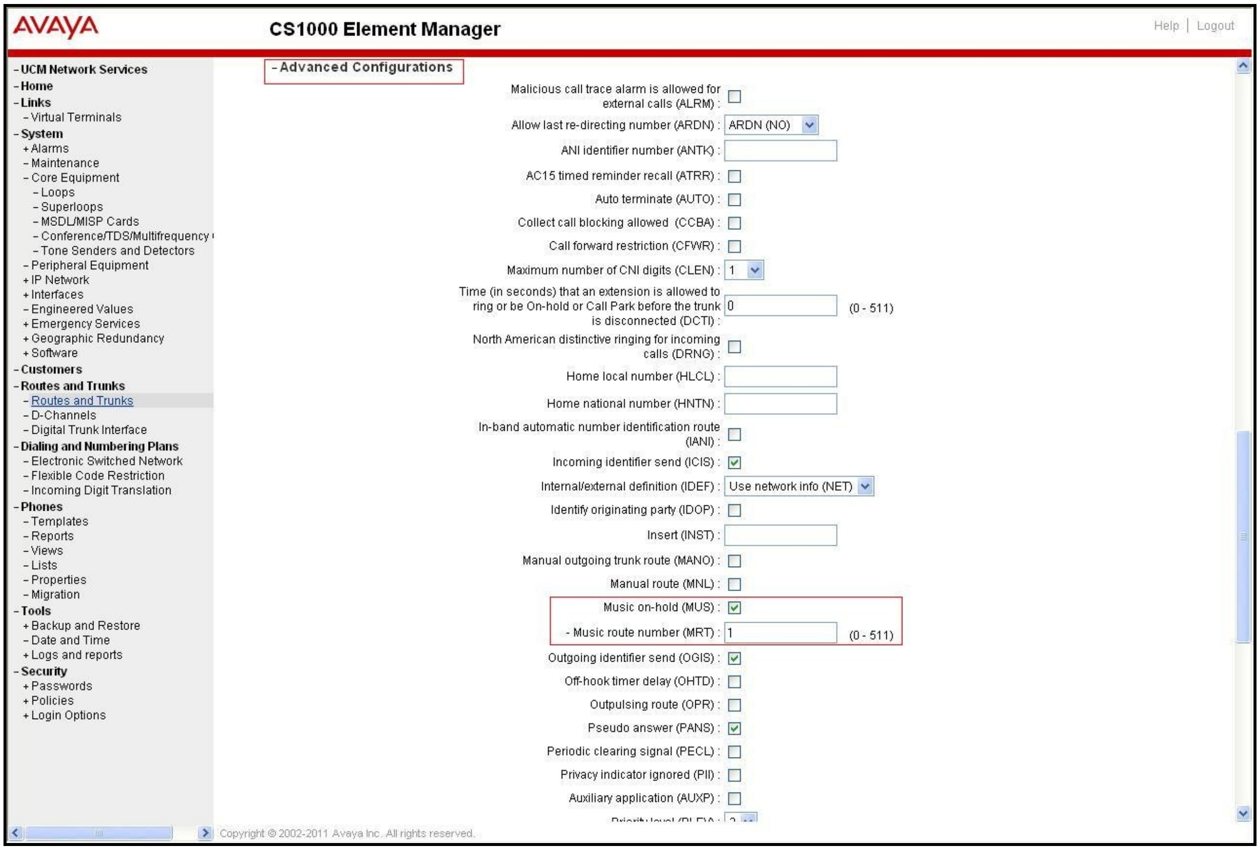

Figure 4:35 Route Configuration Details Pages 3

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

4.5.7. Administer Virtual Trunks

a) Continue **Section 4.5.6**, after click **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 100 was being added. Click on the **Add trunk** button next to the newly added route 100 as shown in **Figure 4:36**.

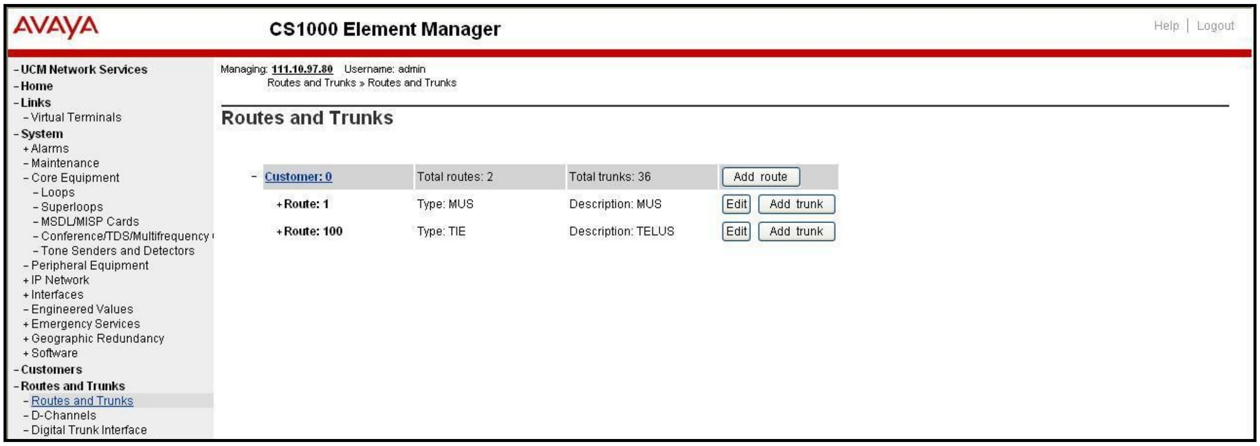

Figure 4:36 Route and Trunks

b) The **Customer 00, Route 100, Trunk 1 Property Configuration** screen is displayed in **Figure 4:37.** Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom basic trunk configuration page. Click on the **Edit** button as shown in **Figure 4:37**.

- 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 4.5.4**)
- **Designator field for trunk** (**DES**): A descriptive text
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**
- **Member number** (**RTMB**): Current route number and starting member
- **Start arrangement Incoming** (**STRI**): **Immediate (IMM)**
- **Start arrangement Outgoing (STRO)**: **Immediate (IMM)**
- **Trunk Group Access Restriction (TGAR)**: Desired trunk group access restriction level
- **Channel ID for this trunk** (**CHID**): An available starting channel ID

©2011 Avaya Inc. All Rights Reserved.

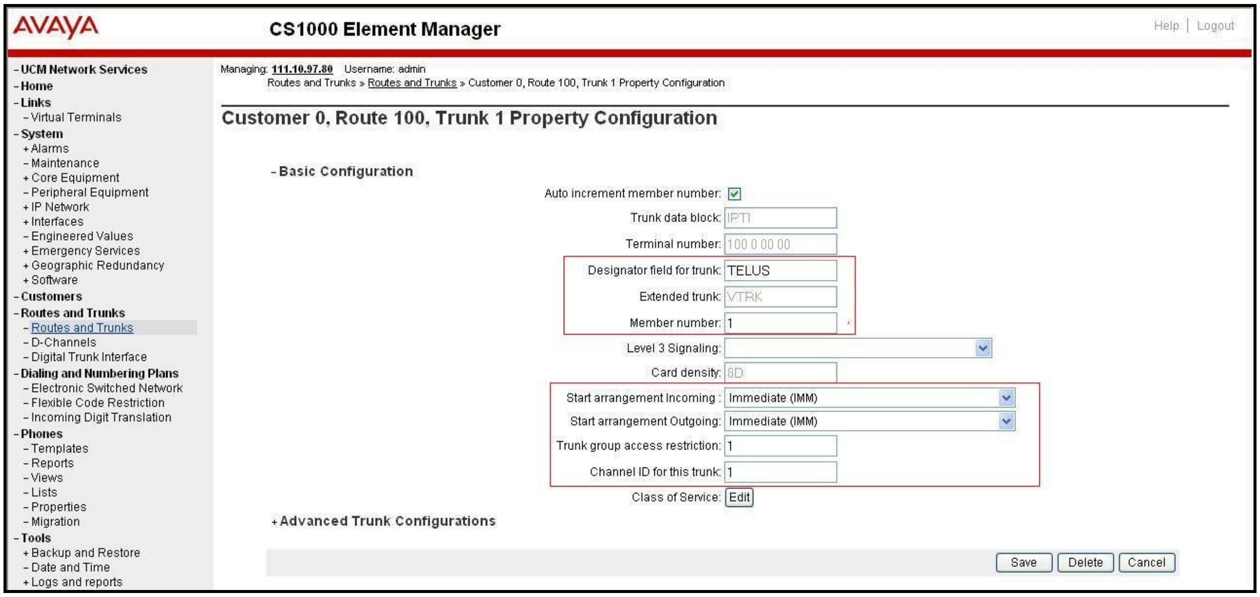

Figure 4:37 New Trunk Configuration Details

©2011 Avaya Inc. All Rights Reserved.

c) For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in **Figure 4:38**. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).

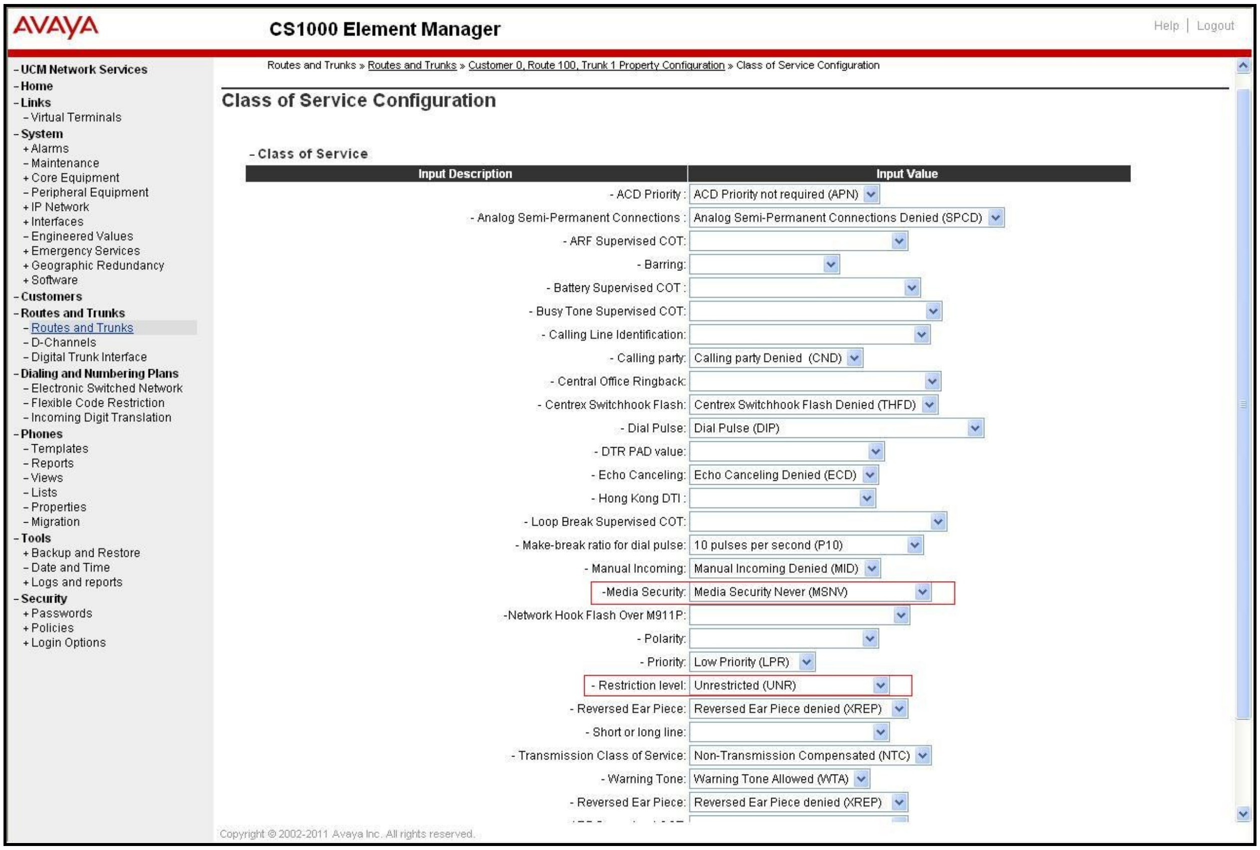

Figure 4:38 Class of Service Configuration Details Page

©2011 Avaya Inc. All Rights Reserved.

4.5.8. Administer Calling Line Identification Entries

a) Select **Customers** > **00** > **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in **Figure 4:39**.

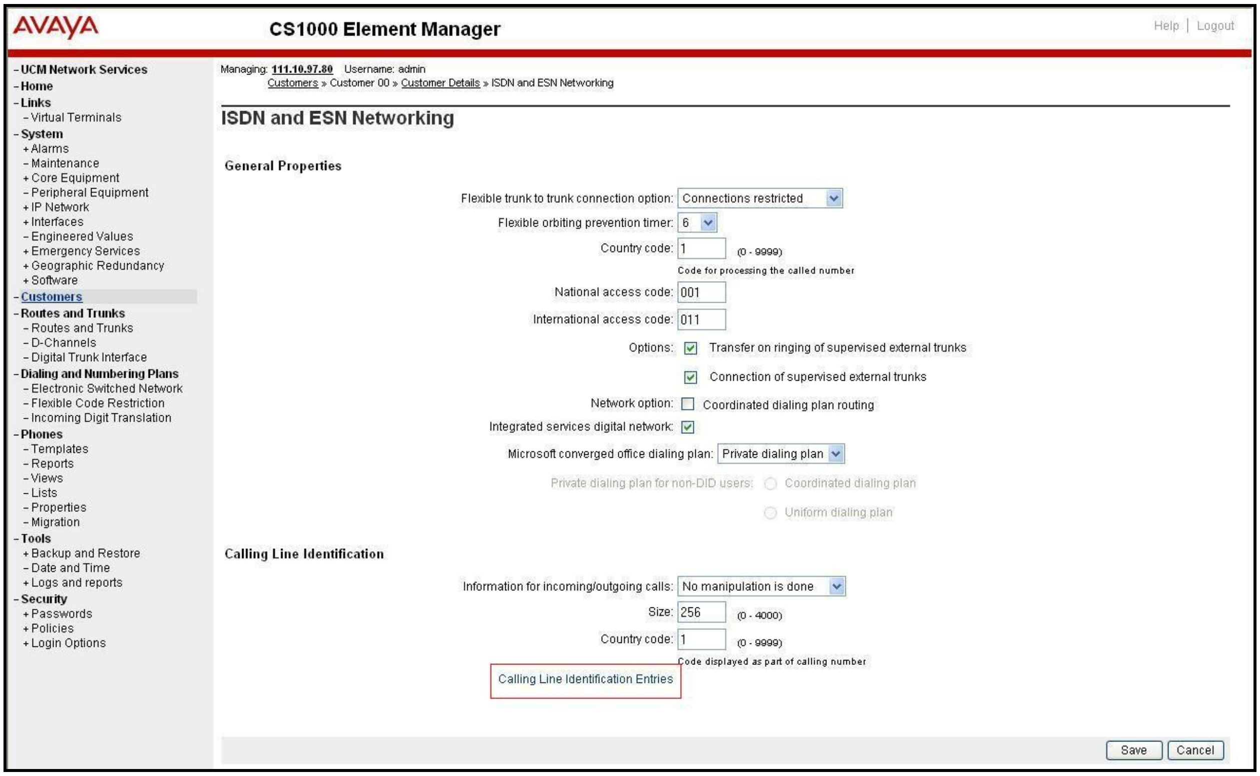

Figure 4:39 ISDN and ESN Networking

b) Click on **Add** as shown in **Figure 4:40**.

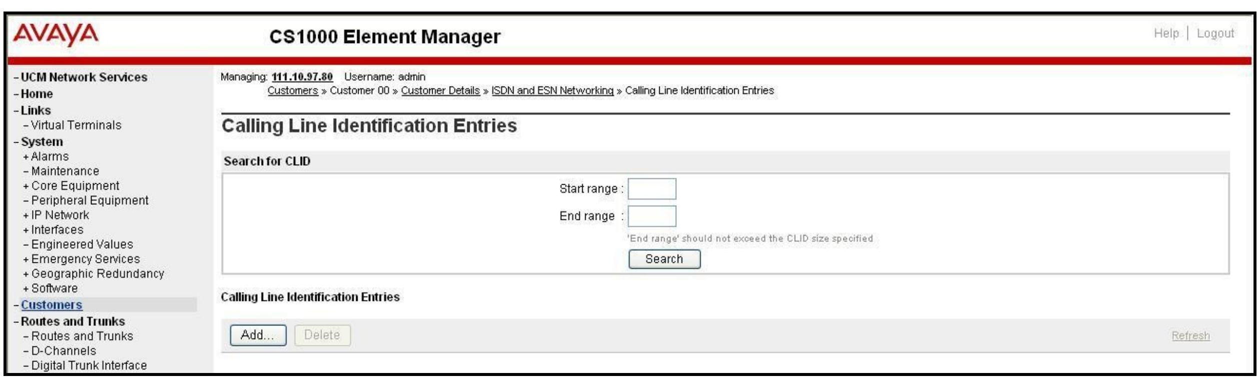

Figure 4:40 Calling Line Identification Page

c) Add entry **0** as shown in **Figure 4:41**

- **National Code**: leave as blank

©2011 Avaya Inc. All Rights Reserved.

- **Local Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits – 403692. This **Local Code** will be used for call display purpose of outbound international call configuration in **Section 4.6.6** in where the **Special Number 0** is associated with 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**.

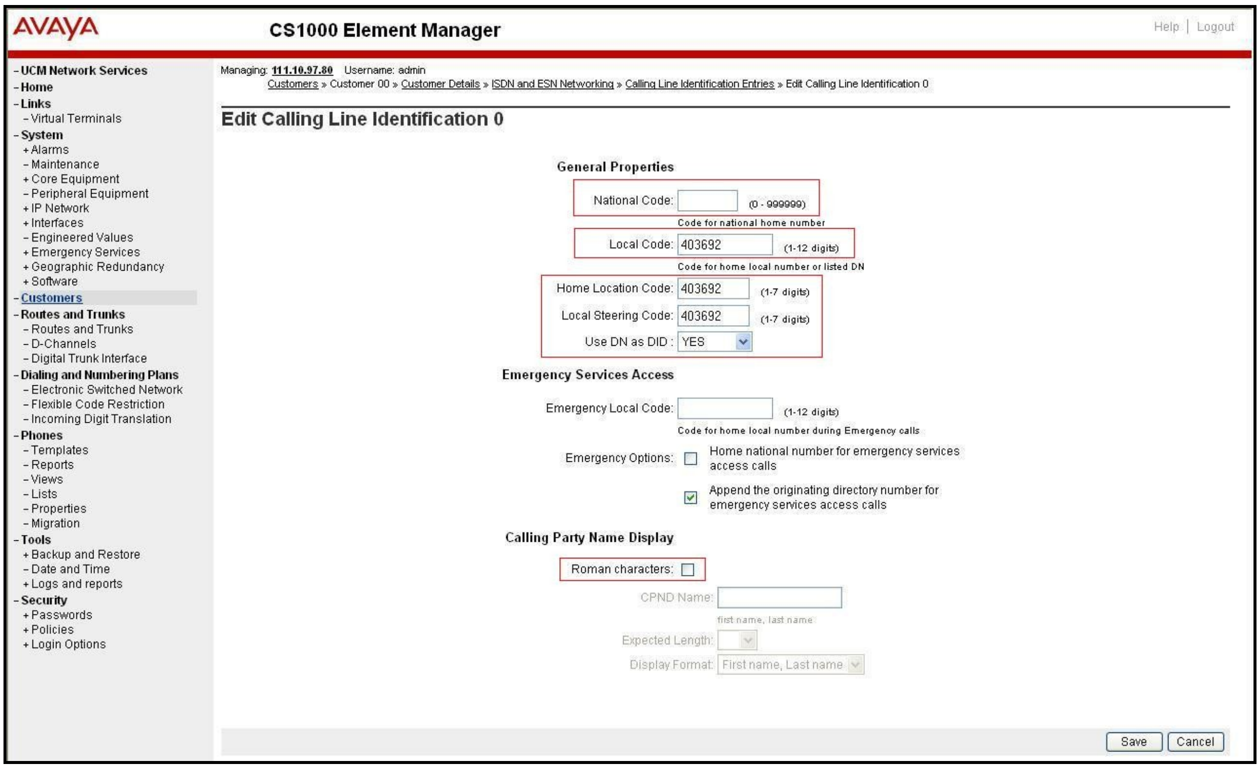

Figure 4:41 Edit Calling Line Identification 0

d) Click on **Save**.

