Avaya Solution & Interoperability Test Lab

Application Notes for Amtelco Infinity Intelligent SIP Attendant Console with Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Amtelco Infinity SIP Attendant Console to interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks. Amtelco Infinity SIP Attendant Console is a SIP-based soft phone solution that provides phone and operator state controls during call handling.

In the compliance testing, Amtelco Infinity SIP Attendant Console used the SIP trunks interface from Avaya Aura® Session Manager to provide attendant consoles for Avaya Communication Server 1000.

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

1. Introduction

These Application Notes describe the configuration steps required for Amtelco Infinity SIP Attendant Console to interoperate with Avaya Communication Server 1000 (hereafter referred as Communication Server 1000) and Avaya Aura® Session Manager (hereafter referred to as Session Manager) using SIP trunks. Amtelco Infinity SIP Attendant Console (hereafter referred to as Infinity) is a SIP-based soft phone solution that provides phone and operator state controls during call handling.

In the compliance testing, Amtelco Infinity SIP Attendant Console used the SIP trunks interface from Avaya Aura® Session Manager to provide attendant consoles for Avaya Communication Server 1000.

The Amtelco Infinity SIP Attendant Console solution consists of an Infinity server and attendants with desktop computers running Amtelco Infinity Telephone Agent. The Infinity server controls routing of calls to/from the attendants, and with all attendant related activities such as answer/drop calls performed from Amtelco Infinity Telephone Agent.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were placed manually with necessary attendant actions such as hold and transfer performed from the attendant desktops to verify various call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Infinity server and to the attendants.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included G.711, G.729, codec negotiation, DTMF, hold/resume, drop, display, blind transfer, attended conference, inbound, outbound, multiple calls, and multiple agents.

The serviceability testing focused on verifying the ability of Infinity to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the Infinity server and to the attendants.

2.2. Test Results

All test cases were executed and passed. The following were observations on Infinity from the compliance testing.

- Infinity needs to be configured to send OPTIONS, else won't respond to OPTIONS and Session Manager will assume the connectivity is down. Furthermore, enabling OPTIONS on Infinity requires configuration of an account, or else OPTIONS won't be sent.
- Infinity only supports G 7.11 for outgoing calls and G 7.11 and G 729 for incoming calls.
- There is no MUTE feature available on the Infinity GUI. Infinity expects agents to use this feature if available on their headsets locally.
- In case of Ethernet connectivity being lost to the Infinity Server during an active call, audio connection gets dropped, member graphical user interface (GUI) shows red OFF. Upon link restoration, member needs to end call, logout and login, and may see "Next Call Ring x yyyyy" on screen, depending on whether the calling party held on to the call while Ethernet connectivity was lost.
- In case of Ethernet connectivity being lost to the Infinity Telephone agent during an active call, audio drops and agent sees a login screen. Upon link restoration and agent performing a login, GUI may appear as if call waiting and alerting tone applied, even when there is no active call. Agent will need to connect and end before returning back to normal. Upon agent pressing F1, alerting stops and GUI appears as if agent connected to a call when there is no call. If the caller on the other end is still on line, then call is presented to the next available agent.

2.3. Support

Technical support on Infinity can be obtained through the following:

- **Phone:** (800) 553-7679
- **Email:** service@amtelco.com
- **Web:** www.amtelco.com/Welcome.htm

3. Reference Configuration

As shown in **Figure 1**, attendants are running the Infinity Telephone Agent soft phone application on the desktops, and the administrator is running the Infinity Supervisor.

SIP trunks are used between Infinity SIP Attendant Console and Session Manager. A five digit Uniform Dial Plan was used to facilitate dialing with Infinity. Calls to extensions 76xxx are routed over the SIP trunks to Infinity. Calls from internal/ external users will be routed with digits 76000 to Infinity. Infinity will route the received call to an available attendant, and populate the answering attendant with pertinent information for the call.

The detailed administration of connectivity between Communication Server 1000 and Session Manager are not the focus of these Application Notes and will not be described.