4.5.9. Enable External Trunk to Trunk Transferring

This section shows how to enable External Trunk to Trunk Transferring feature which is a mandatory configuration to make call transfer and conference work properly over SIP trunk.
a) Login Call Server CLI (please refer to **Section 4.1.2** for more detail)
b) Allow External Trunk To Trunk Transferring for **Customer Data Block** by using LD 15

©2011 Avaya Inc. All Rights Reserved.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600176    USED U P: 8325631 954062    TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
…
TRNX yes
EXTT yes
…
```

4.6. Administer Dialing Plans

4.6.1. Define ESN Access Codes and Parameters (ESN)

a) Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen. **Select ESN Access Code and Parameters (ESN)** as shown in **Figure 4:42**.

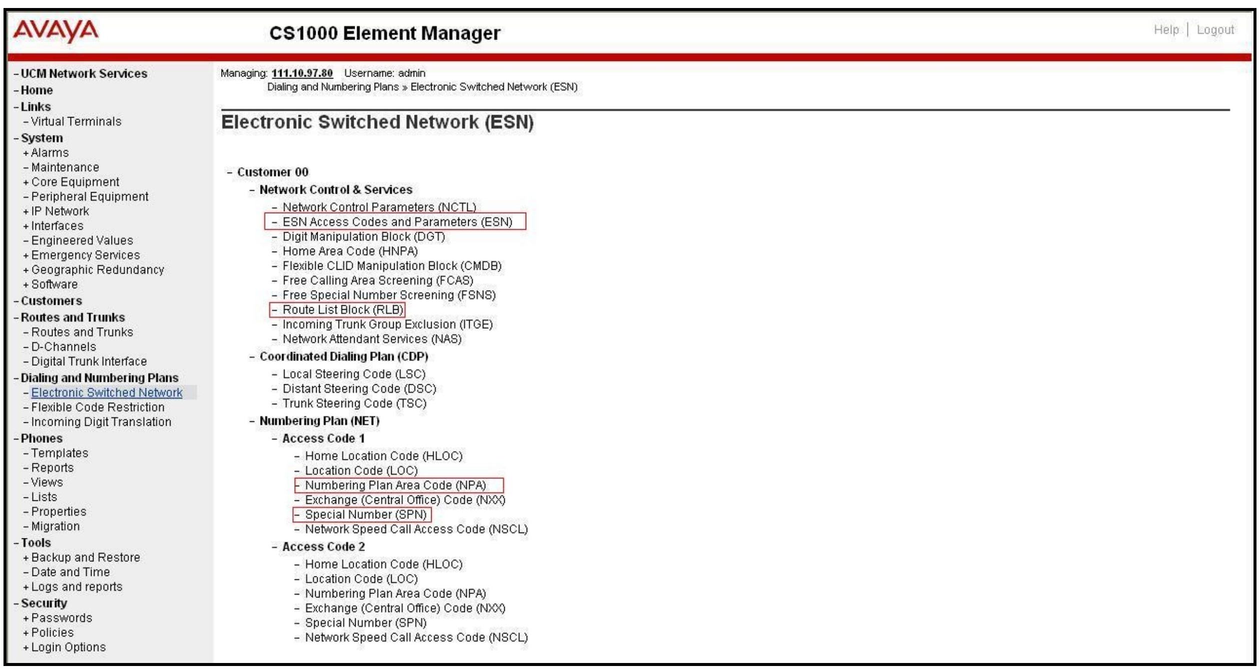

Figure 4:42 Electronic Switch Network (ESN)

b) In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** as shown in **Figure 4:43**.

©2011 Avaya Inc. All Rights Reserved.

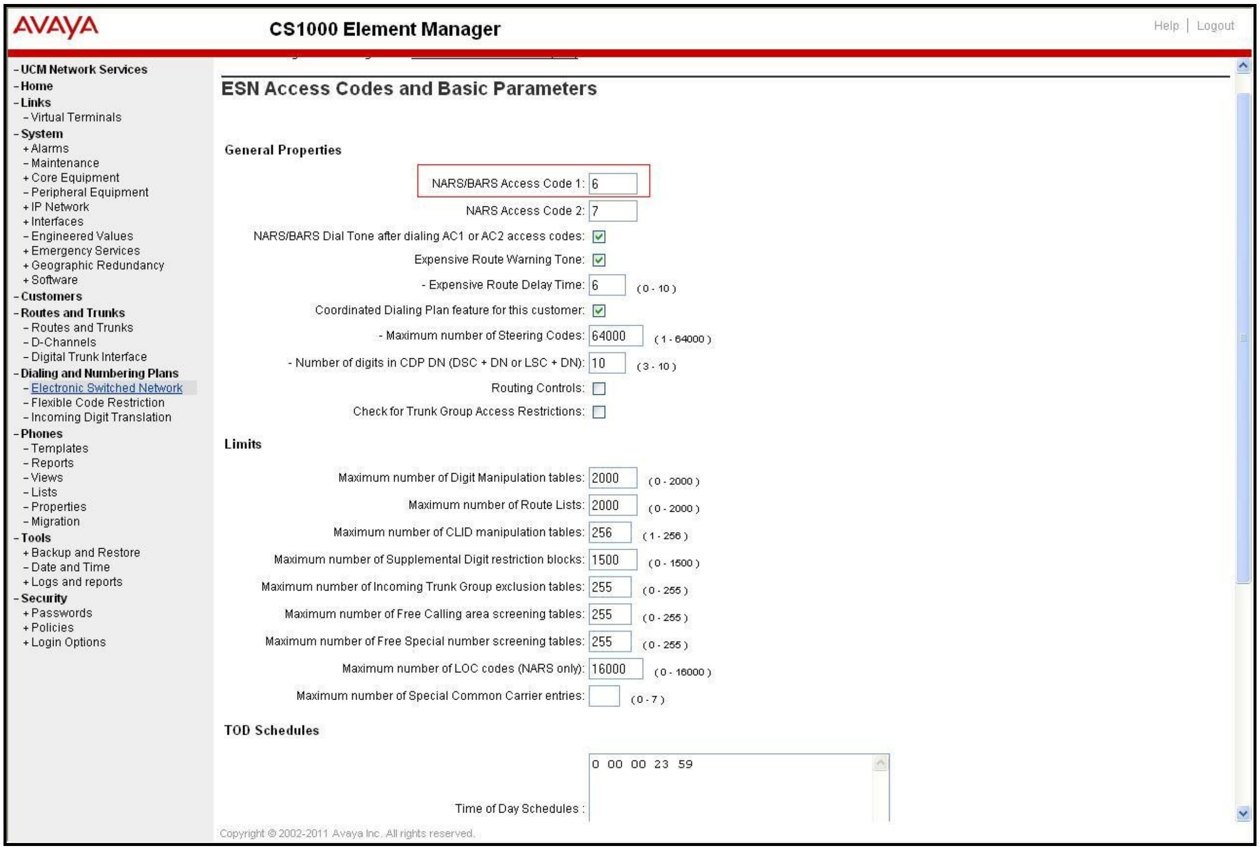

Figure 4:43 ESN Access Codes and Basic Parameters

c) Click **Submit** (not shown).

4.6.2. Associate NPA and SPN call to ESN Access Code 1

a) Login Call Server CLI (please refer to **Section 4.1.2** for more detail)
b) In LD 15, change Customer Net_Data block by disabling NPA and SPN to be associated to Access Code 2. It means Access Code 1 will be used for NPA and SPN calls.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35717857    USED U P: 8241949 920063    TOT: 44879869
DISK SPACE NEEDED: 1697 KBYTES
REQ: chg
TYPE: net_data
CUST 0
OPT
AC2 xnpa xspn
FNP
CLID
ISDN
…
```


©2011 Avaya Inc. All Rights Reserved.

c) 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
AC2
FNP YES
…
```

4.6.3. Digit Manipulation Block (DMI)

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Digit Manipulation Block** (DGT) as shown in **Figure 4:42**.

b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click **to Add** as shown in **Figure 4:44**.

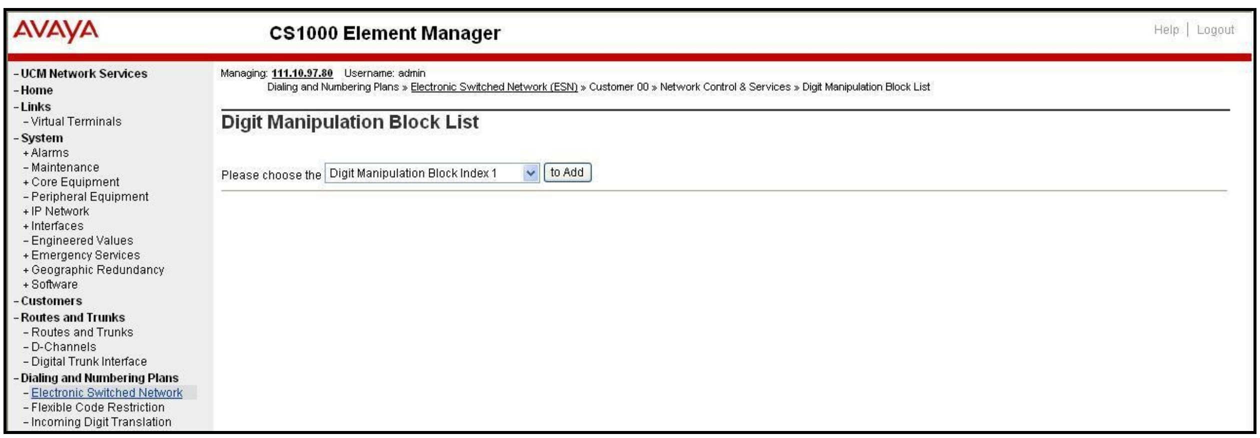

Figure 4:44 Digit Manipulation Block List

c) Enter **0** for the **Number of leading digits to be Deleted** (Del) field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** (CTYP) and then click **Submit** as shown in **Figure 4:45**.

©2011 Avaya Inc. All Rights Reserved.

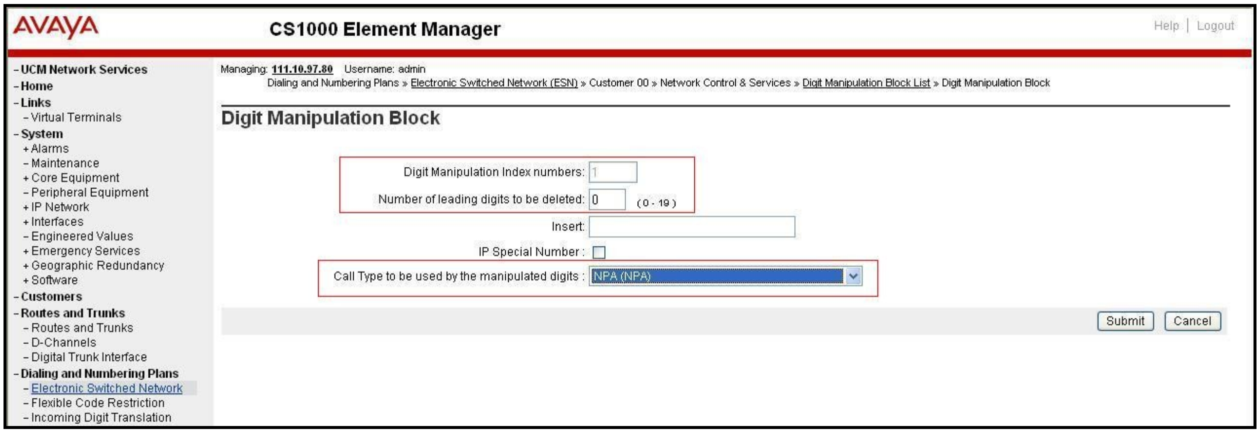

Figure 4:45 Digit Manipulation Block

4.6.4. Route List Block (RLB) (RLB 100)

This section shows how to add a RLB associated with the DMI created in **Section 4.6.3**.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Route List Block** (RLB) as shown in **Figure 4:42**.

b) Select an available value in the textbox for the **route list index** and click on the **"to Add"** button (in this case is 100) as shown in **Figure 4:46**.

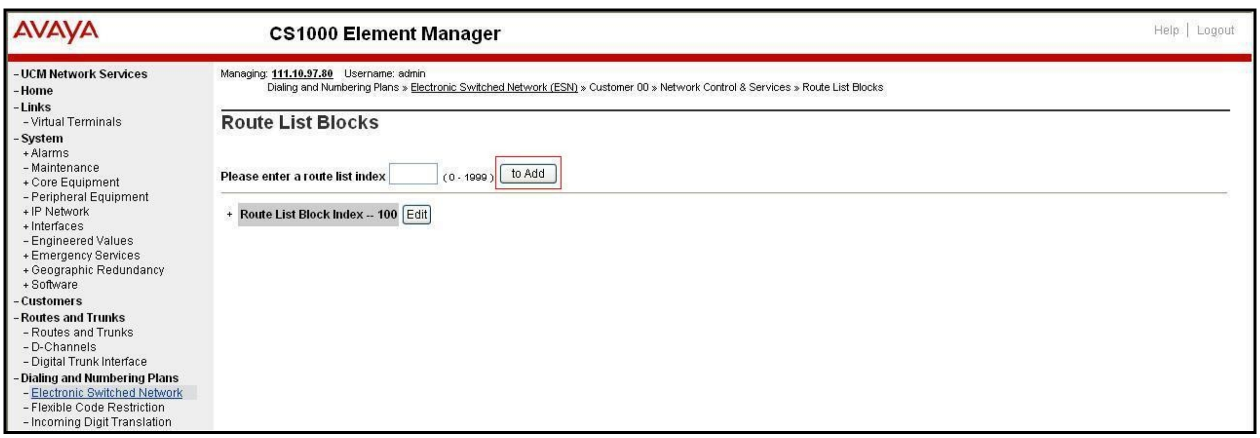

Figure 4:46 Route List Blocks

c) Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 4:47**. Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route number** (ROUT): 100 (created in **Section 4.5.6**)
- **Digit Manipulation Index** (DMI): 1 (created in **Section 4.6.3**)

©2011 Avaya Inc. All Rights Reserved.

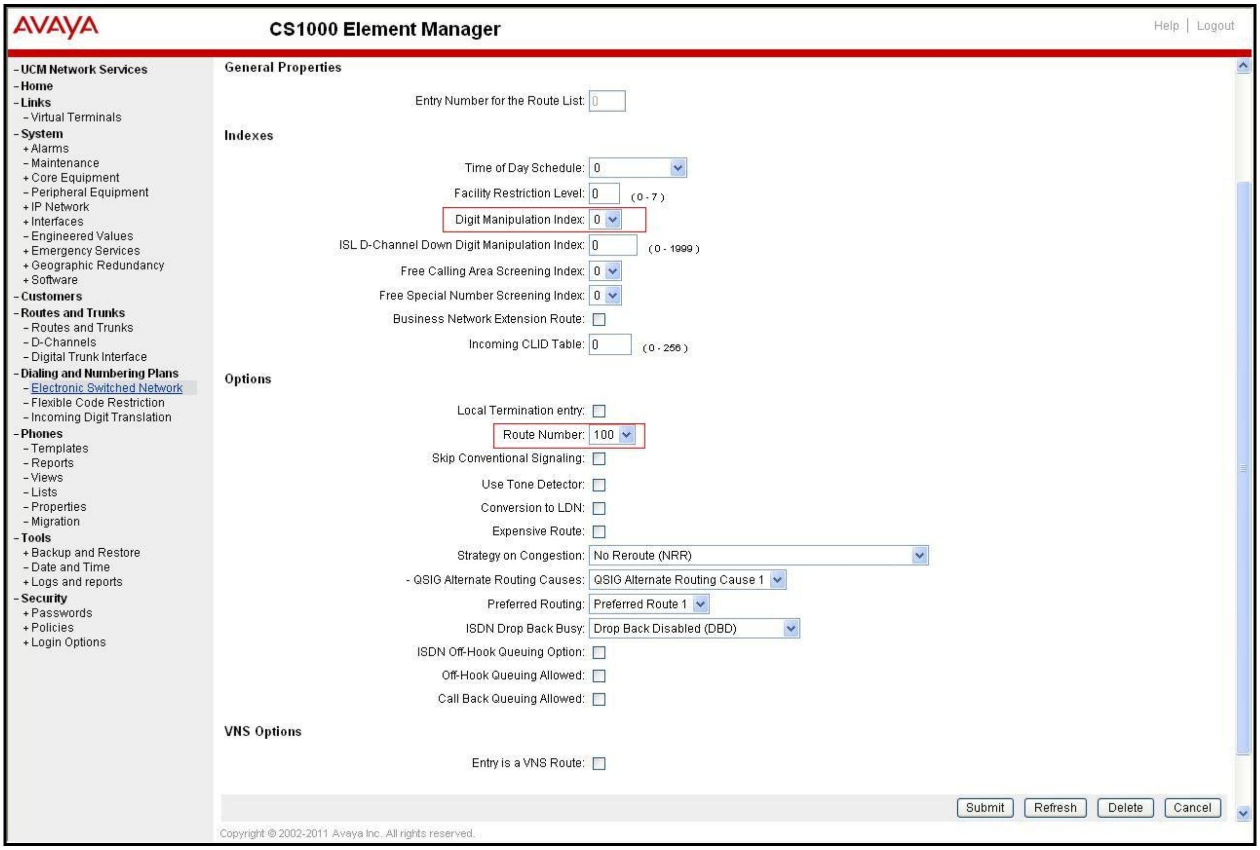

Figure 4:47 Route List Blocks Configuration Details

4.6.5. Inbound Call Digit Translation

This section describes the steps for receiving the calls from PSTN via the TELUS system.
a) Select **Dialing and Numbering Plans** -> **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown in **Figure 4:48**

Figure 4:48 Incoming Digit Translation

b) Click on the **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number (**DCN0**) 1 has been created as shown in **Figure 4:49**.

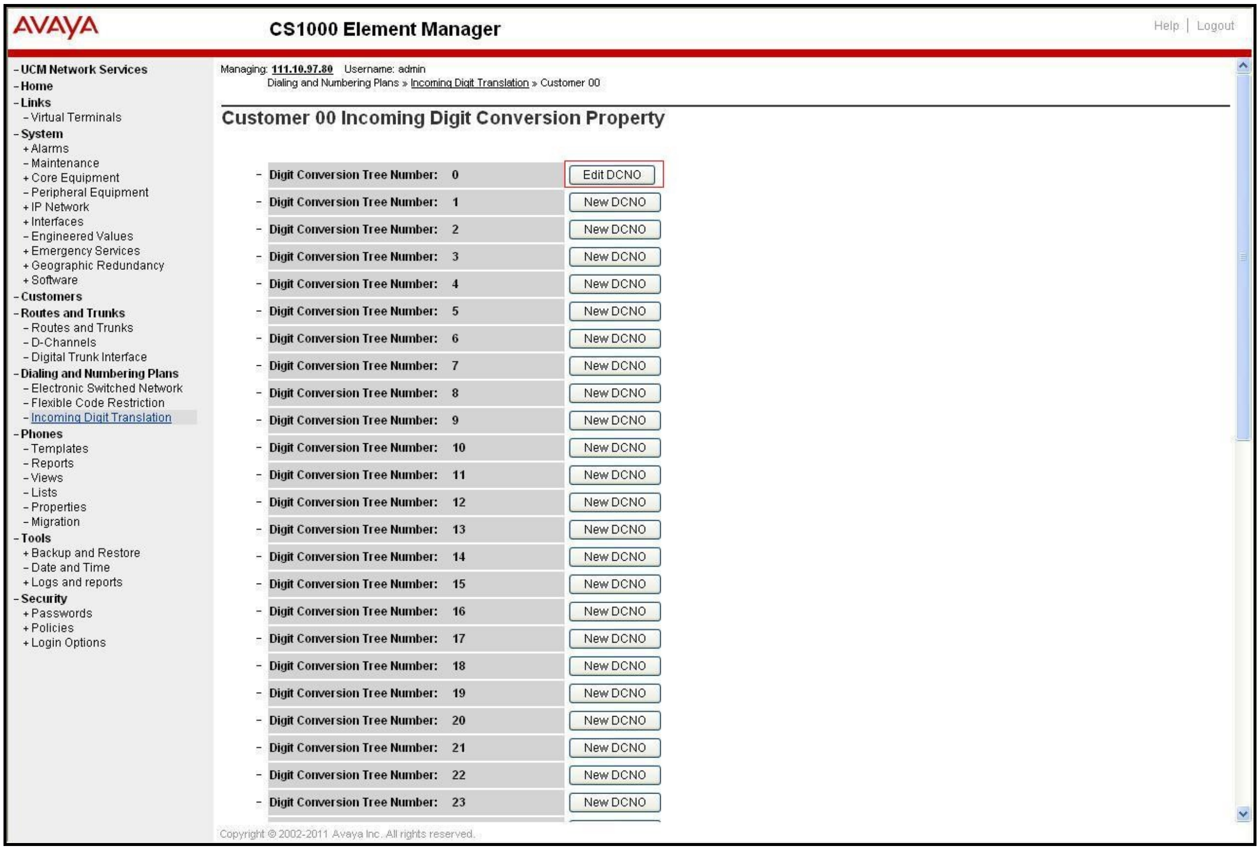

Figure 4:49 Incoming Digit Conversion Property

c) Detail configuration of the **DCNO** is shown in **Figure 4:50**. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1K system phones DN. This **DCN0** has been assigned to route 100 as shown in **Figure 4:34**.
In the following configuration, the incoming call from PSTN with the prefix 403692946X will be translated to CS1K DN 946X. The DID 4036929468 is translated to 1700 for Voicemail accessing purpose.

©2011 Avaya Inc. All Rights Reserved.

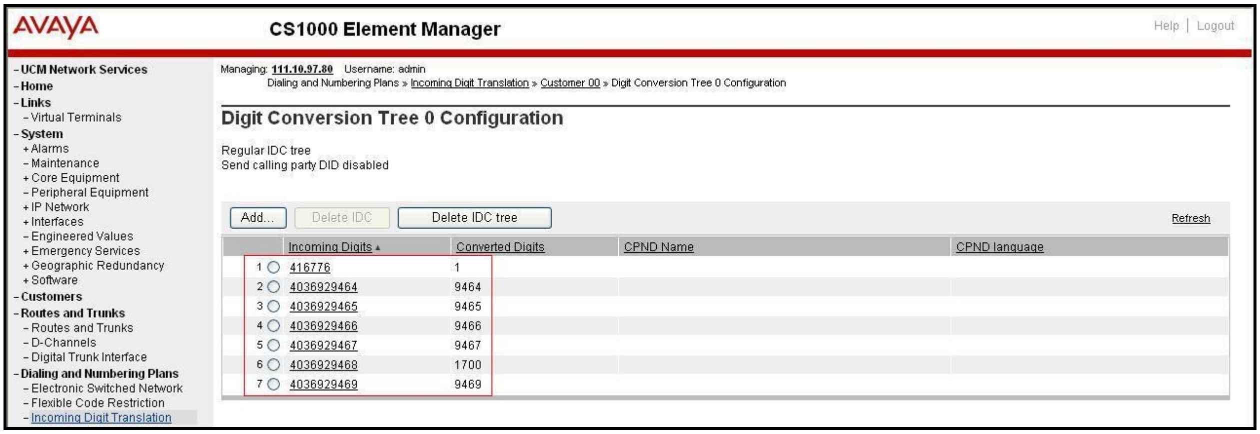

Figure 4:50 Digit Conversion Tree Configuration

4.6.6. Outbound Call - Special Number Configuration.

There are special numbers which have been configured to be used for this testing such as; **0** to reach Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911** and so on.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Special Number** (SPN) as shown in **Figure 34**.
b) Enter SPN and then click on the "**to Add**" button. **Figure 4:51** shows all the special numbers were used for this testing.

Special Number: 0

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType:** NONE
- **Route list index:** 100, created in **Section 4.6.4**

Special Number: 1

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType**: NATL
- **Route list index**: 100, created in **Section 4.6.4**

Special Number: 411

- **Flexible length**: 3
- **CallType**: NATL
- **Route list index**: 100, created in **Section 4.6.4**

Special Number: 911

- **Flexible length**: 3
- **CallType**: NATL

©2011 Avaya Inc. All Rights Reserved.

- **Route list index**: 100, created in **Section 4.6.4**

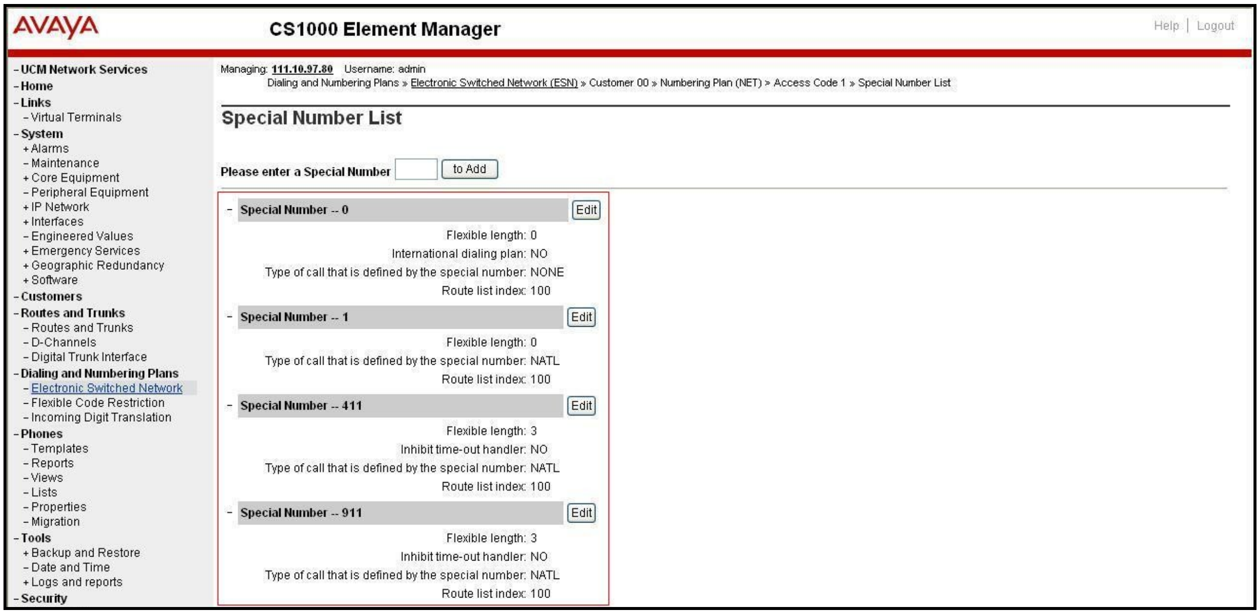

Figure 4:51 Special Number List

4.6.7. Outbound Call - Numbering Plan Area (NPA)

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

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Numbering Plan Area Code** (NPA) as shown in **Figure 4:42**.
b) Enter area code desired in the textbox and click on the "**to Add**" button. **Figure 4:52** shows NPA numbers **613** configured for this testing. These codes are associated to SIP route.

©2011 Avaya Inc. All Rights Reserved.

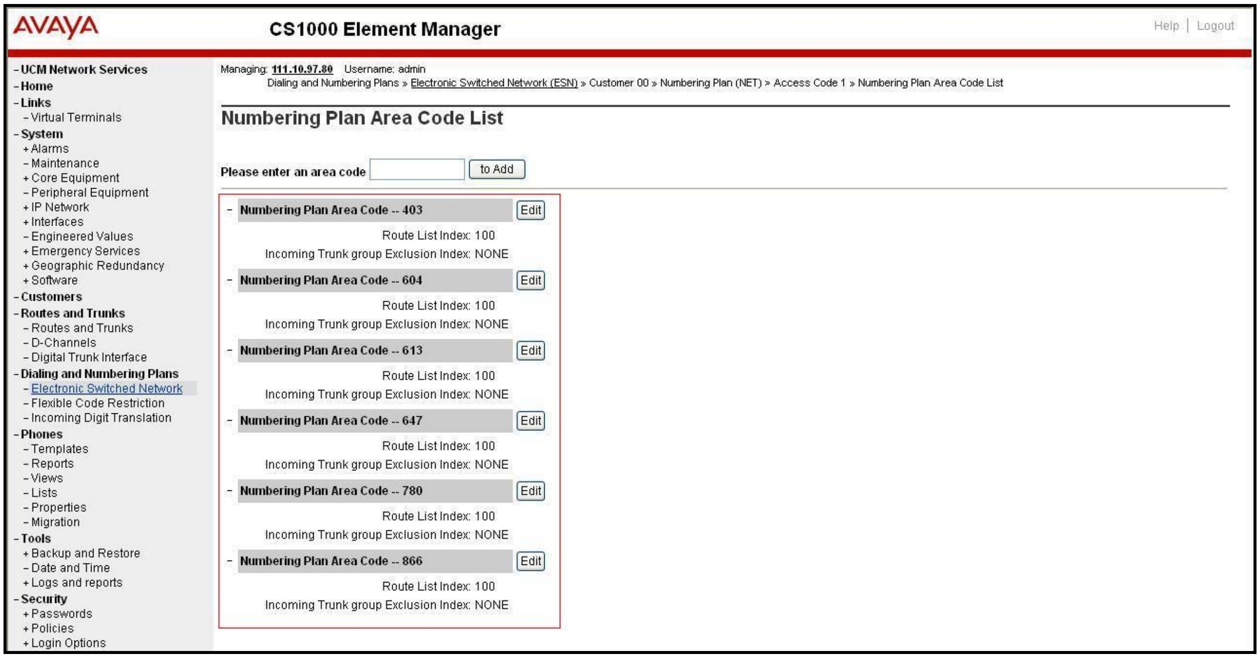

Figure 4:52 Numbering Plan Area Code List

4.7. Administer Phone

This section describes the creation of CS1K clients used in this testing configuration.

4.7.1. Phone creation

a) Refer to **Section 4.5.4** to create a virtual super-loop - **108** used for IP phone.
b) Refer to **Section 4.4.1** to create a bandwidth zone - **10** for IP phone.
c) Login Call Server CLI (please refer to **Section 4.1.2** for more detail).
d) Create an IP phone by using LD 11.

```
REQ: prt
TYPE: 2004p1

TN   96 0 0 1
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES  PHONE
TN   096 0 00 01  VIRTUAL
TYPE 2004P1
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010
```


©2011 Avaya Inc. All Rights Reserved.

```
CUR_ZONE 00010
MRT
ERL  0
ECL  0
FDN  16139675204
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
LNRS 16
XLST
SFLT NO
CAC_MFC 0
CLS  UNR FBA WTA LPR MTD FNA HTA ADD 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
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDD CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM2 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO  0
HUNT 16139675204
LHK  0
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 TELUS i2004P1
            XPLN 13
            DISPLAY_FMT FIRST,LAST
     01 MSB
     02
     03
     04
     05
```


©2011 Avaya Inc. All Rights Reserved.

```
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16  616139675204
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

4.7.2. 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 4.7.1**, the display of the outbound call will be changed appropriately. The privacy for a single call can be done by configuring per-call blocking and a corresponding dialing sequence, for example *67. The resulting SIP privacy setting will be the same in either case.

a) To hide display name, set CLS to **namd**. CS1K will include “Privacy:user” in SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2004p1
TN   96 0 0 1
ECHG yes
ITEM cls namd
ITEM
…
```


©2011 Avaya Inc. All Rights Reserved.

b) To hide display number, set CLS to **ddgd**. CS1K will include “Privacy:id” in SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2004p1
TN   96 0 0 1
ECHG yes
ITEM cls ddgd
…
```

c) To hide display name and number, set CLS to **namd, ddgd**. CS1K will include “Privacy:id, user” in SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2004p1
TN   96 0 0 1
ECHG yes
ITEM cls namd ddgd
…
```

d) To allow display name and number, set CLS to **nama, ddga**. CS1K will send header “Privacy:none” to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2004p1
TN   96 0 0 1
ECHG yes
ITEM cls nama ddga
…
```


©2011 Avaya Inc. All Rights Reserved.

4.7.3. Enable Call Forward for Phone

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

a) Select **Customer** > **01** > **Call Redirection**. The Call Redirection page is shown as **Figure 4:53**.

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

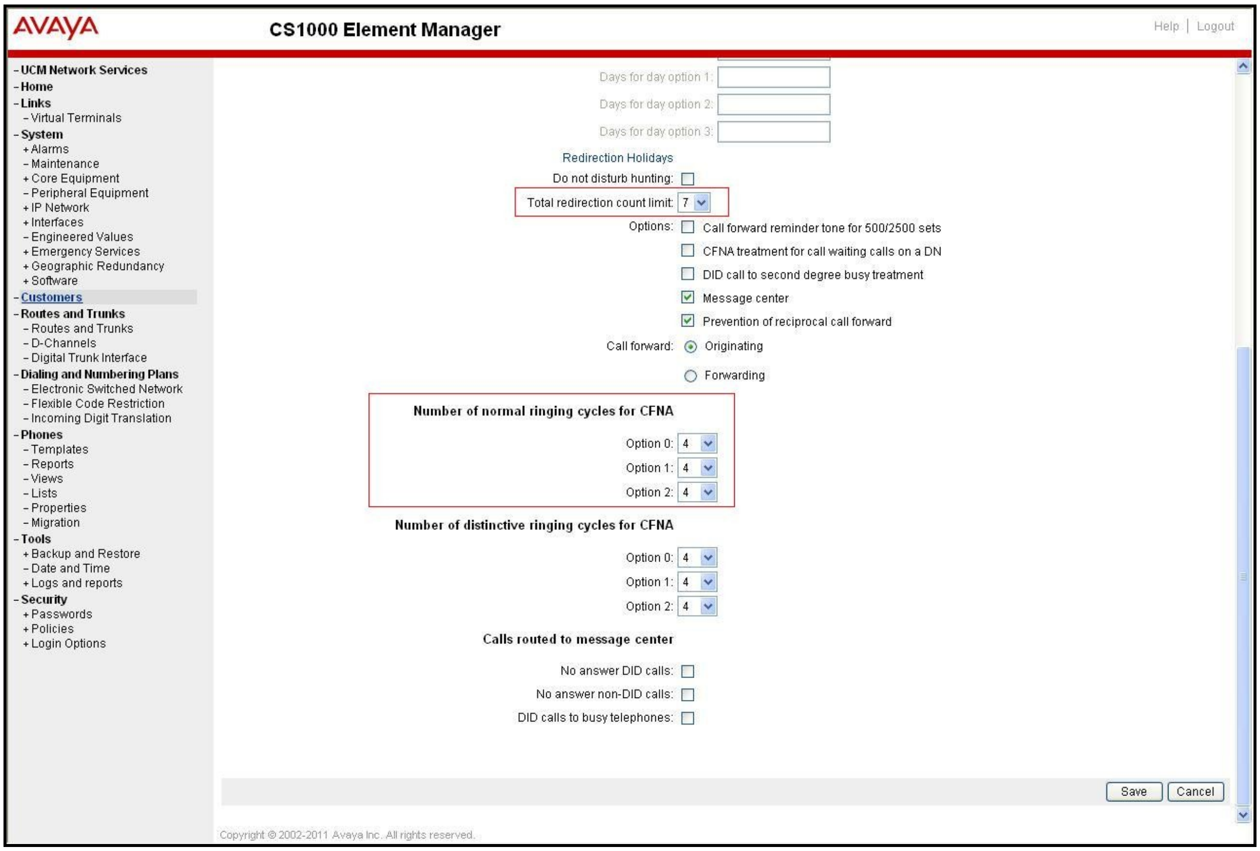

Figure 4:53 Call Redirection

b) To enable **Call Forward All Call** (**CFAC**) for phone over trunk by using LD 11, change its CLS to **CXFA** then program the forward number on the phone set. Following is the configuration of a phone has CFAC enabled with forwarding number is 66139675204.

©2011 Avaya Inc. All Rights Reserved.

```
REQ: prt
TYPE: 2004p1
TN   96 0 0 1
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  PHONE
TN   96 0 00 01  VIRTUAL
TYPE 2004P1
…
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  66139675204
…
```

c) To enable **Call Forward Busy (CFB)** for phone over trunk by using LD 11, change its CLS to **FBA, HTA** then program the forward number as **HUNT**. Following is the configuration of a phone has CFB enabled with forward number 66139675204.

```
REQ: prt
TYPE: 2004p1
TN   96 0 0 1
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  PHONE
TN   96 0 00 01  VIRTUAL
TYPE 2004P1
…
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
…
HUNT 66139675204
…
```


©2011 Avaya Inc. All Rights Reserved.

d) To enable **Call Forward No Answer (CFNA)** for phone over 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 has CFNA enabled with forward number 66139675204.

```
REQ: prt
TYPE: 2004p1
TN   96 0 0 1
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  PHONE
TN   96 0 00 01  VIRTUAL
TYPE 2004P1
…
FDN  66139675204
…
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
   …
```

4.7.4. Enable Call Waiting for Phone

In this section, it shows how to configure Call Waiting feature at phone level.

a) Login Call Server CLI (please refer to **Section 4.1.2** for more detail).
b) Configure Call Waiting feature for phone by using LD 11 to change CLS to **HTD**, **SWA** and adding a **CWT** key.

©2011 Avaya Inc. All Rights Reserved.

```
REQ: prt
TYPE: 2004p1
TN   96 0 0 1
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES  2004P1
TN   96 0 00 00  VIRTUAL
TYPE 2004P1
…
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 5904 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME TELUS i2004P1
            XPLN 13
            DISPLAY_FMT FIRST,LAST
     01 CWT
…
```


©2011 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to the CS1K, the Acme SBC and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

5.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the Session Manager Log On screen, provide the appropriate credentials and click on **Login**.

©2011 Avaya Inc. All Rights Reserved.

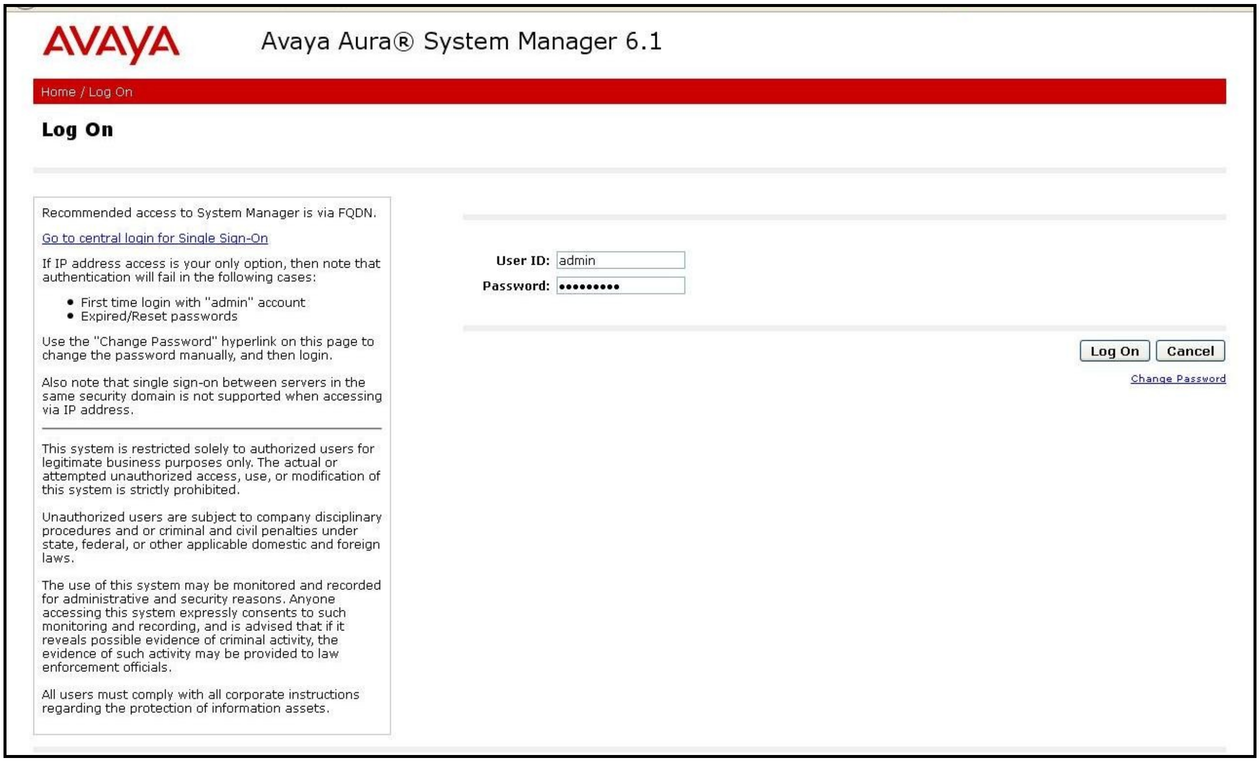

Figure 5:1 SM Login

The home screen shown **Figure 5:2** below in is then displayed, from this page is it possible to access all areas of System Manager.