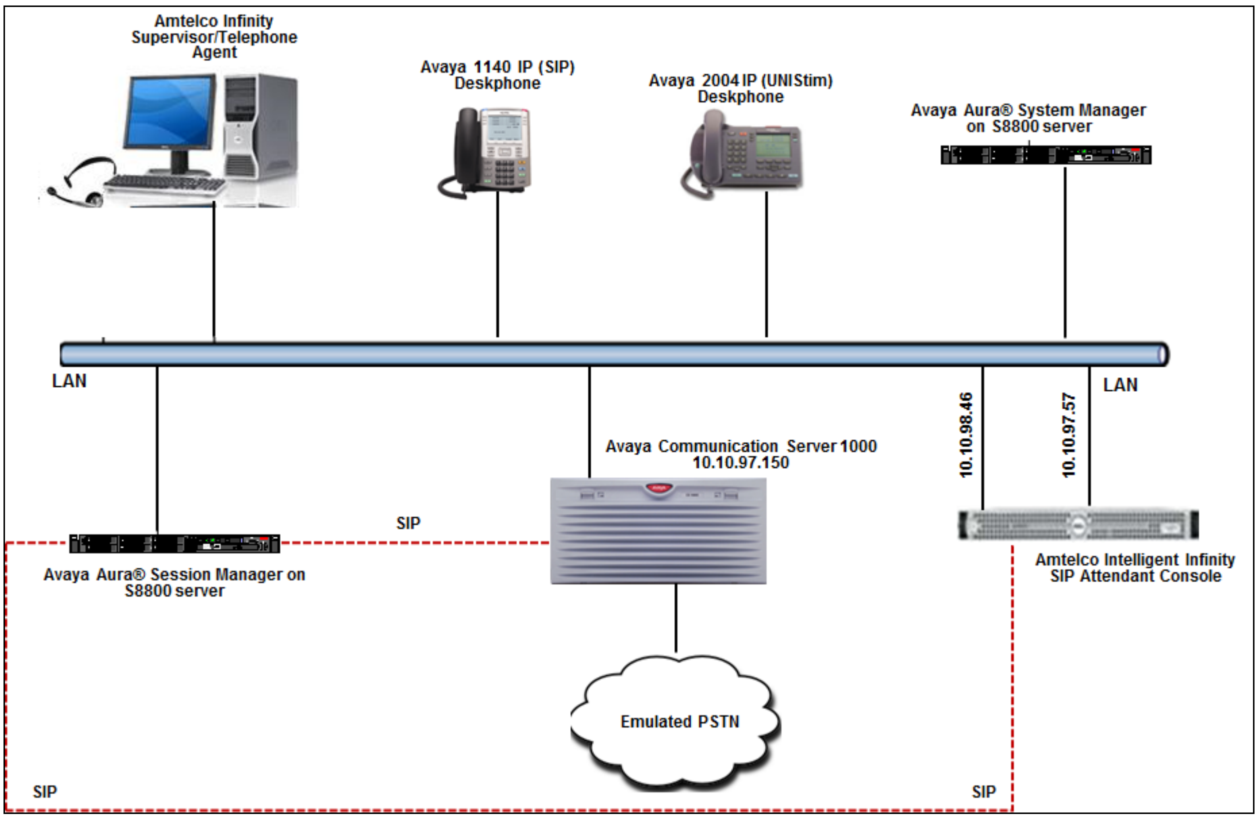


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65
Avaya Aura® Session Manager	6.3
Avaya Aura® System Manager	6.3
Avaya 2004 IP Deskphone (UNIStim)	0602B76
Avaya 1140 IP Deskphone (SIP)	04.03.12
Amtelco Infinity Intelligent SIP Attendant Console • XDS VoIP Card	5.61.08 4.48
Amtelco Infinity Supervisor	5.60.0020
Amtelco Infinity Telephone Agent	5.60.4364.53

5. Configure Avaya Communication Server 1000

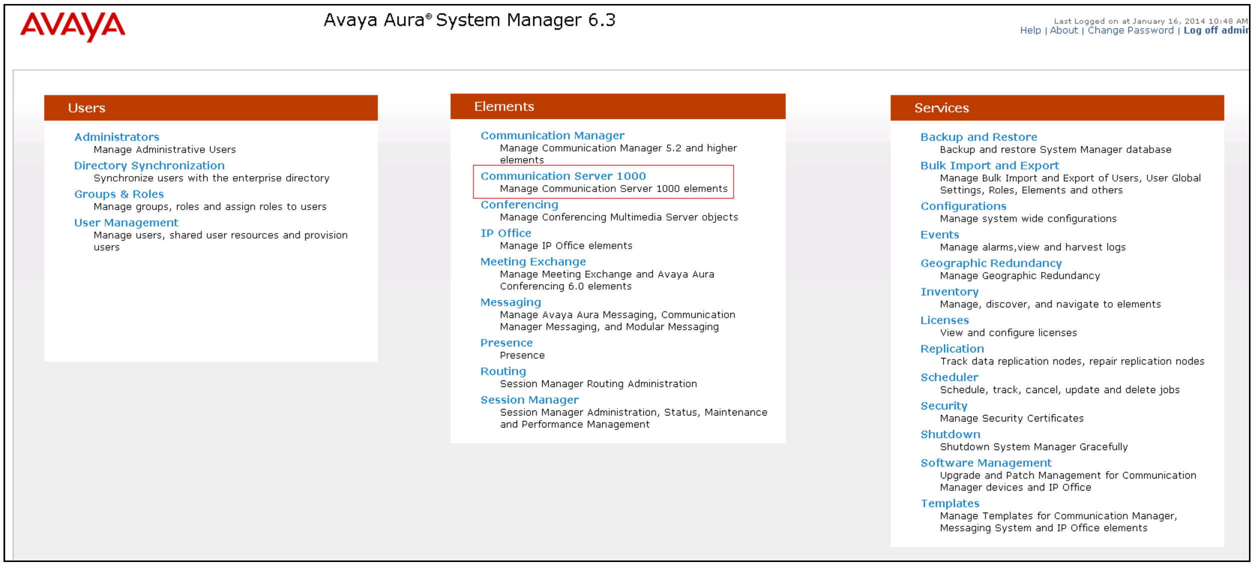
This section describes the Communication Server 1000 configuration necessary to interoperate with Session Manager and Infinity. It provides the procedures for configuring Avaya Communication Server 1000 system. The procedures include the following areas:

- Logging into the Element Manager via System Manager.
- Configuring the SIP Signaling Gateway.
- Configuring Voice Codecs on Media Gateways.
- Configuring Zones.
- Configure Integrated Services Digital Network (ISDN).
- Configuring a D-Channel.
- Configuring Route and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Dialing Plan.

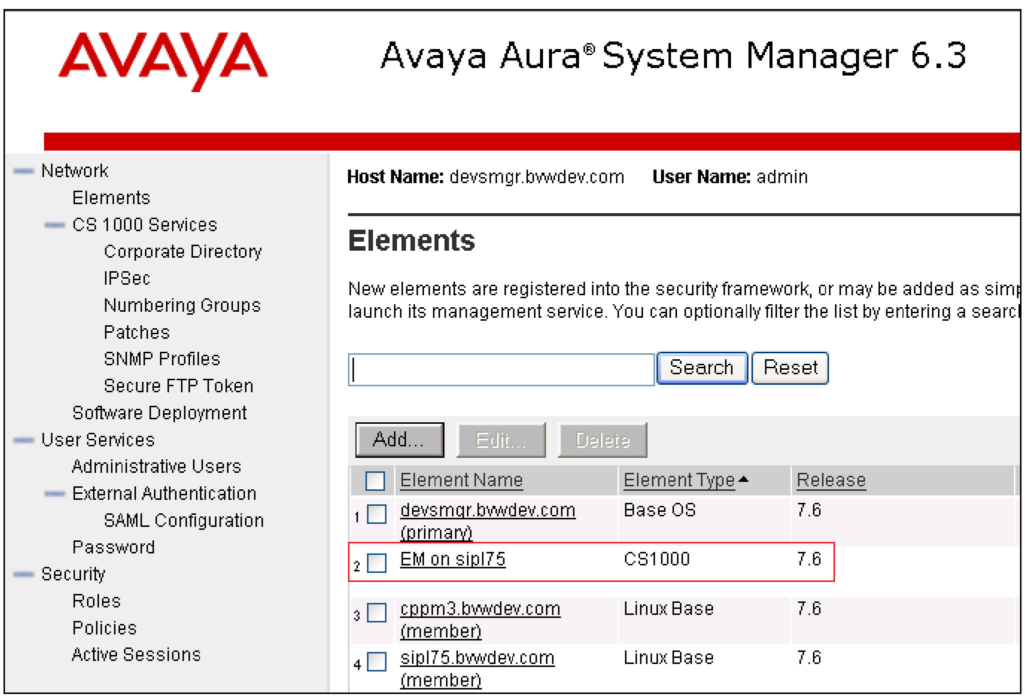
For detail configuration details of the Communication Server 1000 refer to **Section 10**.

5.1. Logging into Element Manager via Avaya Aura® System Manager

To login to the System Manager open an IE browser and type in the IP address of the System Manager in the URL (not shown). Screen below shows the main dashboard. Navigate to **Elements → Communication Server 1000**.



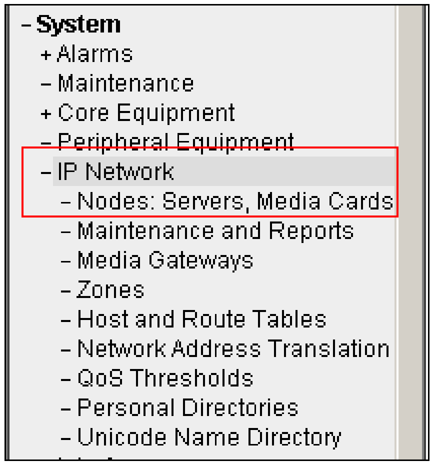
From the **Elements** page of Communication Server 1000 as shown in screen below, click on the Element **EM on sipl75**. This is the element which is configured to access the Element Manager (EM) for the Communication Server 1000 Call Server.



5.2. Configuring the SIP Signaling Gateway

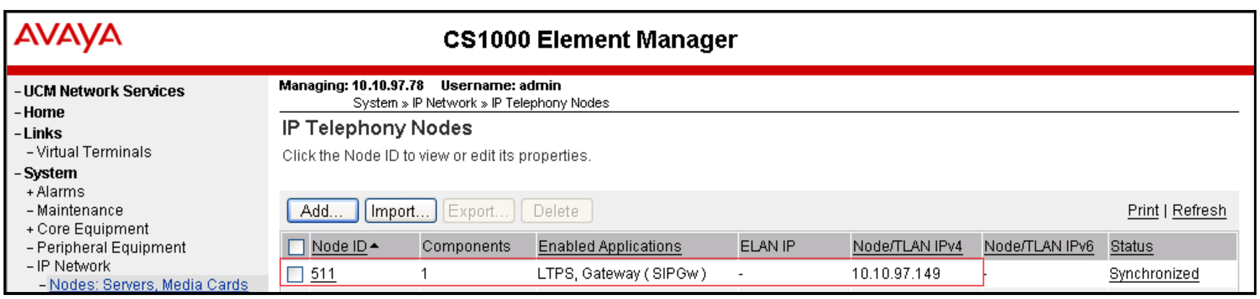
This section describes the configuration required on the SIP Signaling Gateway present on the Communication Server 1000 so that Communication Server 1000 can communicate with Session Manager via SIP Trunks.

To add a Node, from the EM left navigator screen, navigate to **System →IP Network → Nodes: Servers, Media Cards** as shown below.

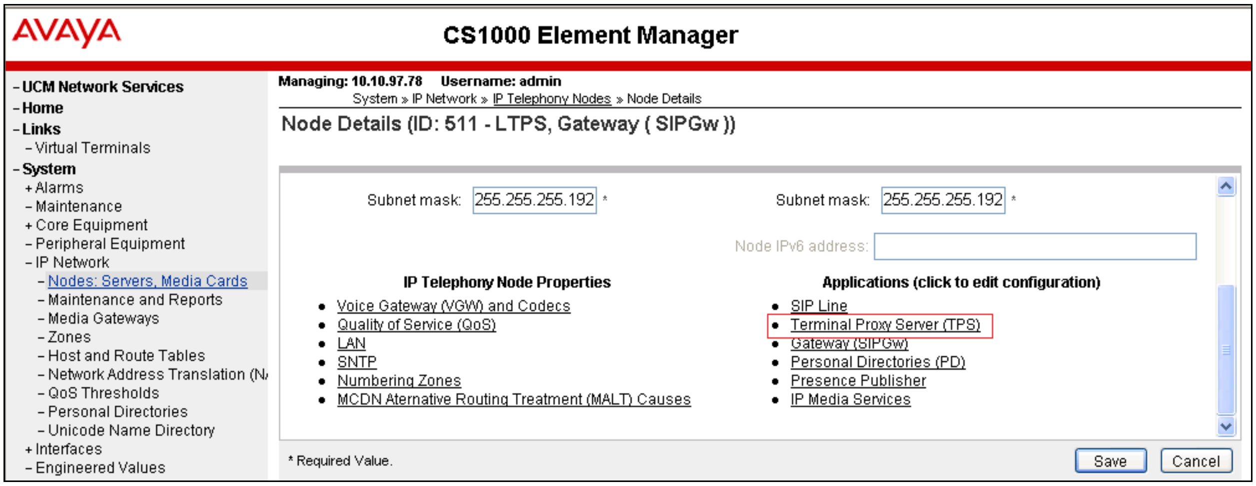


Assumption is made here that the IP Telephony node is already added.

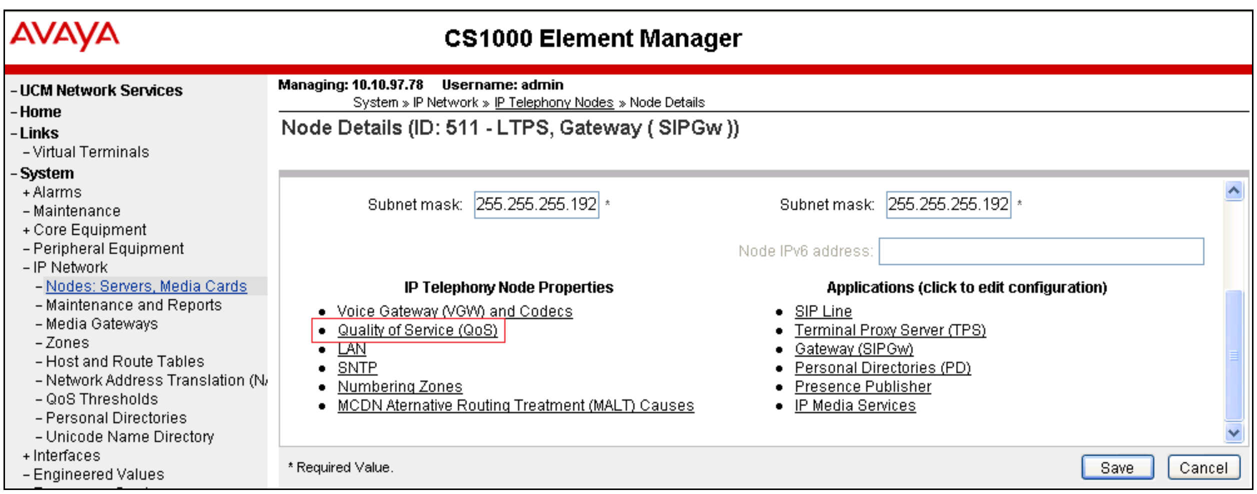
During compliance testing Node **511** was added. Click on this Node as shown in screen below to view the configured values.