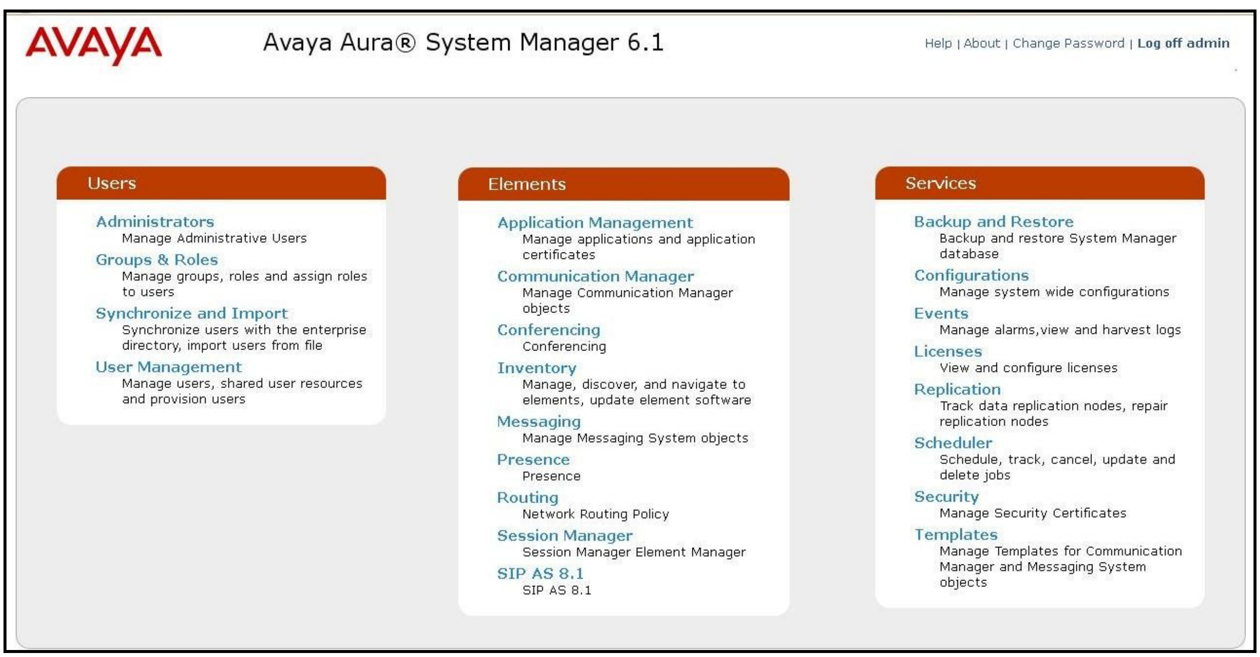

Figure 5:2 SM Home

©2011 Avaya Inc. All Rights Reserved.

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown in **Figure 5:2** to bring up the Introduction to Network Routing Policy screen shown in **Figure 5:3**.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

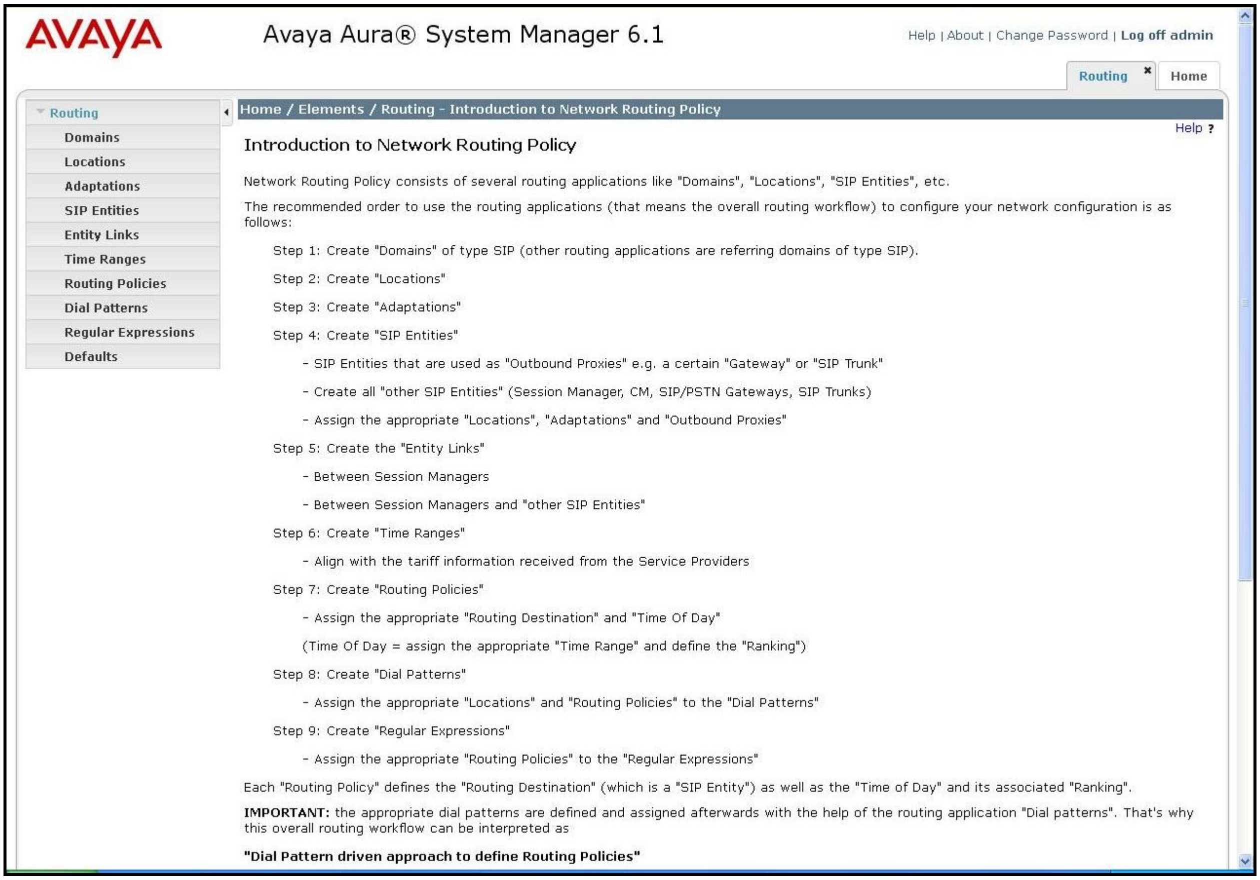

Figure 5:3 SM Routing Policy

©2011 Avaya Inc. All Rights Reserved.

5.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**bvwdev.com**). Navigate to **Routing → Domains** in the left navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. **Figure 5:4** below shows the entry for the enterprise domain.

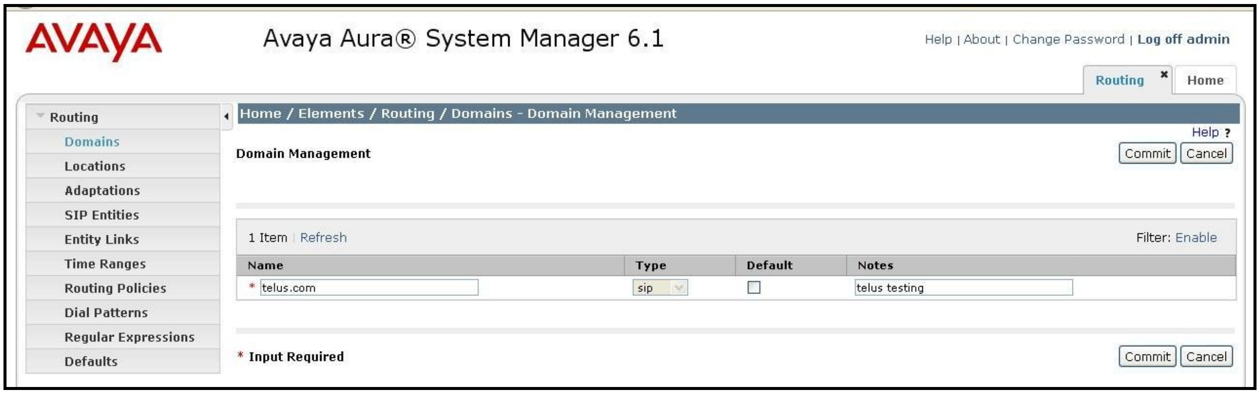

Figure 5:4 Routing Domains

©2011 Avaya Inc. All Rights Reserved.

5.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

Figure 5:5 displayed below are the top and bottom halves of the screen for addition of the **Belleville** Location, which includes all equipment on the **111.10.97.x** subnet including the CS1K, the IP phones, and the Session Manager itself. Click **Commit** to save.

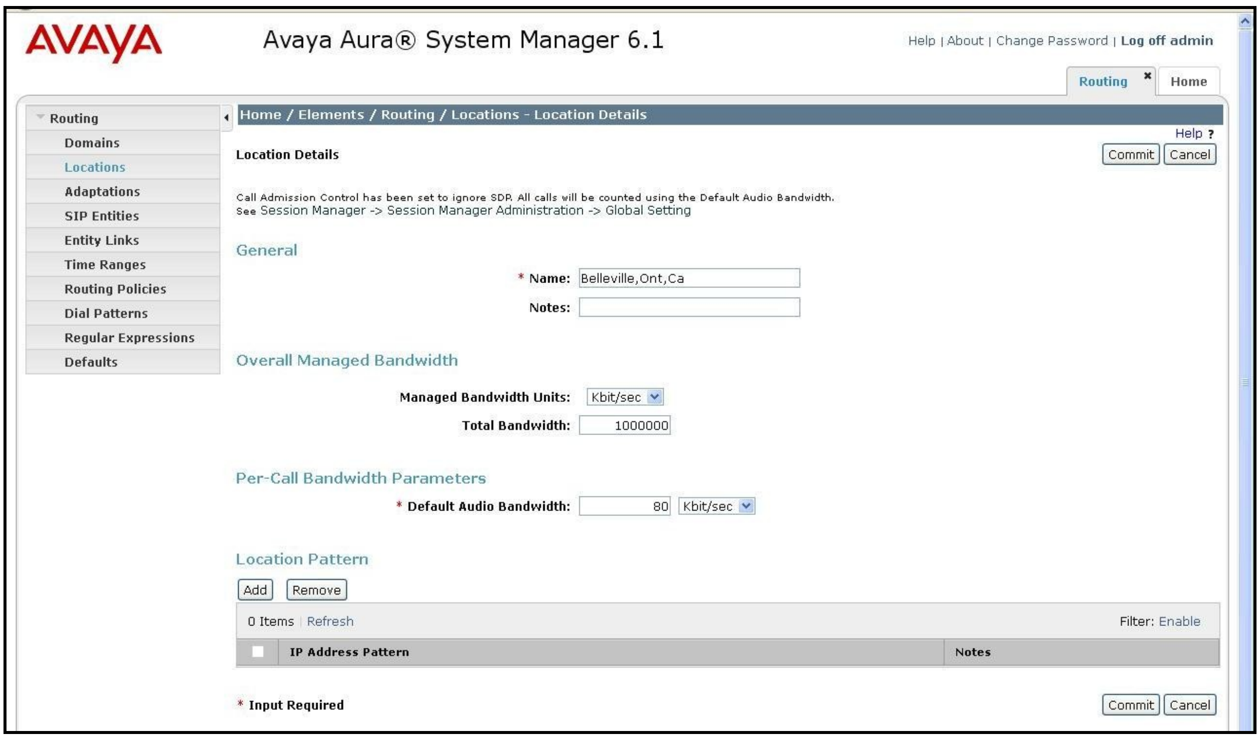

Figure 5:5 SM Routing Locations

5.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes the CS1K and the Acme SBC. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.

©2011 Avaya Inc. All Rights Reserved.

- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling. There are three Entities that need to be configured for this particular configuration: the SM signaling interface, the Node of the CS1K and the internal interface of the Acme SBC.
- **Type:** Enter ***Session Manager*** for Session Manager, ***Other*** for the CS1K and ***Other*** for the Acme SBC.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

Figure 5:6 below shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module (the Session Manager signaling interface) is entered for **FQDN or IP Address**. The Entity Links shown below will be configured in Section 5.5.

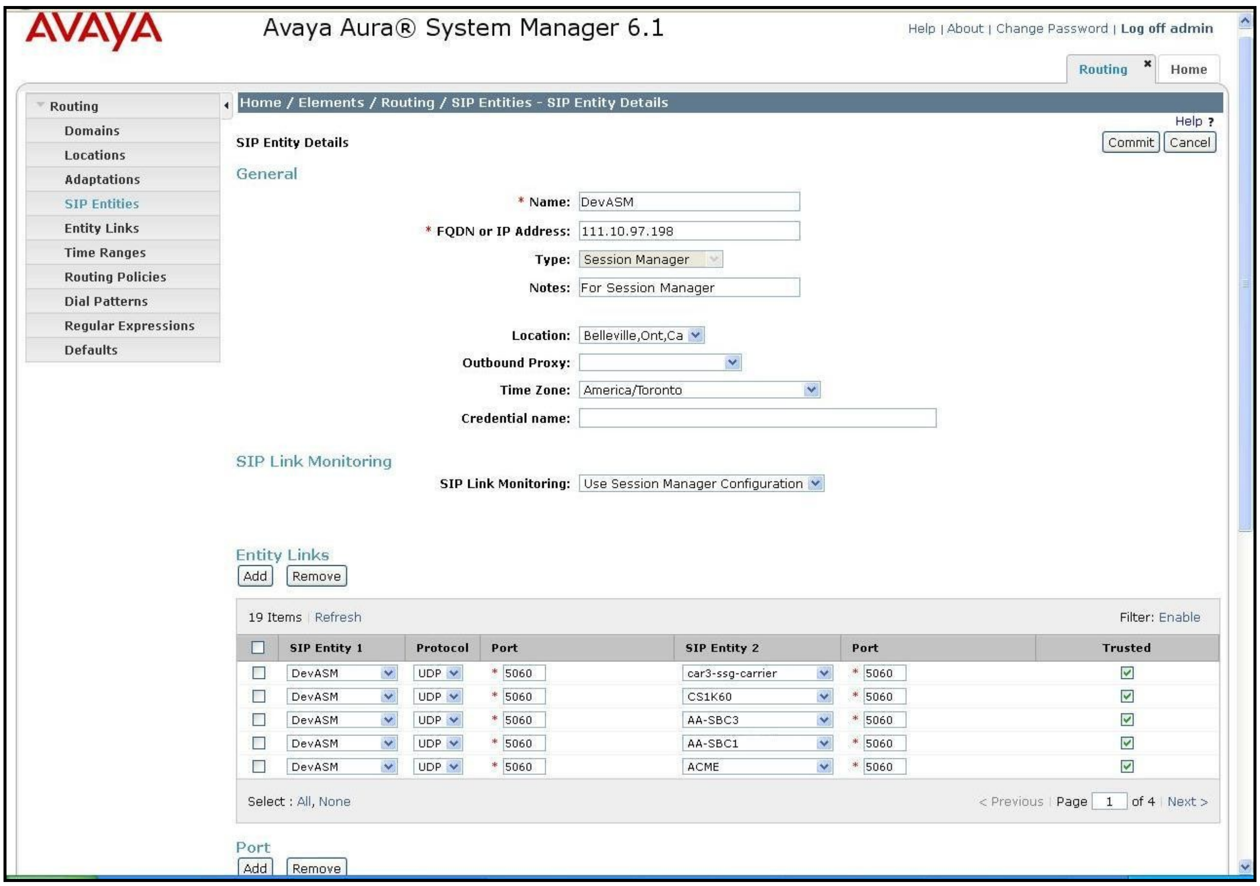

Figure 5:6 SM SIP Entity

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

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

©2011 Avaya Inc. All Rights Reserved.

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

The compliance test used 2 **Port** entries:
- **5060** with **UDP** for connecting to Acme SBC
- **5060** with **UDP** for connecting to the CS1K
- The Entity Links shown below will be configured in Section 5.5.

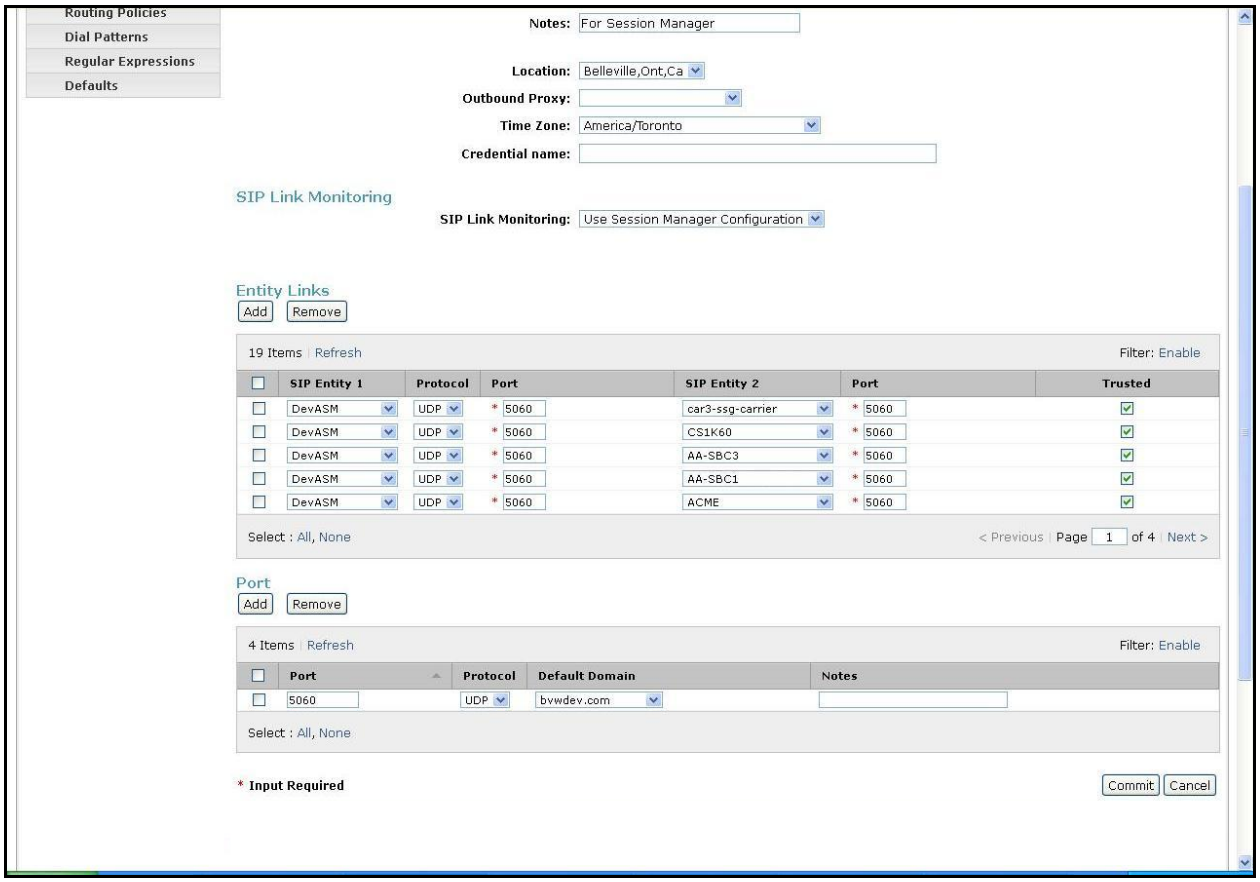

Figure 5:7 SM SIP Entities Details

©2011 Avaya Inc. All Rights Reserved.

Figure 5:8 shows the addition of the CS1K. In order for Session Manager to send SIP service provider traffic on a separate entity link to the CS1K, it is necessary to create a separate SIP entity for the CS1K in addition to the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the CS1K.

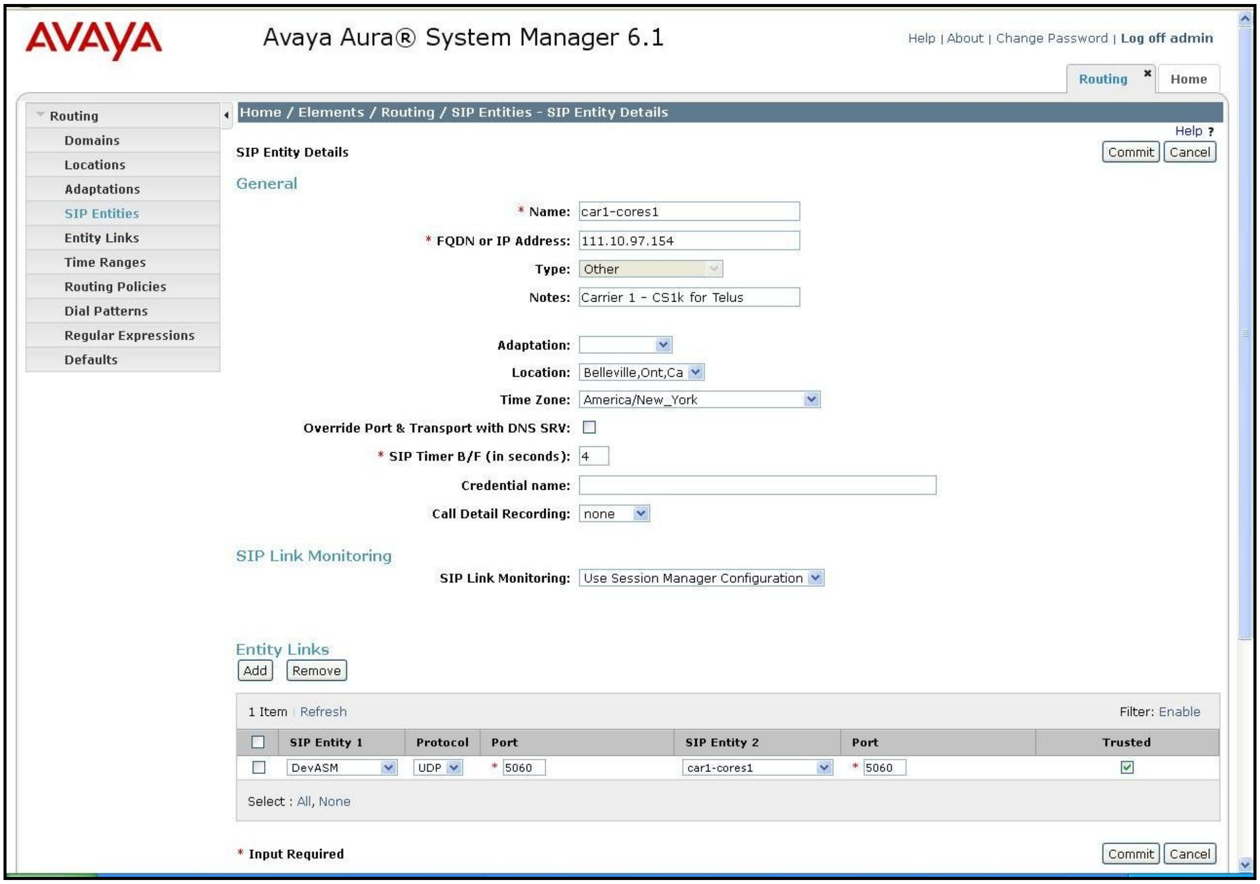

Figure 5:8 CS1K SIP Entity

©2011 Avaya Inc. All Rights Reserved.

Figure 5:9 shows the addition of the Acme SBC SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface. **Link Monitoring Enabled** was disabled for **SIP Link Monitoring.** If monitoring is enabled the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** should be adjusted or left at their default values per customer needs and requirements.

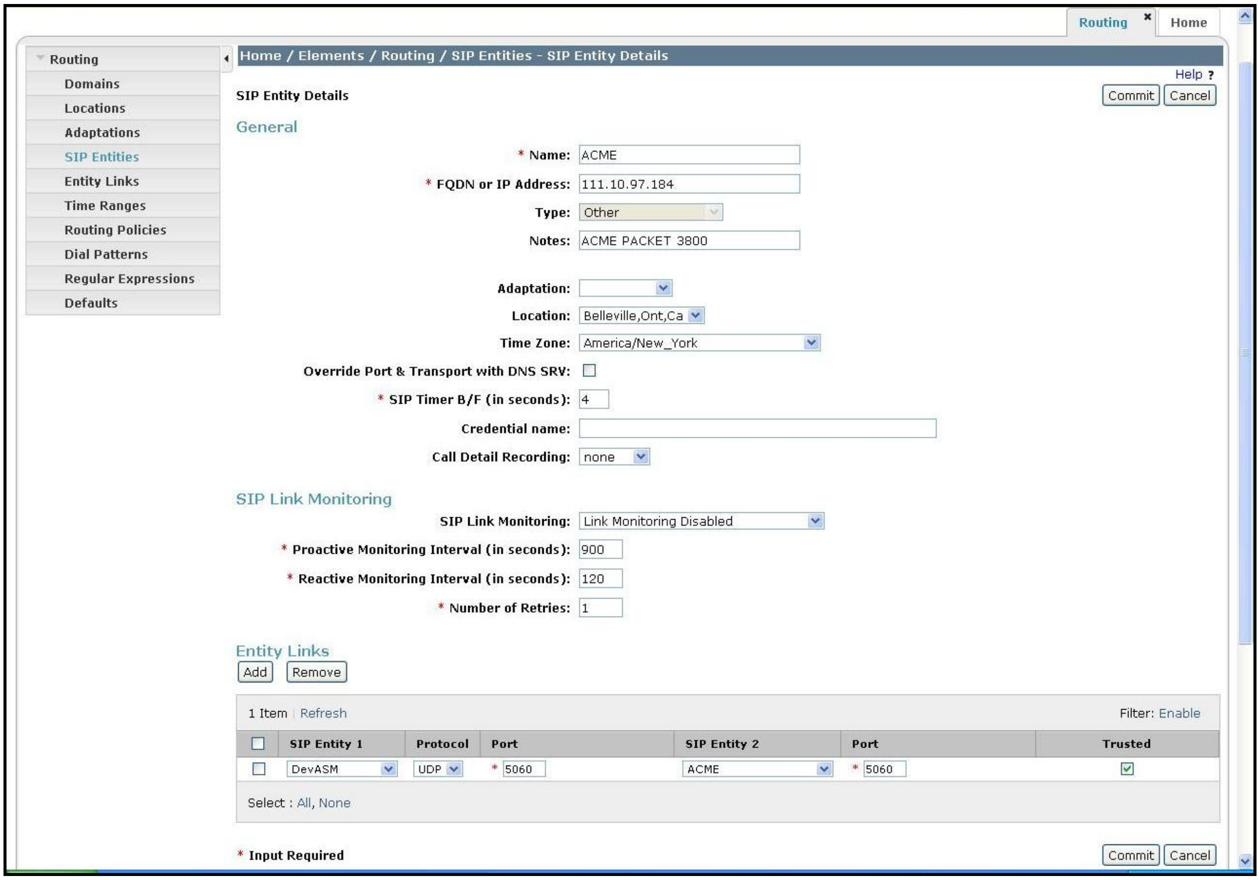

Figure 5:9 Acme SBC SIP Entity

5.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the CS1K for use only by service provider traffic and one to the Acme SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.

©2011 Avaya Inc. All Rights Reserved.

- **SIP Entity 2:** Select the name of the other system. For CS1K, select the CS1K SIP Entity defined in **Figure 5:8**. For Acme SBC, select the Acme SBC SIP Entity defined in **Figure 5:9**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **5.4** will be denied.*

Click **Commit** to save.

The following screens illustrate the Entity Links to CS1K and the Acme SBC. It should be noted that in a customer environment the Entity Link to CS1K can be configured to use UDP, TCP or TLS. For this compliance test was UDP was used.

Entity Link to the CS1K:

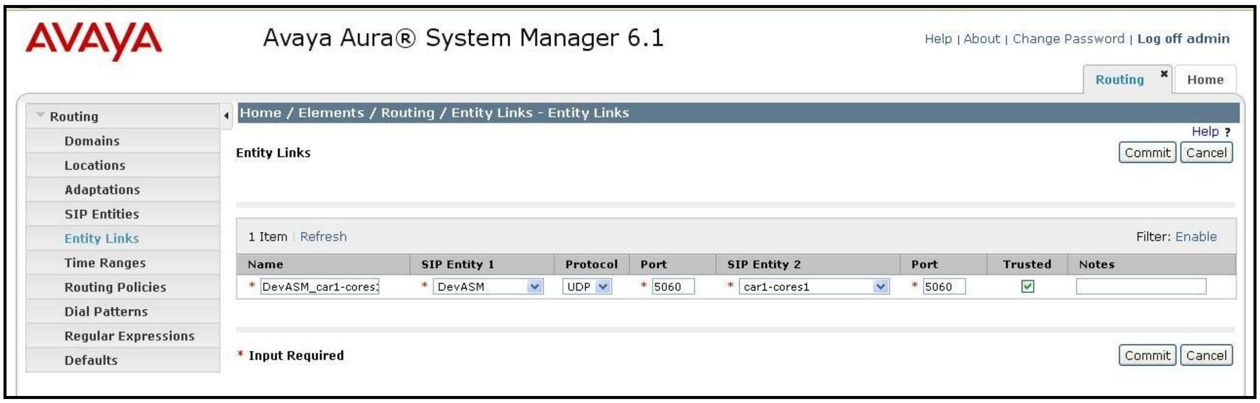

Figure 5:10 SM Routing Entity Link – CS1K

Entity Link to the Acme SBC:

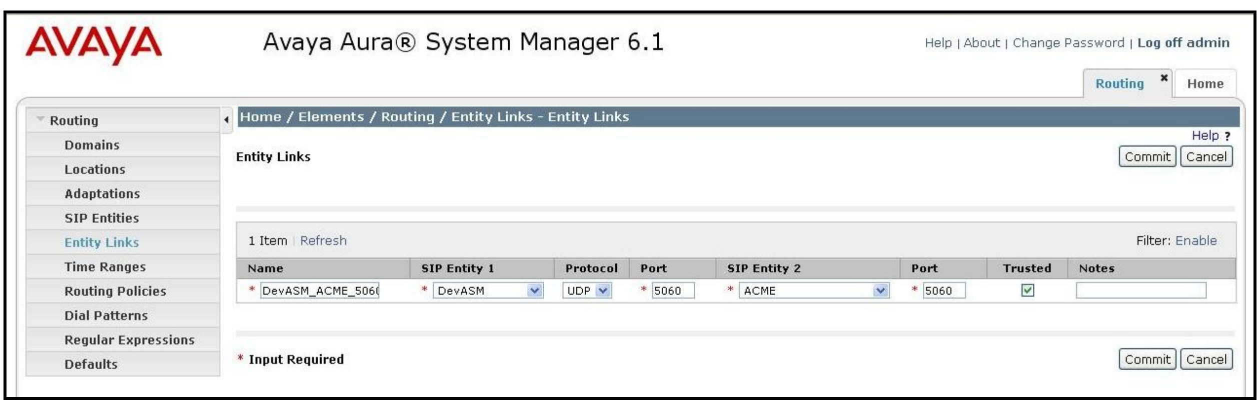

Figure 5:11 SM Routing Entity Link – Acme SBC

©2011 Avaya Inc. All Rights Reserved.

5.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.4**. Two routing policies must be added: one for the CS1K and one for the Acme SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select.** The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields. Click **Commit** to save. The Time of Day and Dial Patterns shown in the screen capture will not be displayed until they are added in the following section.

The following screens show the Routing Policies for CS1K and the Acme SBC.

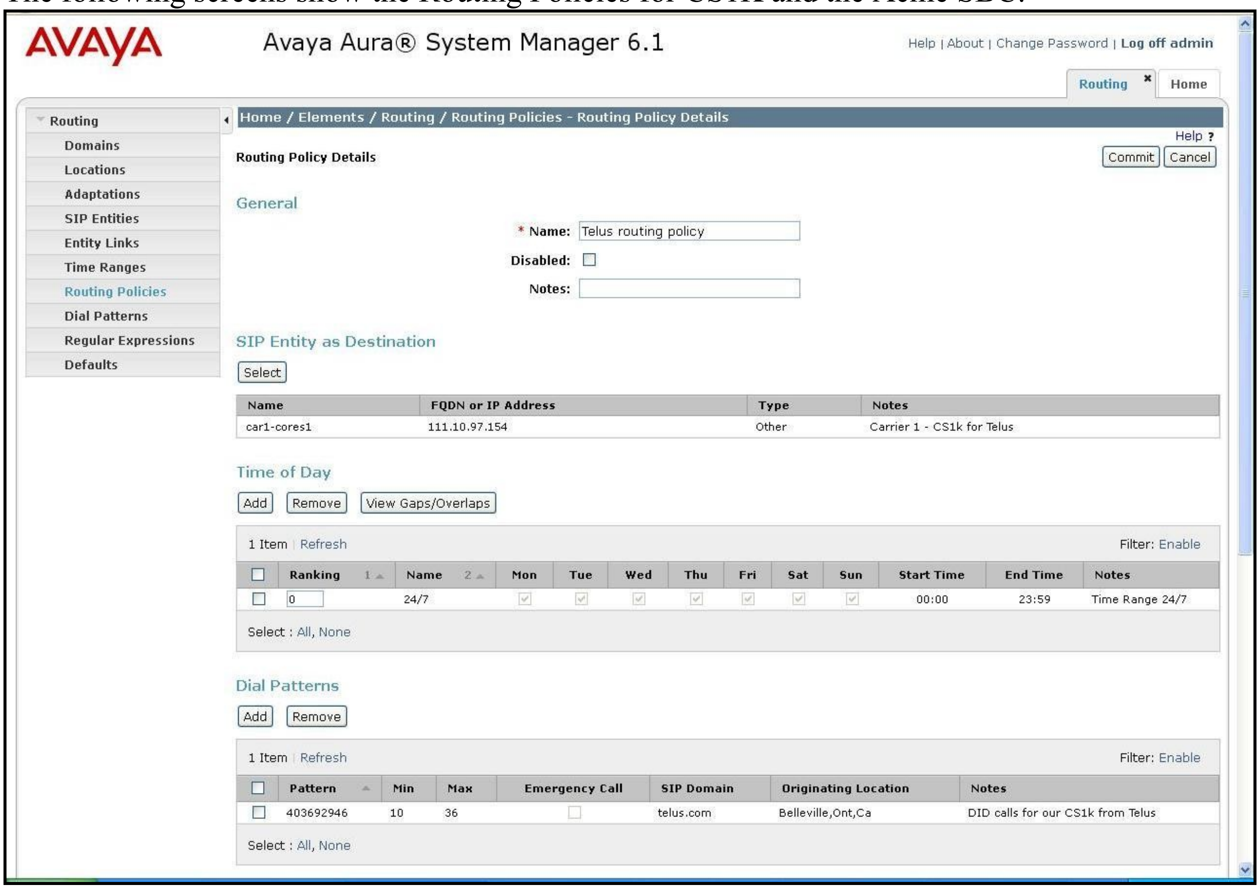

Figure 5:12 SM Routing Policy – CS1K

©2011 Avaya Inc. All Rights Reserved.

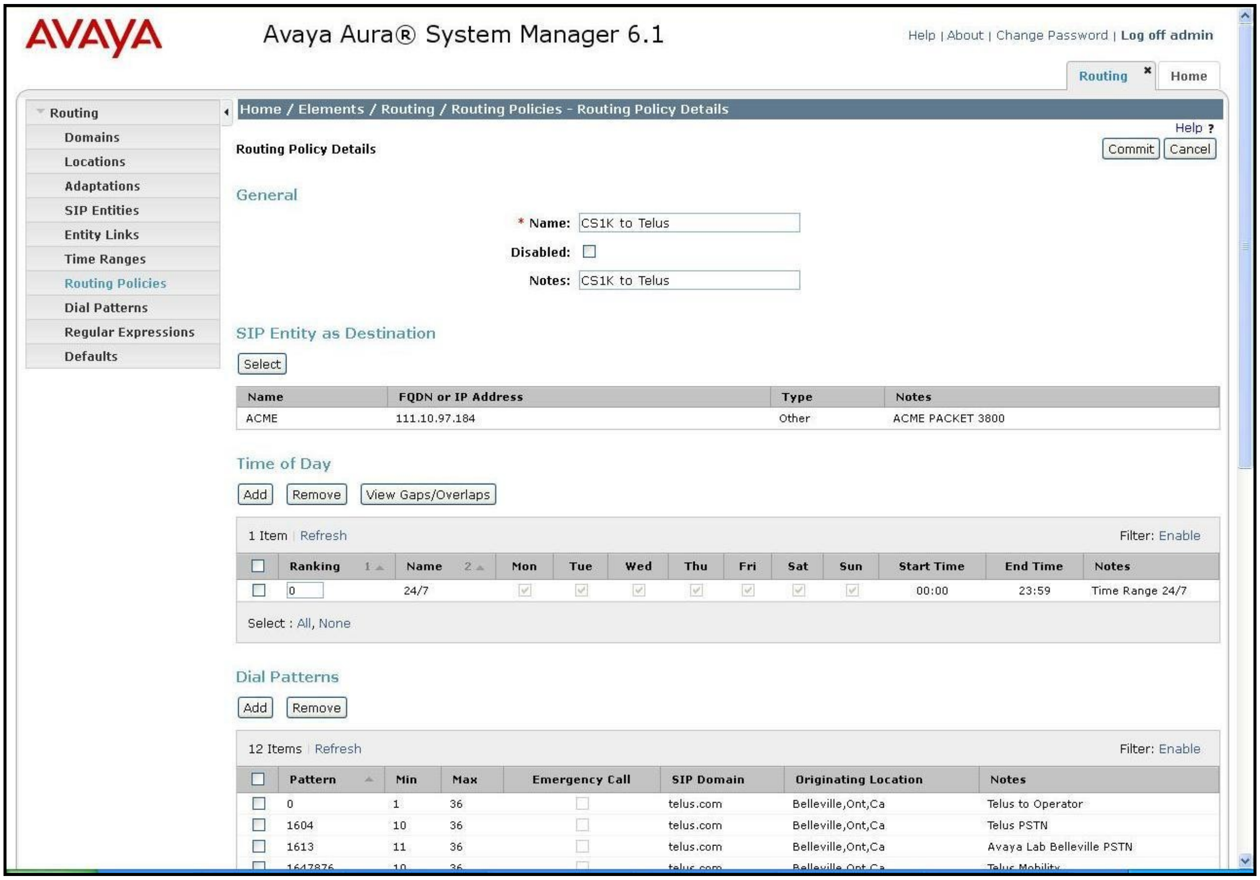

Figure 5:13 SM Routing Policy Acme Packet

5.7. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from the CS1K to TELUS and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the Originating Locations and Routing Policies section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating

©2011 Avaya Inc. All Rights Reserved.

location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Four examples of the dial patterns used for the compliance test are shown below, one for outbound calls from the enterprise to TELUS Mobility, one for outbound calls from the enterprise to the TELUS lab, one for outbound 911 calls and one for incoming calls to the CS1K system. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls, etc., were similarly defined. All dial patterns are shown in **Figure 5:18**.

The first example in **Figure 5:14** shows that 11 digit dialed numbers that begin with **1647876**, which are for TELUS Mobility sets, and have a destination domain of **TELUS.com** uses route policy **CS1K_to_TELUS**.