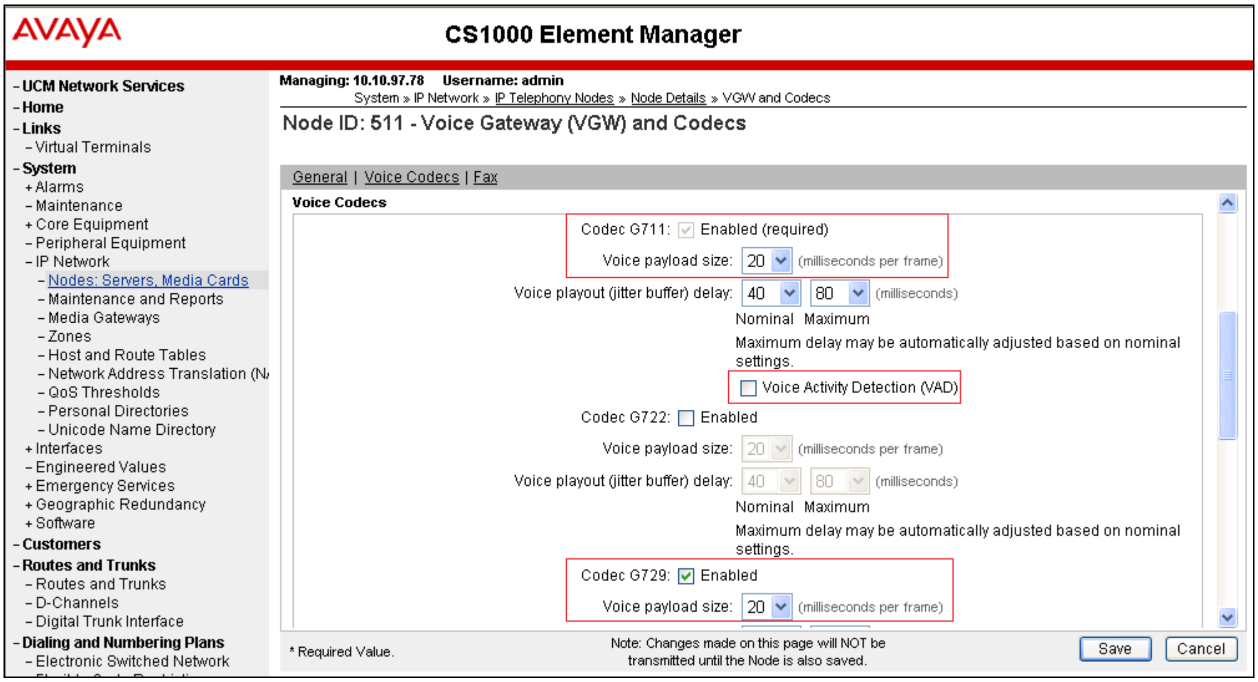
On the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link as shown in screen below. In the field **UNIStim Line Terminal Proxy Server** check the box for *Enable proxy server on this node* (not shown) and then click the **Save** button (not shown).



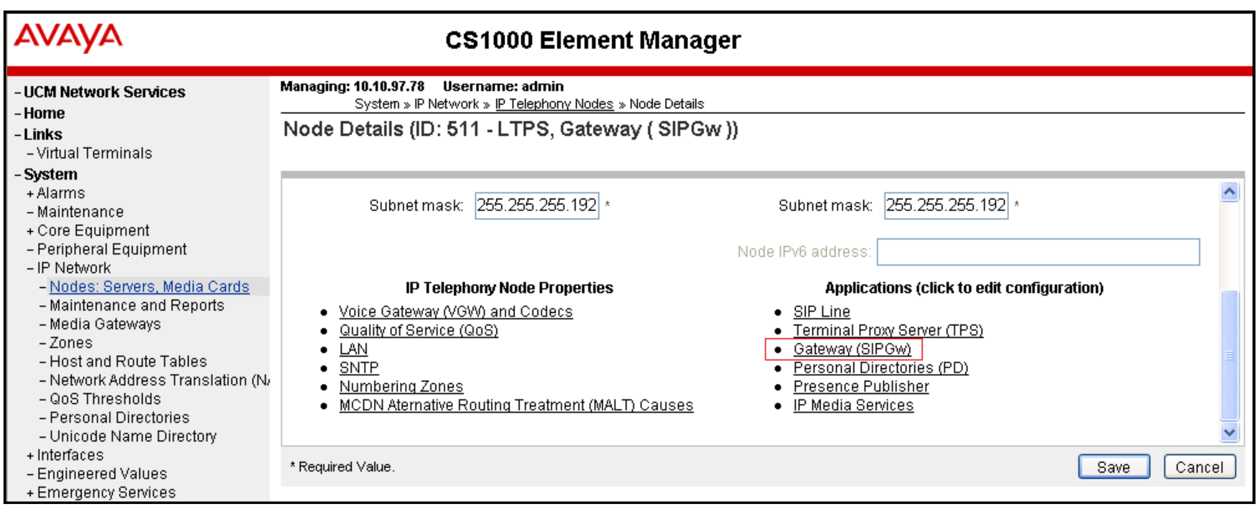
On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in screen below. Retain default values under the **Diffserv Codepoint (DSCP)** section (not shown). Click on the **Save** button (not shown).



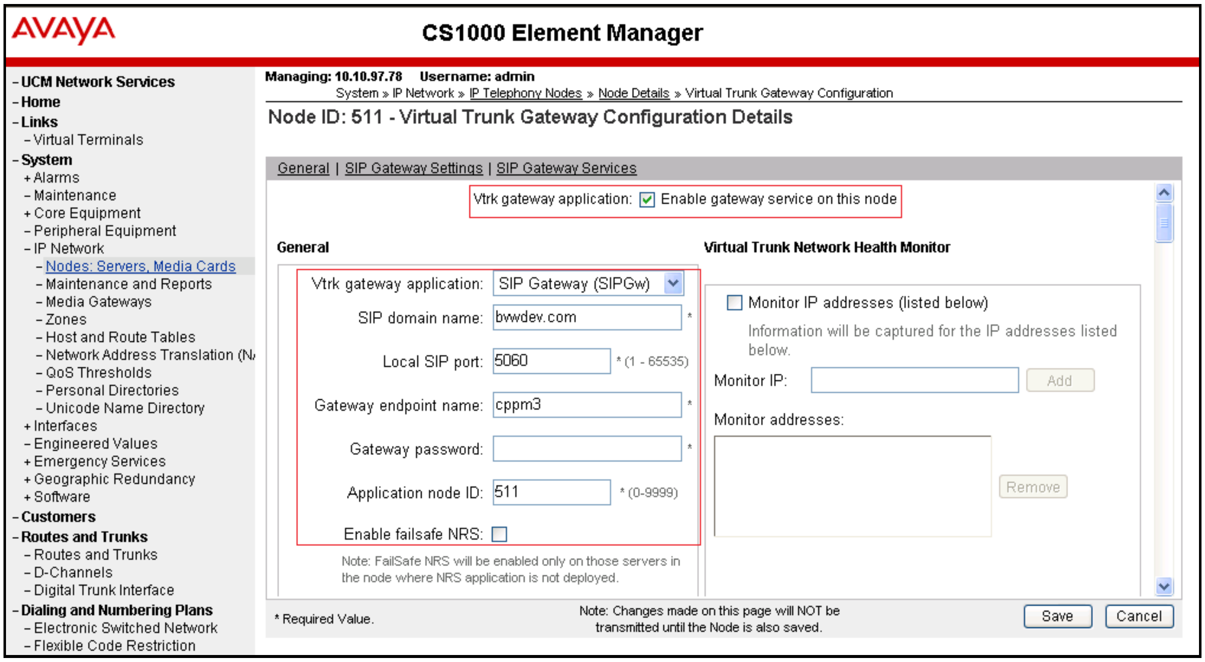
On the **Node Details** page as shown in the screen above select **Voice Gateway (VGW) and Codecs** link. The following values were configured during compliance testing as shown in the screen below.
Codec G711: Enabled by default.
Voice payload size: Select *20* from the drop down menu.
Voice Activity Detection (VAD): Uncheck this box.
Repeat the same for codec G729 and retain default values for other fields.
Click on **Save** button.



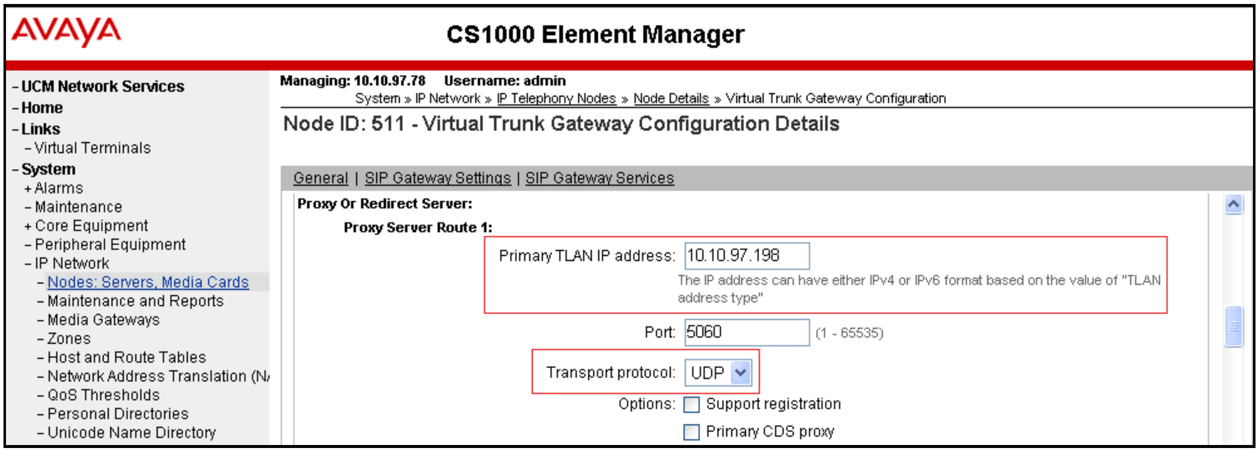
Select **Gateway (SIPGw)** link as shown below from the Node Details page.



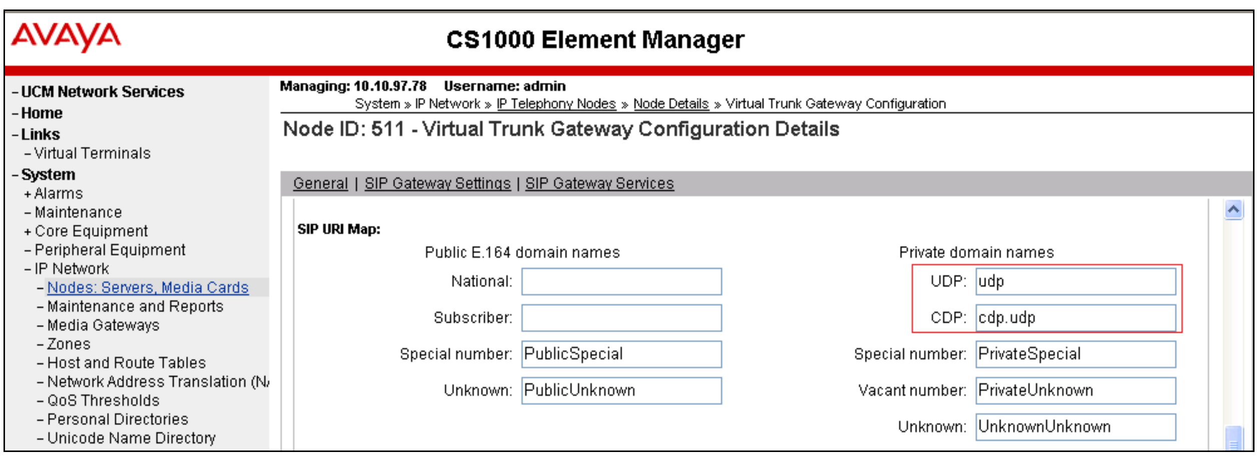
The following values were configured during compliance testing as shown in the screen below.
Vtrk gateway application: Check the ***Enable gateway service on this node*** box.
Vtrk gateway application: Select ***SIP Gateway (SIPGw)*** from the drop down menu.
SIP domain name: *bvwdev.com*. This will be the same domain name that will be configured on Session Manager.
Local SIP port: *5060*.
Gateway endpoint name: *cppm3*.
Application node ID: *511*.
Retain default values for other fields.



Scroll down to the **Proxy or Redirect Server** section. The following values were configured during compliance testing.
Primary TLAN IP address: *10.10.97.198*. This is the IP address of Session Manager.
Transport protocol: Select *UDP* from the drop down menu.
Retain default values for other fields.