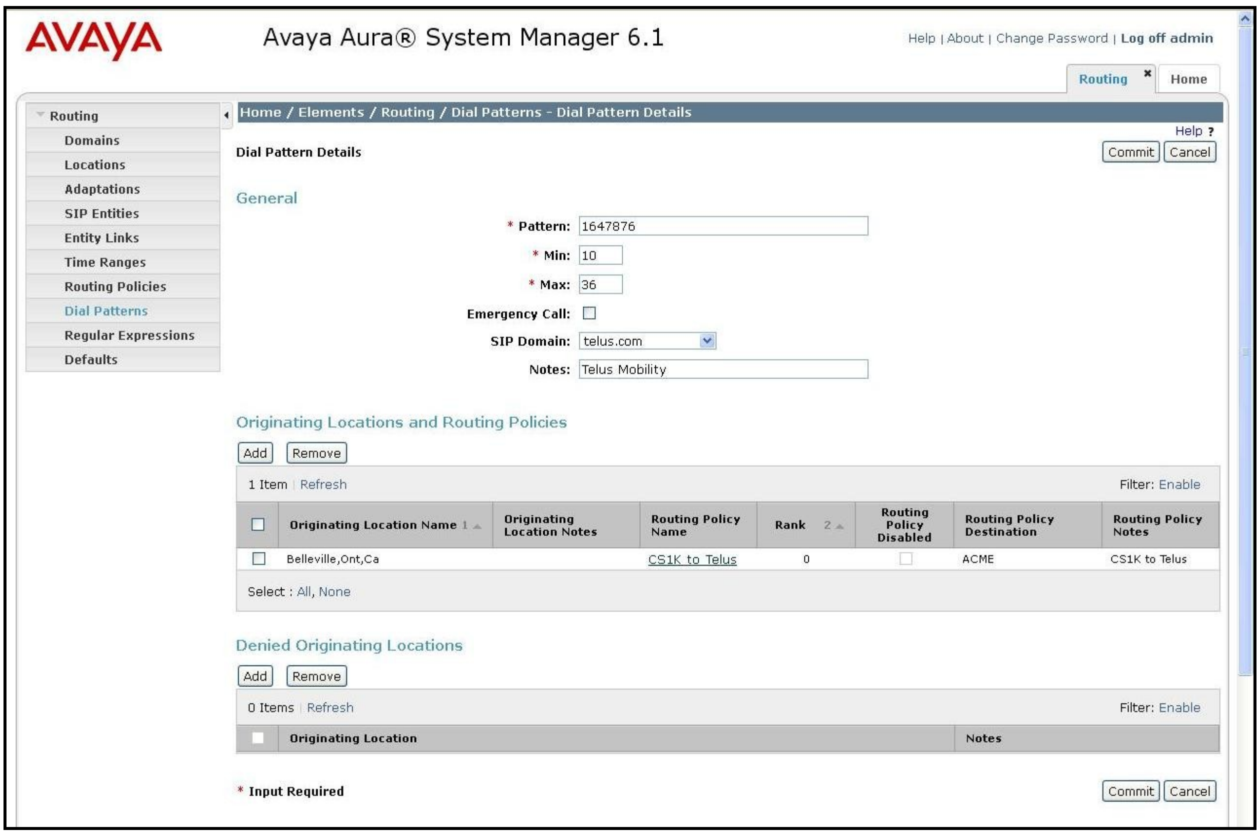

Figure 5:14 SM 11 digit Dial Pattern to Telus

©2011 Avaya Inc. All Rights Reserved.

The second example in **Figure 5:15** shows that 10 digit dialed numbers that begin with **403692947**, which are for TELUS lab sets, and have a destination domain of **TELUS.com** uses route policy **CS1K_to_TELUS**.

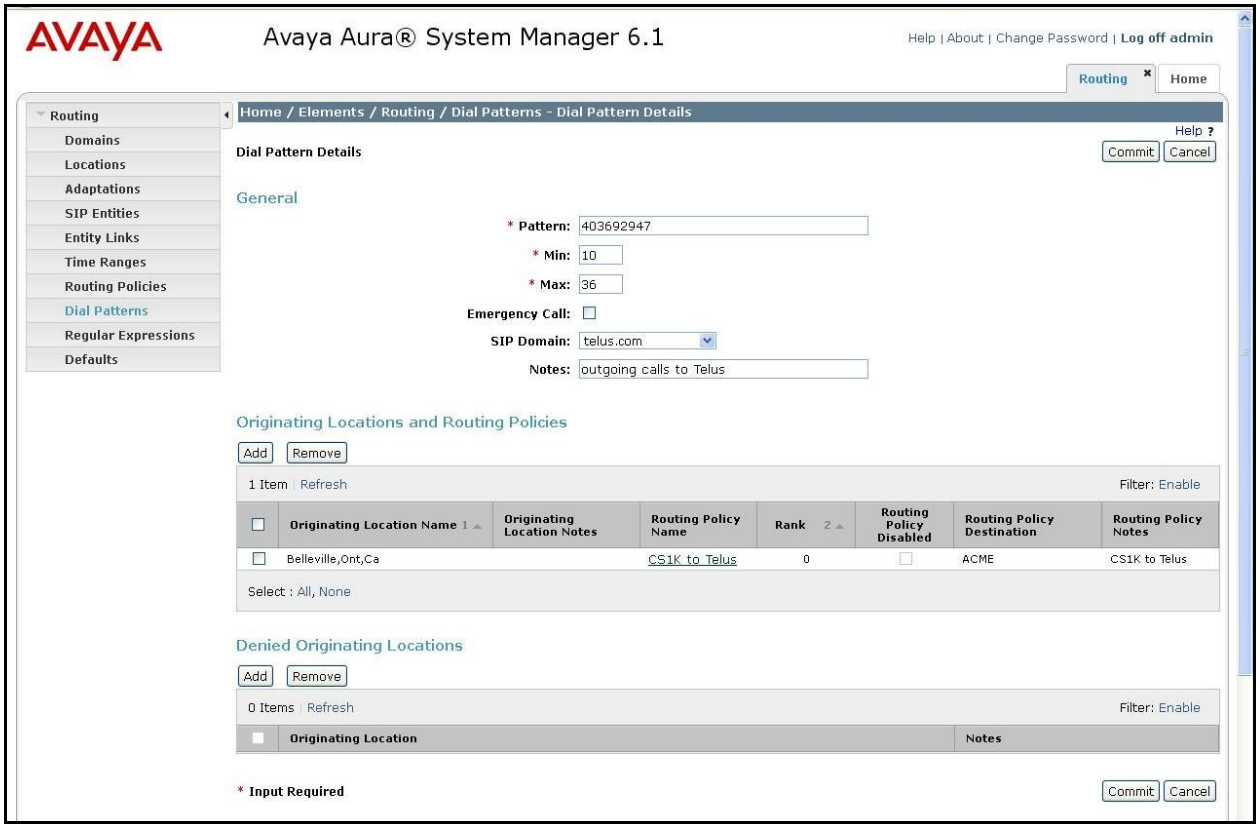

Figure 5:15 SM 10 digit Dialing Pattern to Telus

©2011 Avaya Inc. All Rights Reserved.

The third example in **Figure 5:16** shows that the 3 digit 911 dialed number for emergency calls have a destination domain of **TELUS.com** uses route policy **CS1K_to_TELUS**.

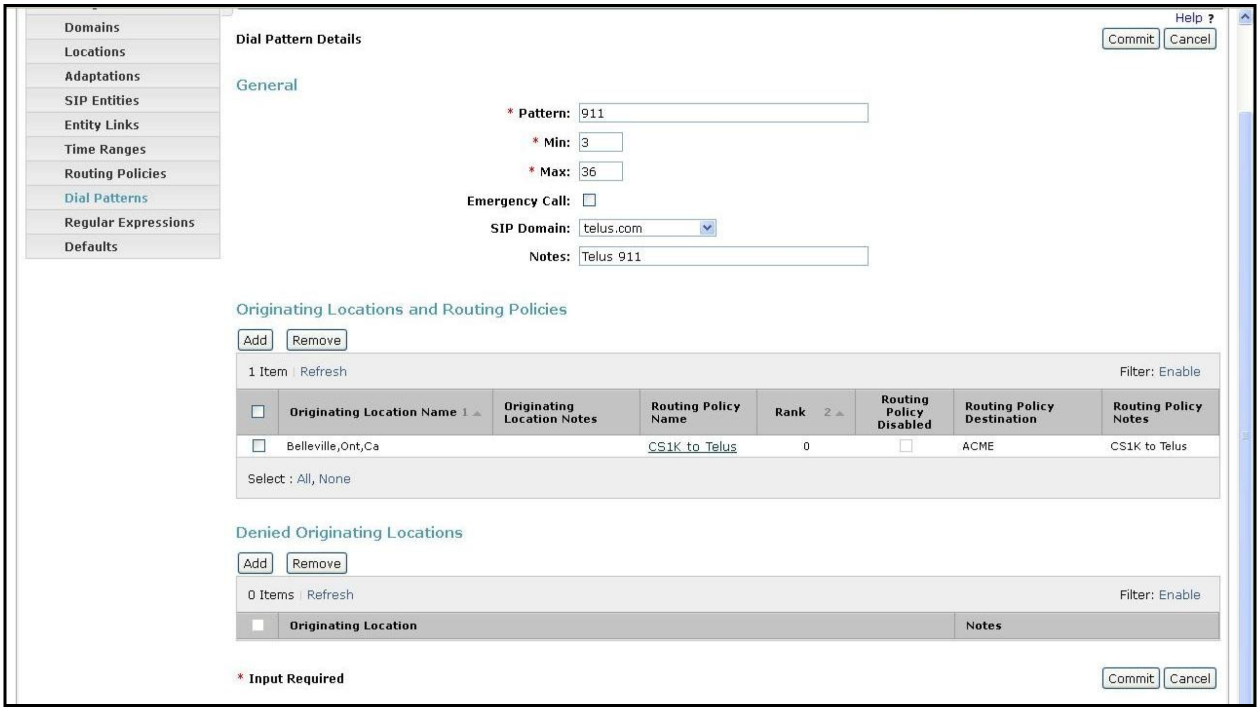

Figure 5:16 SM 911 Dialing Pattern to Telus

The fourth example shown in **Figure 5:17** illustrates that in this case 9 digits are used to route the incoming call to the destination car1-cores1 which is the CS1K system.

©2011 Avaya Inc. All Rights Reserved.

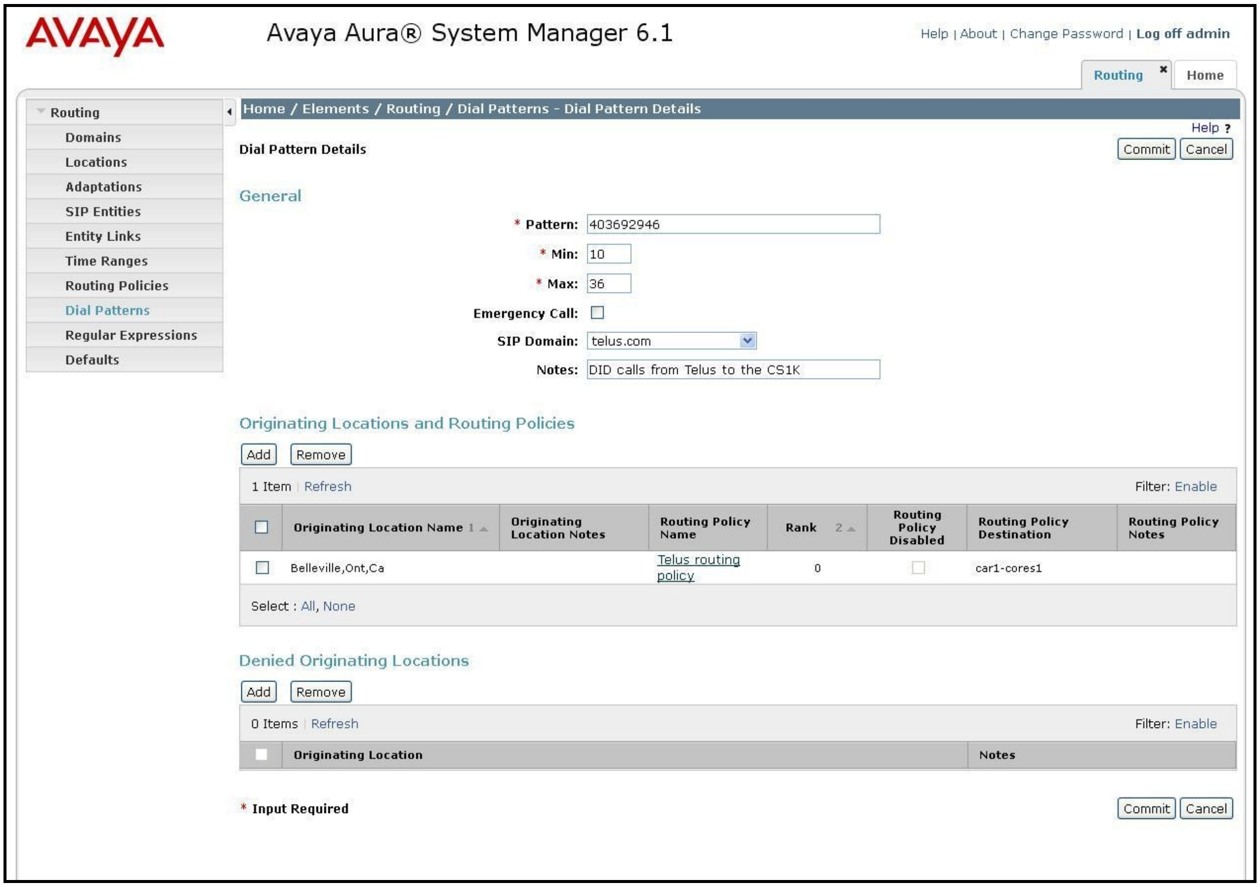

Figure 5:17 SM Dialing Pattern to CS1K

©2011 Avaya Inc. All Rights Reserved.

Figure 5:18 shows all the dial patterns that were configured for outbound calls to the TELUS network and local PSTN calls.

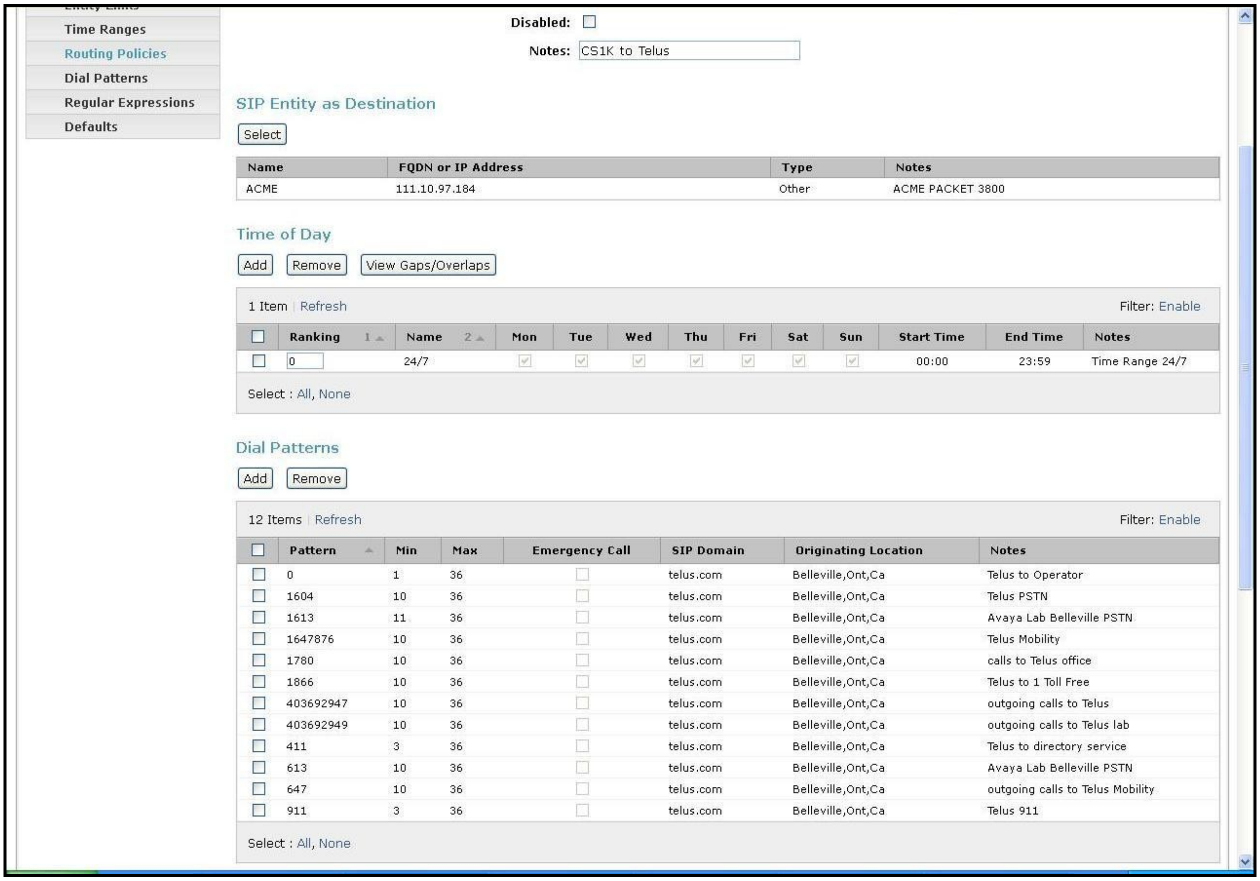

Figure 5:18 SM all Dial Patterns to Telus

5.8. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane. If the Session Manager already exists, click **View** to view the configuration.

©2011 Avaya Inc. All Rights Reserved.

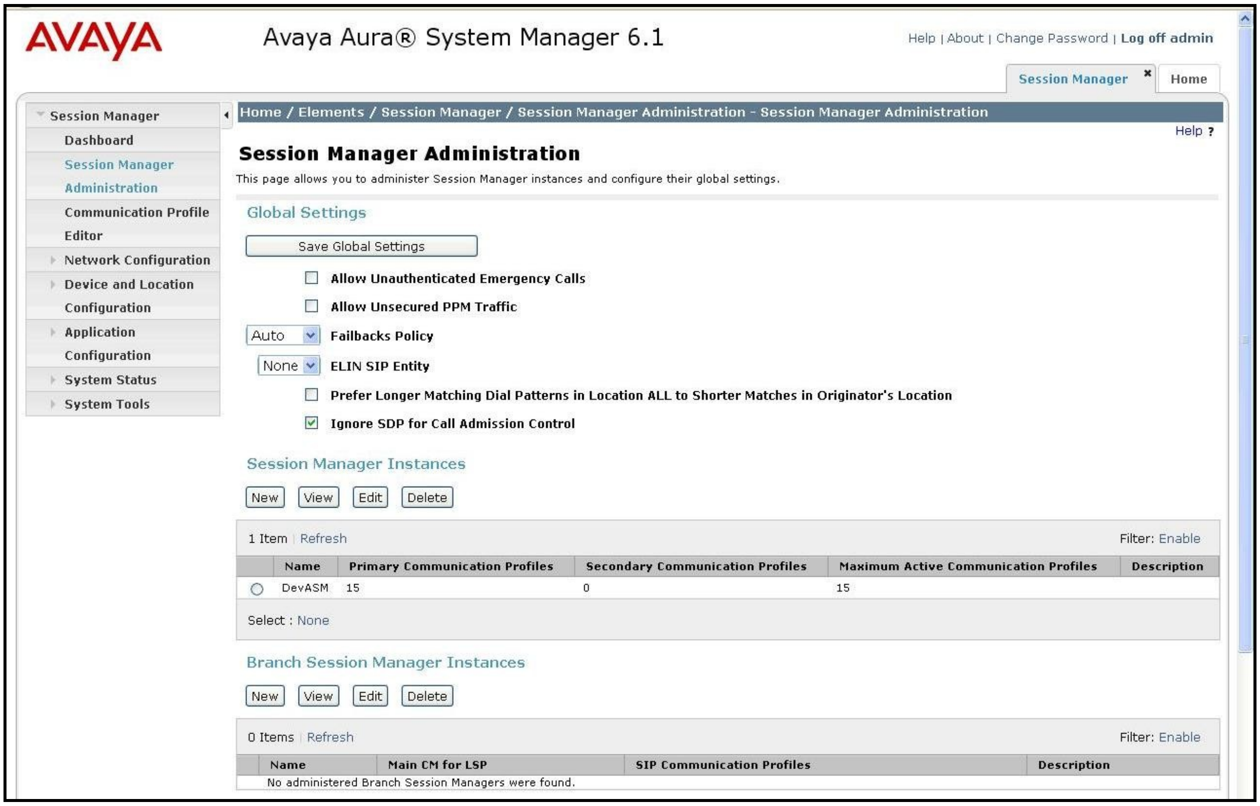

Figure 5:19 SM Session Manager Administration

Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

©2011 Avaya Inc. All Rights Reserved.

Figure 5:20 below shows the Session Manager values used for the compliance test. Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager.