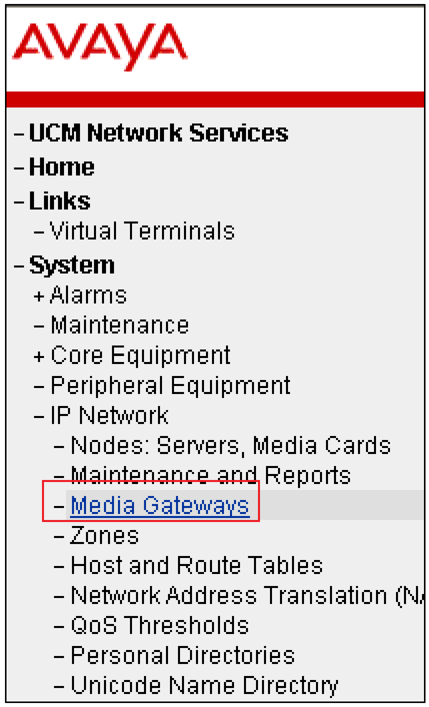
Scroll down to the **SIP URI Map** section. The following values were configured under the **Private domain names** during compliance testing.
UDP: *udp*
CDP: *cdp.udp*
Retain default values for other fields.



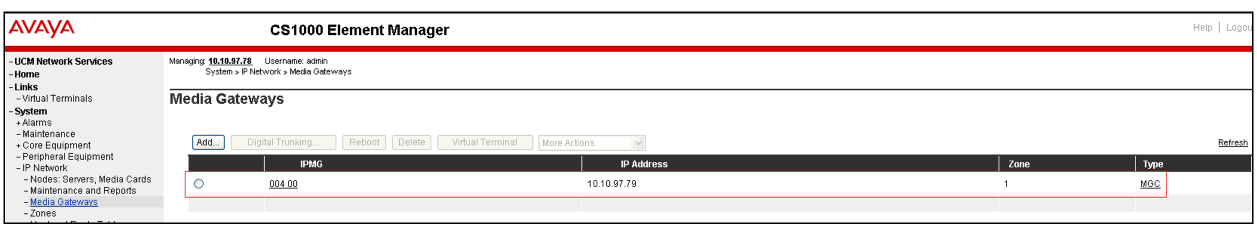
Save and transmit (not shown) these Node properties to complete the SIPGw configuration.

5.3. Configuring Voice Codecs on Media Gateways

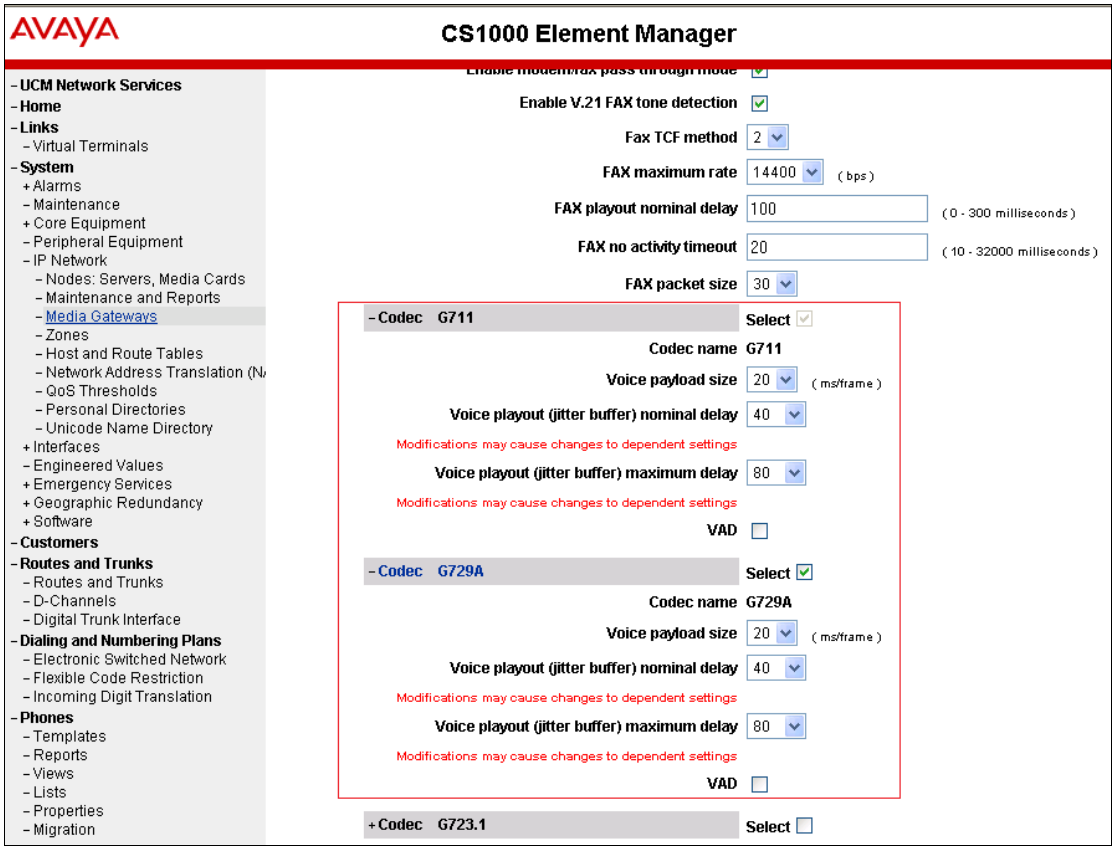
To configure voice codecs on Media Gateway Card (MGC) from the EM left navigator screen, navigate to **System →IP Network → Media Gateways** as shown below.



Screen below shows an already added MGC **004 00**. Click on the IPMG, in this case 004 00, to view the MGC configuration page. Click on the link **VGW and IP phone codec profile** (not shown).



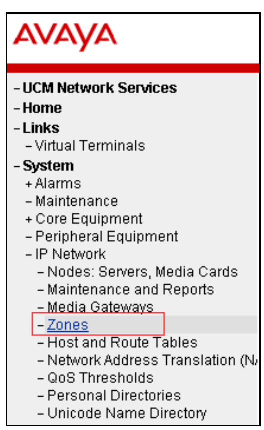
Ensure that the Codecs **G711** and **G729A** are selected as shown in the screen below. Note that the MGC has to be rebooted for the changes to take effect.



5.4. Configuring Zones

This section describes the steps to create 2 zones: One for Voice Gateways (VGW)/ IP phones, and the other for SIP Trunk.

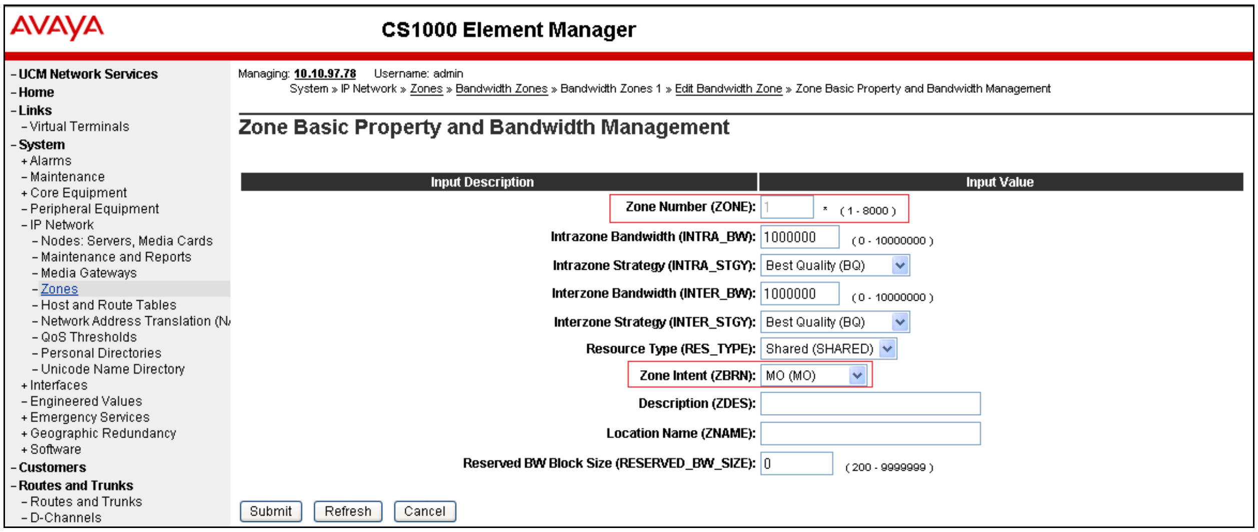
To configure zones, from the EM left navigator screen, navigate to **System →IP Network → Zones** as shown below.



During compliance testing zone 1 was configured for VGW/IP phones and zone 2 was configured for SIP trunks.

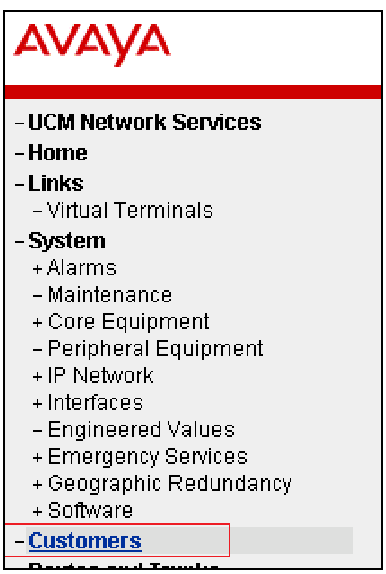
Screen below shows the configuration used for Zone number **1**. For **Zone Intent (ZBRN)** field select *MO (MO)* from the drop down list. Retain default values for other fields.

Configuration for Zone number **2** is similar to the screen below; except for **Zone Intent (ZBRN)** field select *VTRK* from the drop down list (not shown).

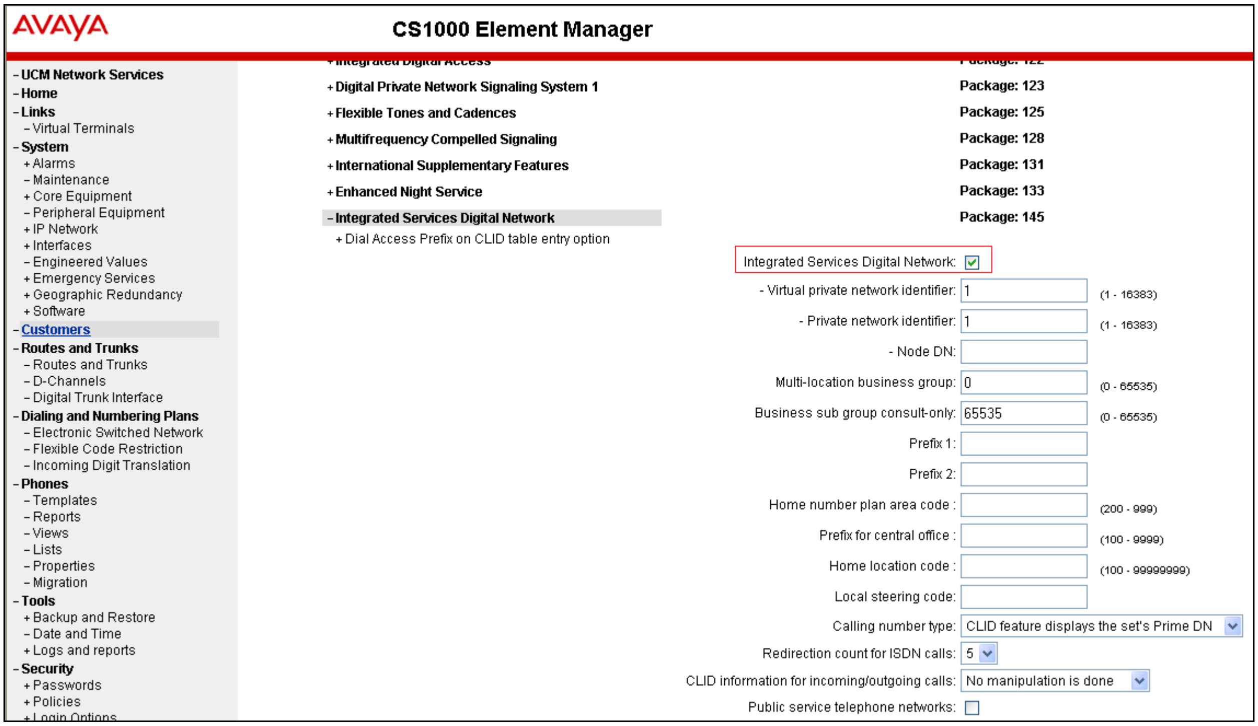


5.5. Configure Integrated Services Digital Network (ISDN)

This section ensures that the ISDN option under the Features package is selected. From the EM left navigator screen, navigate to **Customers** as shown below.

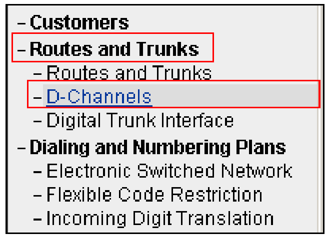


Select a customer and click on it to navigate to the **Customer Details** page (not shown). Click on the **Feature Packages** link (not shown) and from this page click on **Integrated Services Digital Network** link. Ensure that the **Integrated Services Digital Network** box is checked as shown in the screen below.