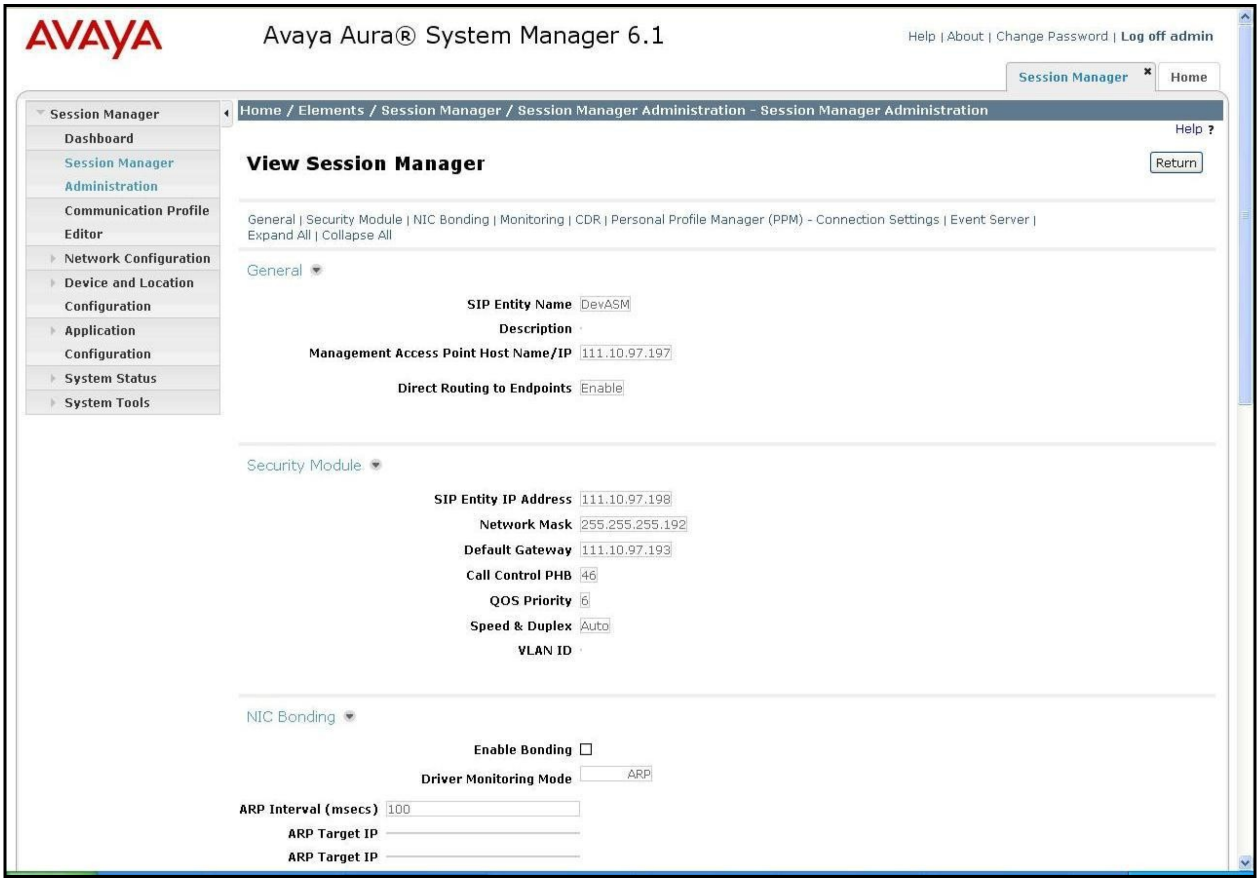

Figure 5:20 SM View Session Manager

©2011 Avaya Inc. All Rights Reserved.

6. Configure Acme Packet Net-Net 3800 Session Border Controller

This section describes the configuration of the Acme Packet Session Border Controllers necessary for interoperability with the CS1K and the TELUS system. The Acme Packet Session Border Controller was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet Session Border Controller.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to CS1K. The remaining fields are generally the default/standard value used by the Acme Packet Session Border Controller for that field.

In this testing, according to the configuration reference **Figure 2:1**, the Avaya elements reside on the Private side and the TELUS elements reside on the Public side of the network.

6.1. Acme Packet Command Line Interface Summary

The Acme Packet Session Border Controller is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Acme Packet Session Border Controller using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Session Border Controller for cable connection). Use the following settings for the serial port on the PC.
    - Bits per second: 115200
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: None
2. Log in to the Acme Packet Session Border Controller with the proper user password.
3. Enable the Super-user mode by entering the **enable** command and then the super user password. The command prompt will change to include a "#" instead of a ">" while in Super user mode. This level of system access (i.e. at the "acmesystem#" prompt) will be referred to as the ***main*** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific ***elements*** and specific ***parameters*** of those elements.
4. In Super-user mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the ***configuration*** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface).**
7. Enter the name of an element parameter followed by its value (e.g., **name INSIDE**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all other elements.

©2011 Avaya Inc. All Rights Reserved.

11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

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

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

6.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 01/port 0 of the Acme Packet Session Border Controller was connected to the external un-trusted network. The Ethernet slot 0/port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

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

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

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

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


©2011 Avaya Inc. All Rights Reserved.

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

```
network-interface
        name                            INSIDE
        sub-port-id                     0
        description
        hostname
        ip-address                      111.10.97.184
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.192
        gateway                         111.10.97.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     111.10.97.184
        ftp-address
        icmp-address                    111.10.97.184
        snmp-address
        telnet-address
        ssh-address                     111.10.97.184
        last-modified-by                admin@console
        last-modified-date              2011-04-28 17:44:45
```

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

```
network-interface
        name                            OUTSIDE
        sub-port-id                     0
        description
        hostname
        ip-address                      222.10.98.98
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.224
        gateway                         222.10.98.97
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
```


©2011 Avaya Inc. All Rights Reserved.

```
            health-score                        0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    222.10.98.98
        ftp-address
        icmp-address                   222.10.98.98
        snmp-address
        telnet-address
        ssh-address
        last-modified-by               admin@console
        last-modified-date             2011-01-10 15:26:28
```

6.3. Realm

A realm represents a group of related Acme Packet Session Border Controller components. Two realms were defined for the compliance test. The realm configuration "INSIDE" below represents the internal network on which the Avaya elements reside.

```
realm-config
        identifier                     INSIDE
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       INSIDE:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
...
        last-modified-by               admin@console
        last-modified-date             2011-01-08 20:08:00
```

The realm configuration "OUTSIDE" below represents the external network on which the TELUS system reside.

```
realm-config
        identifier                     OUTSIDE
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       OUTSIDE:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
```


©2011 Avaya Inc. All Rights Reserved.

```
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
...
        last-modified-by                admin@222.10.98.103
        last-modified-date              2011-07-15 13:09:54
```

6.4. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet Session Border Controller such as CS1K and/or Service Provider SBC.

The **session agent** below represents the TELUS border element. The ACME will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". NOTE: TELUS requires a hops=0 setting for the OPTIONS parameter. The hops=0 setting is in line with Acme Packet best practices recommendation for customer deployments. The hops=0 setting can be a useful keep alive method which can trigger a failover mechanism if the CS1K network employs redundant SBCs. A hops=0 setting guarantees the ping reply comes from directly from the TELUS SBC and if there is no response it indicates an outage condition.

The **in-manipulationid** and **out-manipulationid** are defined in the SIP header manipulation applying to the OUTSIDE realm.

```
session-agent
        hostname                        333.91.119.218
        ip-address                      333.91.119.218
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        OUTSIDE
        egress-realm-id
        description                     CS1K_to_TELUS
        carriers
...
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   30
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
...
        in-manipulationid               TELUS_To_CS1K
        out-manipulationid              CS1K_To_TELUS
...
        last-modified-by                admin@222.10.98.103
        last-modified-date              2011-07-08 12:10:10
```


©2011 Avaya Inc. All Rights Reserved.

The **session agent** below represents the Session Manager which is the border element of the Avaya system.

```
session-agent
        hostname                       111.10.97.198
        ip-address                     111.10.97.198
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       INSIDE
        egress-realm-id
        description                    TELUS_CS1K7.5
        carriers
...
        last-modified-by               admin@222.10.98.103
        last-modified-date             2011-07-07 08:36:36
```

6.5. SIP Configuration

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

- **home-realm-id**: The name of the realm on the private side of the Acme Packet Session Border Controller.
- **egress-realm-id**: The name of the realm on the private side of the Acme Packet Session Border Controller.

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id                INSIDE
        nat-mode                       None
...
        last-modified-by               admin@console
        last-modified-date             2011-01-13 12:02:31
```

6.6. SIP Interface

The SIP interface (***sip-interface***) defines the receiving characteristics of the SIP interfaces on the Acme Packet Session Border Controller. Two SIP interfaces were defined; one for each realm. The SIP interface below is used by the Acme Packet Session Border Controller to communicate with CS1K system.

```
sip-interface
        state                          enabled
        realm-id                       INSIDE
        description
        sip-port
```


©2011 Avaya Inc. All Rights Reserved.

```
                address                         111.10.97.184
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        sip-port
                address                         111.10.97.184
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
...
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by                admin@222.10.98.103
        last-modified-date              2011-07-12 08:20:39
```

The SIP interface below is used by the Acme Packet Session Border Controller to communicate with the TELUS system.

```
sip-interface
        state                           enabled
        realm-id                        OUTSIDE
        description
        sip-port
                address                         222.10.98.98
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        sip-port
                address                         222.10.98.98
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
...
        tcp-keepalive                   none
        add-sdp-invite                  reinvite
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by                admin@222.10.98.103
        last-modified-date              2011-07-15 13:09:18
```


©2011 Avaya Inc. All Rights Reserved.

6.7. SIP Header Manipulation

SIP manipulation rules are used to modify the SIP messages headers and values (if necessary) for interoperability.

The following sip-manipulation **CS1K_To_TELUS** is applied to **OUTSIDE** realm ***out-manipulationid***. These rules perform the following:

- The header manipulation rule **manipRURI**, along with the other "manip" rules, perform address translation and topology hiding for SIP messages between the TELUS system and the Avaya elements. **manipRURI** changes the Avaya Domain Name to 333.91.119.218 (the IP address of the TELUS border element) in the Request URI headers sent to TELUS.
- The header manipulation rule **manipFrom** changes the Avaya Domain Name/IP address to 333.91.119.218 (the IP address of the TELUS border element) in the From headers sent to TELUS.
- The header manipulation rule **manipTo** changes the Avaya Domain Name/IP address to 333.91.119.218 (the IP address of the TELUS border element) in the To headers sent to TELUS.
- The header manipulation rule **maniPassert** changes the Avaya Domain Name/IP address to 333.91.119.218 (the IP address of the TELUS border element) in the P-Asserted-Identity headers sent to TELUS.
- The header manipulation rule **HistRegex** stores the user and host portion of the History –Info header. The user and host from the History-Info header will be used to construct a diversion header by the **Create_Diversion_unavailable** header rule.
- The header manipulation rule **storeSDP** stores the information in the SDP header in the case where the c=0.0.0.0 and a=inactive. The CS1K uses this type of SDP when an RTP stream is placed on hold.
- The header manipulation rule **ModifySDP** changes the SDP for the above condition when a call is placed on hold. It will change the c=0.0.0.0 to the actual IP address of the Avaya SBC, which is 222.10.98.98.
- The header manipulation rule **HstInfChkTmpUnav** will check the History-Info header for the redirection case when the user is "Temporarily Unavailable". The value will be checked for the construction of the PAI and Diversion headers.
- The header manipulation rule **HstInfChkMvTmp** will check the History-Info header for the redirection case when the user is "Moved Temporarily". The value will be checked for the construction of the PAI and Diversion headers.
- The header manipulation rule **HstInfChkBsyHere** will check the History-Info header for the redirection case when the user is "Busy Here". The value will be checked for the construction of the PAI and Diversion headers.
- The header manipulation rule **FmatHistInfo** strips the index=1 host and user information from the History-Info header. The history information is then used by the **HstInfStrURI** rule to extract the user and host in cases of call redirection.
- The header manipulation rule **HstInfStrURI** stores the host and user information from the History-Info header in the case where a redirection has occurred as indicated by the previous "HstInfChk" rules. This information will be used to create a P-Asserted-Identity header by the **RplcPAI** rule.

- The header manipulation rule **RplcPAI** will construct a P-Asserted-Identity header when a call has been redirected. The host and user information from the History-Info header is used to populate the P-Asserted-Identity header.
- The header manipulation rule **nt8000Removal** will remove the Nortel mime information from the SDP.
- The header manipulation rule **Status180Str** will check for 18x message types so that the RmvPAI rule can then remove the P-Asserted-Identity header from these messages.
- The header manipulation rule **RmvPAI** will remove the P-Asserted-Identity header for all 18x messages only.
- The header manipulation rule **delete_mcdn** will remove the Nortel mime information.
- The header manipulation rule **delete_X_nt_e164_clid** will remove the Nortel X_nt_e164_clid header.
- The header manipulation rule **delete_Alert_Info** will remove the Alert-info header.
- The header manipulation rule **search_privacy** will examine the Privacy header if it is present and store the information so that it can be used in the creation of the diversion header to ensure the privacy settings are carried forward.
- The header manipulation rule **Create_Diversion_unavailable** will create a Diversion header with the user and host gathered from the History-Info header. The Diversion header will be created for all 3 redirection reasons but the reason in the Diversion header will always be "unavailable".
- The header manipulation rule **DelHstInfo** will remove the History-Info header.
- The header manipulation rule **delPLocation** will remove the P-Location header that is inserted by the SM.
- The header manipulation rule **delRoute** will remove the Route header which in not needed.

Note: Any header manipulation rule parameters that have spaces must be enclosed in "quotes" in order to be accepted properly.

```
sip-manipulation
        name                               CS1K_To_TELUS
        description
        split-headers
        join-headers
        header-rule
                name                               manipRURI
                header-name                        request-uri
                action                             manipulate
                comparison-type                    case-sensitive
                msg-type                           any
                methods                            INVITE
                match-value
                new-value
                element-rule
                        name                               modRURI
                        parameter-name
                        type                               uri-host
                        action                             replace
                        match-val-type                     any
```


©2011 Avaya Inc. All Rights Reserved.

```
                comparison-type                 case-sensitive
                match-value
                new-value                       333.91.119.218
    header-rule
            name                            manipFrom
            header-name                     From
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
            element-rule
                name                            From
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       333.10.98.98
    header-rule
            name                            manipTo
            header-name                     To
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
            element-rule
                name                            To
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       333.91.119.218
    header-rule
            name                            maniPassert
            header-name                     P-Asserted-Identity
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
            element-rule
                name
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
```


©2011 Avaya Inc. All Rights Reserved.

```
                new-value                        333.91.119.218
        header-rule
                name                             HistRegex
                header-name                      History-Info
                action                           store
                comparison-type                  pattern-rule
                msg-type                         request
                methods                          INVITE
                match-value                      ()
                new-value
                element-rule
                        name                             GetUser
                        parameter-name
                        type                             uri-user
                        action                           store
                        match-val-type                   any
                        comparison-type                  pattern-rule
                        match-value
                        new-value
                element-rule
                        name                             GetHost
                        parameter-name
                        type                             uri-host
                        action                           store
                        match-val-type                   any
                        comparison-type                  pattern-rule
                        match-value
                        new-value
        header-rule
                name                             storeSDP
                header-name                      Content-Type
                action                           store
                comparison-type                  case-sensitive
                msg-type                         any
                methods                          INVITE,UPDATE
                match-value
                new-value
                element-rule
                        name                             StoreZeros
                        parameter-name                   application/sdp
                        type                             mime
                        action                           store
                        match-val-type                   any
                        comparison-type                  pattern-rule
                        match-value                      c=IN IP4 0.0.0.0
                        new-value
                element-rule
                        name                             StoreInactive
                        parameter-name                   application/sdp
                        type                             mime
                        action                           store
                        match-val-type                   any
                        comparison-type                  pattern-rule
                        match-value                      a=inactive
                        new-value
        header-rule
```


©2011 Avaya Inc. All Rights Reserved.

```
            name                                ModifySDP
            header-name                         Content-Type
            action                              manipulate
            comparison-type                     boolean
            msg-type                            any
            methods                             INVITE,UPDATE
            match-value
$storeSDP.$StoreZeros&$storeSDP.$StoreInactive
            new-value
            element-rule
                    name                                changeInactive
                    parameter-name                      application/sdp
                    type                                mime
                    action                              find-replace-all
                    match-val-type                      any
                    comparison-type                     pattern-rule
                    match-value                         a=inactive
                    new-value                           a=sendonly
            element-rule
                    name                                changeIP
                    parameter-name                      application/sdp
                    type                                mime
                    action                              find-replace-all
                    match-val-type                      any
                    comparison-type                     pattern-rule
                    match-value                         0.0.0.0
                    new-value                           222.10.98.98
        header-rule
            name                                HstInfChkTmpUnav
            header-name                         History-Info
            action                              store
            comparison-type                     pattern-rule
            msg-type                            request
            methods                             INVITE
            match-value                         .*Temporarily.*Unavailable.*
            new-value
        header-rule
            name                                HstInfChkMvTmp
            header-name                         History-info
            action                              store
            comparison-type                     pattern-rule
            msg-type                            request
            methods                             INVITE
            match-value                         .*Moved.*Temporarily.*
            new-value
        header-rule
            name                                HstInfChkBsyHere
            header-name                         History-info
            action                              store
            comparison-type                     pattern-rule
            msg-type                            any
            methods                             INVITE
            match-value                         .*Busy.*Here.*
            new-value
        header-rule
            name                                FmatHistInfo
```


©2011 Avaya Inc. All Rights Reserved.

```
                header-name                     History-Info
                action                          manipulate
                comparison-type                 pattern-rule
                msg-type                        any
                methods                         INVITE
                match-value                     ^(.*index=1),.*$
                new-value                       $1
        header-rule
                name                            HstInfStrURI
                header-name                     History-info
                action                          store
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $HstInfChkMvTmp |
$HstInfChkBsyHere | $HstInfChkTmpUnav
                new-value
                element-rule
                        name                            StrHdr
                        parameter-name
                        type                            header-value
                        action                          store
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value
        header-rule
                name                            RplcPAI
                header-name                     P-Asserted-Identity
                action                          manipulate
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     $HstInfChkMvTmp |
$HstInfChkBsyHere | $HstInfChkTmpUnav
                new-value
                element-rule
                        name                            RplceHdrVal
                        parameter-name
                        type                            header-value
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value
$HstInfStrURI.$StrHdr.$0
                element-rule
                        name                            DelIndexVal
                        parameter-name                  index
                        type                            header-param
                        action                          delete-element
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value
                element-rule
```


©2011 Avaya Inc. All Rights Reserved.

```
                name                            DelIndexNam
                parameter-name                  index
                type                            header-param-name
                action                          delete-element
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value
        element-rule
                name                            DelUsrVal
                parameter-name                  reason
                type                            uri-header
                action                          delete-element
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value
        element-rule
                name
                parameter-name
                type                            uri-display
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       "\"TELUS\" "
        element-rule
                name                            ChgURIHost
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       333.10.98.98
    header-rule
        name                            nt8000Removal
        header-name                     Content-Type
        action                          manipulate
        comparison-type                 case-sensitive
        msg-type                        any
        methods                         INVITE
        match-value
        new-value
        element-rule
                name                            rmvMimeType
                parameter-name                  application/sdp
                type                            mime
                action                          find-replace-all
                match-val-type                  any
                comparison-type                 pattern-rule
                match-value                     \Ra=rtpmap:111\s+X-nt-
inforeq/8000.*
                new-value
        element-rule
                name                            rmv111FmMLine
```


©2011 Avaya Inc. All Rights Reserved.

```
                    parameter-name                          application/sdp
                    type                                    mime
                    action                                  find-replace-all
                    match-val-type                          any
                    comparison-type                         pattern-rule
                    match-value
(m=audio.*)\s111(\s?.*)
                    new-value                               $1+$2
        header-rule
                name                                    Status180Str
                header-name                             @status-line
                action                                  store
                comparison-type                         case-sensitive
                msg-type                                any
                methods
                match-value
                new-value
                element-rule
                    name                                    ChkRspCode
                    parameter-name
                    type                                    status-code
                    action                                  store
                    match-val-type                          any
                    comparison-type                         pattern-rule
                    match-value                             18\d
                    new-value
        header-rule
                name                                    RmvPAI
                header-name                             P-asserted-identity
                action                                  delete
                comparison-type                         boolean
                msg-type                                any
                methods
                match-value                             $Status180Str.$ChkRspCode
                new-value
        header-rule
                name                                    delete_mcdn
                header-name                             Content-Type
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                any
                methods
                match-value
                new-value
                element-rule
                    name                                    delete_nt_epid
                    parameter-name                          application/x-nt-epid-
frag-hex;version-ssLinux-7.50.17;base=x2611
                    type                                    mime
                    action                                  delete-element
                    match-val-type                          any
                    comparison-type                         case-sensitive
                    match-value
                    new-value
                element-rule
                    name                                    delete_nt_mcdn
```


©2011 Avaya Inc. All Rights Reserved.

```
                        parameter-name                 application/x-nt-mcdn-
frag-hex;version-ssLinux-7.50.17;base=x2611
                        type                           mime
                        action                         delete-element
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value
        header-rule
                name                           delete_X_nt_e164_clid
                header-name                    X-nt-e164-clid
                action                         delete
                comparison-type                case-sensitive
                msg-type                       any
                methods
                match-value
                new-value
        header-rule
                name                           delete_Alert_Info
                header-name                    Alert-info
                action                         delete
                comparison-type                case-sensitive
                msg-type                       any
                methods
                match-value
                new-value
        header-rule
                name                           search_privacy
                header-name                    Privacy
                action                         store
                comparison-type                boolean
                msg-type                       any
                methods
                match-value                    id
                new-value
        header-rule
                name                           Create_Diversion_unavailable
                header-name                    Diversion
                action                         add
                comparison-type                boolean
                msg-type                       any
                methods
                match-value                    $HstInfChkMvTmp |
$HstInfChkBsyHere | $HstInfChkTmpUnav
                new-value
<sip:+$HistRegex[0].$GetUser.$0+@+$HistRegex[0].$GetHost.$0+>;privacy=off;rea
son=unconditional;screen=no
                element-rule
                        name                           replace_uri_host
                        parameter-name                 uri-host
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      222.10.98.98
```


©2011 Avaya Inc. All Rights Reserved.

```
            element-rule
                    name                                       mod_privacy
                    parameter-name                             privacy
                    type                                       header-param
                    action                                     replace
                    match-val-type                             any
                    comparison-type                            boolean
                    match-value                                $search_privacy
                    new-value                                  Full
        header-rule
            name                                       DelHstInfo
            header-name                                History-Info
            action                                     delete
            comparison-type                            case-sensitive
            msg-type                                   request
            methods                                    INVITE
            match-value
            new-value
        header-rule
            name                                       delPLocation
            header-name                                P-Location
            action                                     delete
            comparison-type                            pattern-rule
            msg-type                                   any
            methods
            match-value
            new-value
        header-rule
            name                                       delRoute
            header-name                                Route
            action                                     delete
            comparison-type                            pattern-rule
            msg-type                                   any
            methods
            match-value
            new-value
        last-modified-by                   admin@222.10.98.103
        last-modified-date                 2011-07-12 15:41:46
```

The following sip-manipulation **TELUS_To_CS1K, *in-manipulationid,*** is applied to the **INSIDE** realm and translates the incoming SIP header information for CS1K. These rules perform the following:

- The header rule **modRURI** changes the incoming IP address of the TELUS SBC to the Avaya CS1K Domain Name in the Request URI headers that are sent to the CS1K elements.

```
sip-manipulation
        name                               TELUS_To_CS1K
        description
        split-headers
        join-headers
        header-rule
            name                                       modRURI
```


©2011 Avaya Inc. All Rights Reserved.

```
            header-name                     request-uri
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
            element-rule
                    name                            modRURI
                    parameter-name
                    type                            uri-host
                    action                          replace
                    match-val-type                  any
                    comparison-type                 case-sensitive
                    match-value
                    new-value                       TELUS.com
    last-modified-by                admin@console
    last-modified-date              2011-05-03 19:35:44
```

6.8. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.

The key steering pool (***steering-pool***) fields are:

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

```
steering-pool
        ip-address                      222.10.98.98
        start-port                      20000
        end-port                        39999
        realm-id                        OUTSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2011-01-08 20:09:01

steering-pool
        ip-address                      111.10.97.184
        start-port                      20000
        end-port                        39999
        realm-id                        INSIDE
        network-interface
        last-modified-by                admin@console
        last-modified-date              2011-01-08 20:09:08
```

6.9. Local Policy

The local policies below govern the routing of SIP messages from elements on the network on which the Avaya elements, (e.g. CS1K), reside to the TELUS system and vice versa.

©2011 Avaya Inc. All Rights Reserved.

```
local-policy
        from-address
                               333.91.119.218
        to-address
                               4036929464
                               4036929465
                               4036929466
                               4036929467
                               4036929468
                               4036929469
                               4036929470
                               4036929471
                               4036929472
                               4036929473
        source-realm
                               OUTSIDE
        description            TELUS_to_CS1K
        activate-time          N/A
        deactivate-time        N/A
        state                  enabled
        policy-priority        none
        last-modified-by       admin@222.10.98.103
        last-modified-date     2011-07-07 11:26:00
        policy-attribute
                next-hop               111.10.97.198
                realm                  INSIDE
                action                 none
                terminate-recursion    disabled
                carrier
                start-time             0000
                end-time               2400
                days-of-week           U-S
                cost                   0
                app-protocol           SIP
                state                  enabled
                methods
                media-profiles
                lookup                 single
                next-key
                eloc-str-lkup          disabled
                eloc-str-match
```

```
local-policy
        from-address
                               TELUS.com
                               anonymous.invalid
        to-address
                               *
        source-realm
                               INSIDE
        description            CS1K_To_TELUS
        activate-time          N/A
        deactivate-time        N/A
        state                  enabled
```


©2011 Avaya Inc. All Rights Reserved.

```
        policy-priority               none
        last-modified-by              admin@222.10.98.103
        last-modified-date            2011-07-14 10:47:05
        policy-attribute
                next-hop                      333.91.119.218
                realm                         OUTSIDE
                action                        none
                terminate-recursion           disabled
                carrier
                start-time                    0000
                end-time                      2400
                days-of-week                  U-S
                cost                          0
                app-protocol                  SIP
                state                         enabled
                methods
                media-profiles
                lookup                        single
                next-key
                eloc-str-lkup                 disabled
                eloc-str-match
```


©2011 Avaya Inc. All Rights Reserved.

7. Verification Steps

The following steps may be used to verify the configuration.

7.1. General

Place an inbound/outbound call to/from to a PSTN phone to/from an internal CS1K phone, answer the call, and verify that two-way speech path exists. Check call display name and number to ensure the correct info was sent/received.   Perform hold/retrieve on calls. Verify the call remains stable for several minutes and disconnect properly.

7.2. Verify Call Establishment on CS1K Call Server

a) Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1K to trace the DN when the call is in progress and or idle. The call scenario involved the CS1K extension 9464 calling PSTN phone number 6139675204.

- Login Call Server CLI (please refer to Section 5.1.2 for more detail)
- Login to the Overlay command prompt, issue the command **LD 80** and then **trace 0 9464**.
- After 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 an active call:

```
>ld 80

.trac 0 9464

ACTIVE  VTN 096 0 00 01

ORIG   VTN 096 0 00 01  KEY 0  SCR MARP  CUST 0  DN 9464  TYPE 2004P1
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 135.10.98.40  PORT: 5200
TERM   VTN 100 0 00 31   VTRK IPTI  RMBR  100 32 OUTGOING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 135.10.97.184
  FAR-END MEDIA ENDPOINT IP: 135.10.97.184  PORT: 20004
  FAR-END VendorID: AVAYA-SM-6.1.1.0.611023
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 616139675204
MAIN_PM  ESTD
TALKSLOT  ORIG  2   TERM  39
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 34360


----  ISDN ISL CALL (TERM) ----
CALL REF # =  416
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
```


©2011 Avaya Inc. All Rights Reserved.

```
CALLING NO =  4036929464  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
CALLED NO  =  16139675204  NUM_PLAN:PRIVATE     TON:NETWORK SPECIFIC  ESN:SPN
```

This is the example after the call on 9464 is completed.

```
.trac 0 9464

IDLE VTN 096 0 00 01   MARP
```

b) SIP Trunk monitoring (LD 32)
Place a call inbound from PSTN (6139675204) to CS1K (4036929464). Then check the SIP Trunk status by using LD 32, the output below shows that one trunk is busy.

```
>ld 32
NPR003
.stat 100 0
031 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

And this is the example after the call is completed, shows that there are no trunks busy.

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

7.3. Protocol Traces

Wireshark is use to analyze the calss to verify the following information:

The following SIP headers are inspected:
- RequestURI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- History-Info: verify the call forward information and reason code.
- Diversion: verity the name and number and reason code.
- P-Asserted-Identity: verify the display name and display number.
- Privacy: verify the “user, id” masking.

The following attributes in SIP message body are inspected:
- Connection Information (c): verify IP address of far end endpoint
- Time Description (t): verify session timeout of far end endpoint
- Media Description (m): verify audio port, codec, DTMF event description

©2011 Avaya Inc. All Rights Reserved.

- Media Attribute (a): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

Figure 7:1 shows a typical capture of an external call made from 6139675204 to CS1K extension 9465.

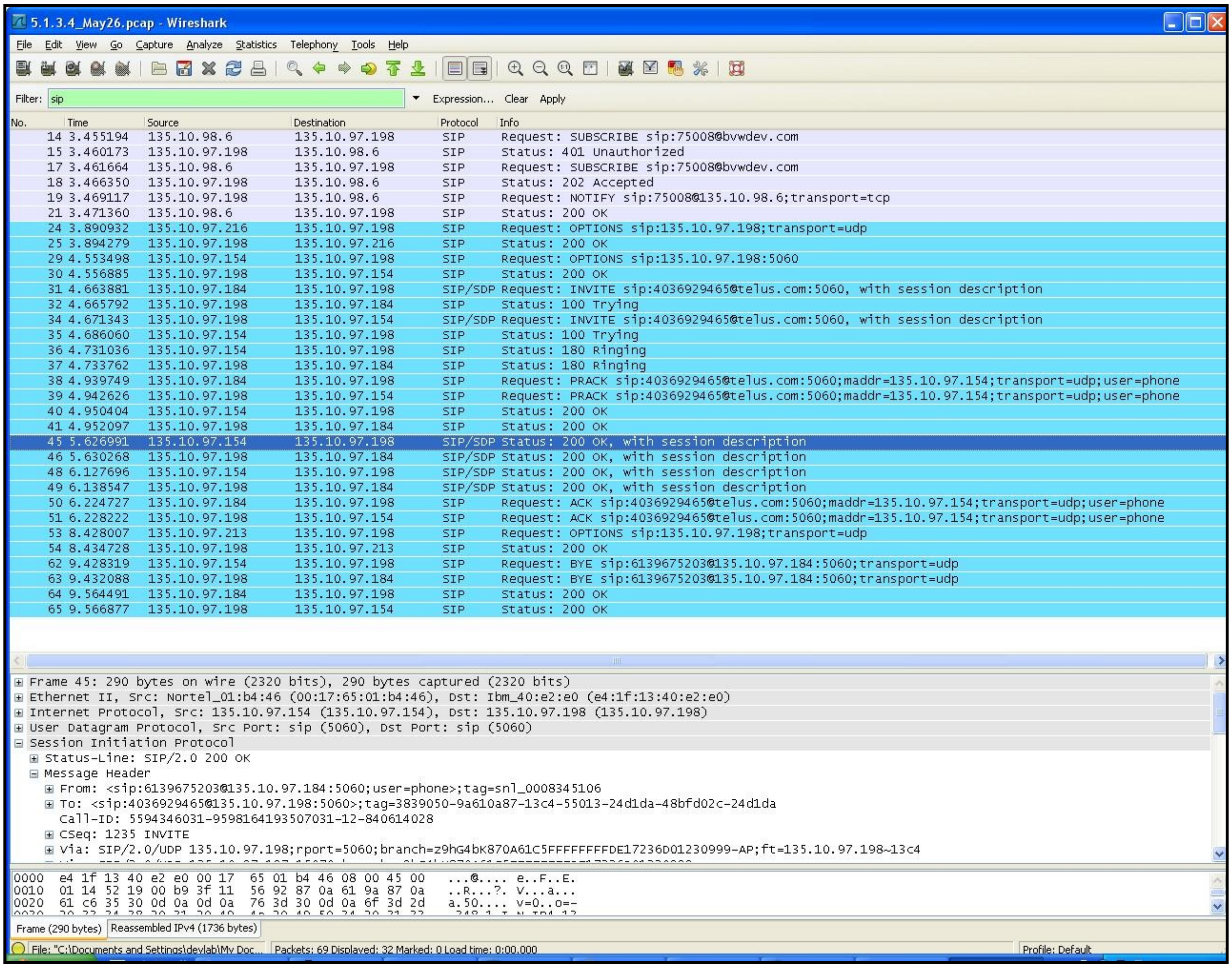

Figure 7:1 Wireshark capture

©2011 Avaya Inc. All Rights Reserved.

The flow of SIP messaging is examined to ensure proper operation, as shown in **Figure 7:2.**

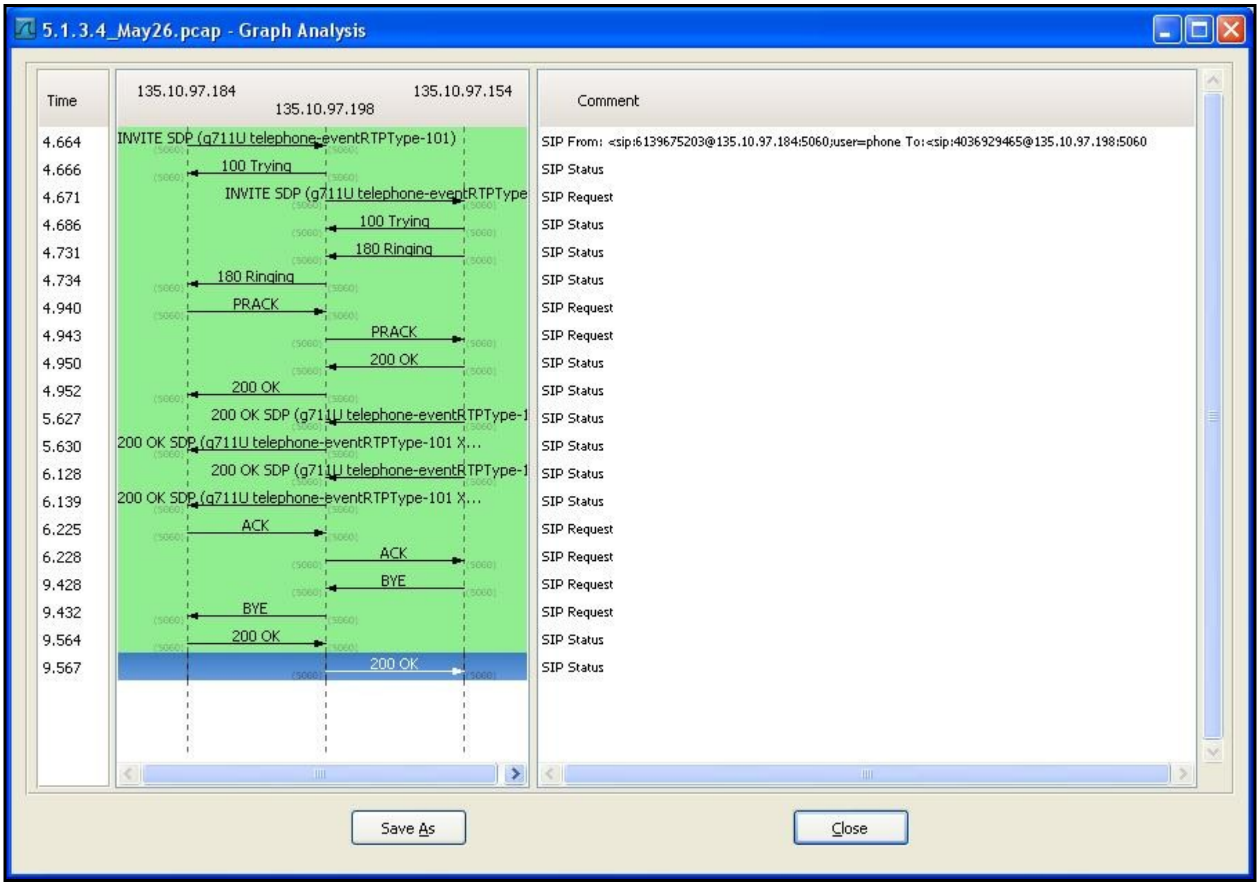

Figure 7:2 Wireshark call flow

©2011 Avaya Inc. All Rights Reserved.

The contents of the SIP headers are examined as well to verify they contain the proper information as seen in **Figure 7:3**.

```
⊞ Frame 45: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits)
⊞ Ethernet II, Src: Nortel_01:b4:46 (00:17:65:01:b4:46), Dst: Ibm_40:e2:e0 (e4:1f:13:40:e2:e0)
⊞ Internet Protocol, Src: 135.10.97.154 (135.10.97.154), Dst: 135.10.97.198 (135.10.97.198)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ From: <sip:6139675203@135.10.97.184:5060;user=phone>;tag=snl_0008345106
    ⊞ To: <sip:4036929465@135.10.97.198:5060>;tag=3839050-9a610a87-13c4-55013-24d1da-48bfd02c-24d1da
      Call-ID: 5594346031-9598164193507031-12-840614028
    ⊞ CSeq: 1235 INVITE
    ⊞ Via: SIP/2.0/UDP 135.10.97.198;rport=5060;branch=z9hG4bK870A61C5FFFFFFFFDE17236D01230999-AP;ft=135.10.97.198~13c4
    ⊞ Via: SIP/2.0/UDP 135.10.97.197:15070;branch=z9hG4bK870A61C5FFFFFFFFDE17236D01230999
    ⊞ Via: SIP/2.0/UDP 135.10.97.197:15070;branch=z9hG4bK870A61C5FFFFFFFFDE17236D11230997
    ⊞ Via: SIP/2.0/UDP 135.10.97.197:15070;branch=z9hG4bK870A61C5FFFFFFFFDE17236D11230996
    ⊞ Via: SIP/2.0/UDP 135.10.97.198;rport;branch=z9hG4bK5nq2g520a0jgrhs1m0g1.1-AP;ft=135.10.97.198~13c4
    ⊞ Via: SIP/2.0/UDP 135.10.97.184:5060;branch=z9hG4bK5nq2g520a0jgrhs1m0g1.1
      Supported: 100rel,x-nortel-sipvc,replaces
      Require: timer
      User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
    ⊞ P-Asserted-Identity: <sip:4036929465@telus.com;user=phone>
      Privacy: none
      Record-Route: <sip:f82d164@135.10.97.198;transport=udp;lr>
      Record-Route: <sip:135.10.97.197:15060;lr;sap=-1458256621*1*016asm-callprocessing.sar-983496313~1306434955764~-1674424857~1>
      Record-Route: <sip:f82d164@135.10.97.198;transport=udp;lr>
    ⊞ Contact: <sip:4036929465@telus.com:5060;maddr=135.10.97.154;transport=udp;user=phone>
      Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
      Content-Type: application/sdp
      Content-Length: 250
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): - 348 1 IN IP4 135.10.97.154
        Session Name (s): -
      ⊞ Connection Information (c): IN IP4 135.10.98.19
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 5200 RTP/AVP 0 101 111
      ⊞ Connection Information (c): IN IP4 135.10.98.19
      ⊞ Media Attribute (a): ptime:20
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
      ⊞ Media Attribute (a): fmtp:101 0-15
      ⊞ Media Attribute (a): rtpmap:111 X-nt-inforeq/8000
```

Figure 7:3 Wireshark packet

©2011 Avaya Inc. All Rights Reserved.

8. Conclusion

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 1.2**, the test result met the objectives outlined in **Section 1.1**. The TELUS system is considered **compliant** with the Avaya Communication Server 1000 Release 7.5, Avaya Aura ® Session Manager Release 6.1 and Acme Packet SBC Release 6.2.

9. Additional References

Product documentation for Avaya products may be found at:
http://support.avaya.com/css/appmanager/public/support

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

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

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

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

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

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

©2011 Avaya Inc. All Rights Reserved.

©2011 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.