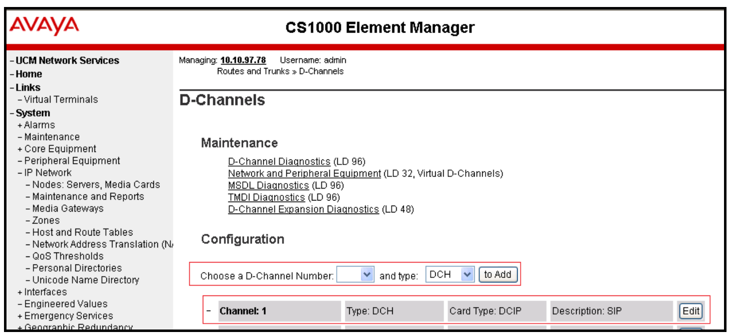


5.6. Configuring D-Channel

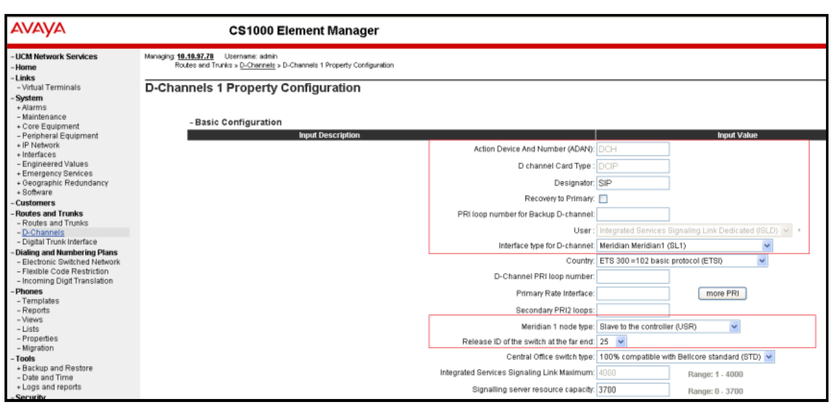
This section explains the configuration of a D-Channel for a SIP Trunk. From the EM navigation screen, navigate to **Routes and Trunks → D-Channels** as shown below.



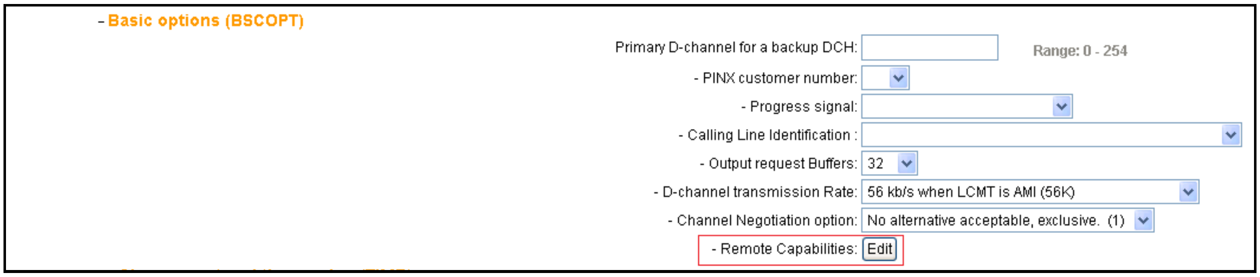
Choose an available D-Channel number to add as shown in the screen below. During compliance testing D-Channel number **1** was configured. Click on **Edit** to view its configuration.



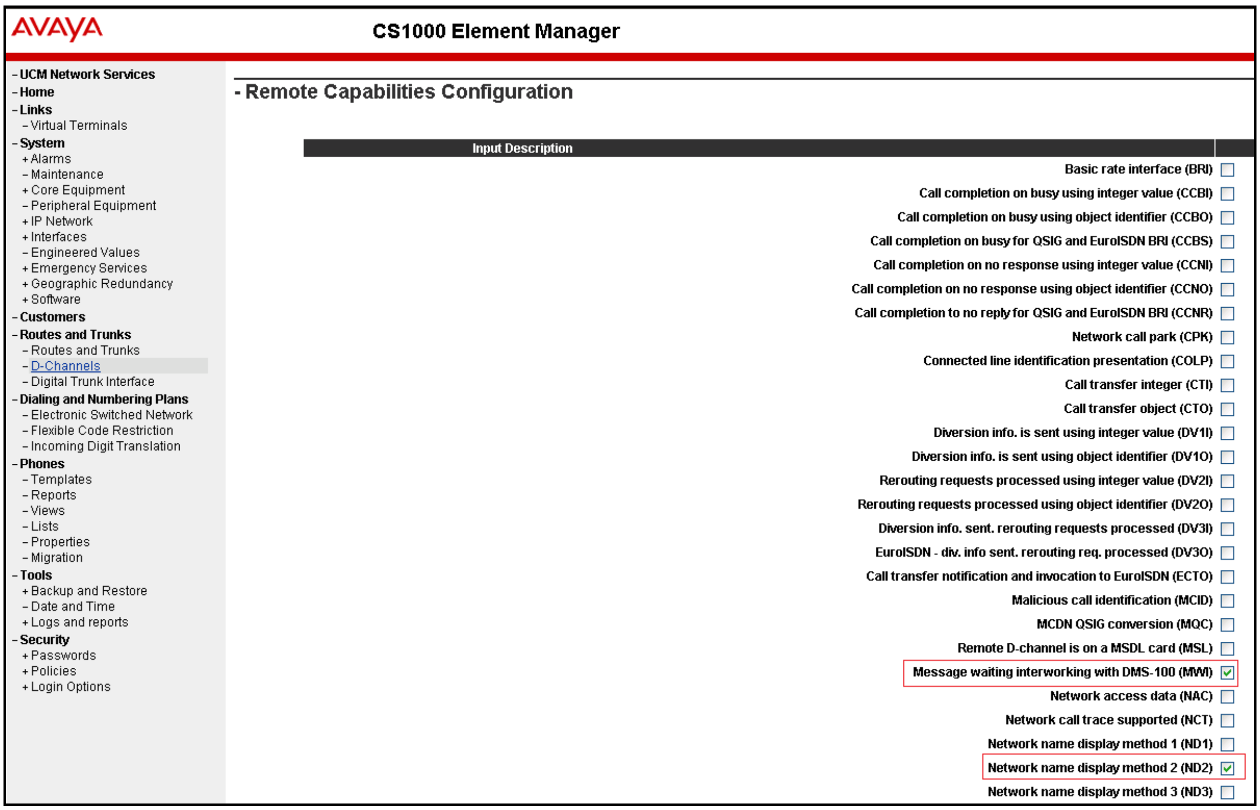
The following values were configured in **Basic Configuration** for the D-Channel as shown below.
Action Device And Number (ADAN): *DCH*.
D channel Card Type: *DCIP*.
Designator: A descriptive name.
Inerface type for D-channel: Select *Meridian Meridian1 (SL1)* from the drop down menu.
Meridian 1 node type: Select *Salve to the controller (USR)* from the drop down menu.
Release ID of the switch at the far end: Select *25* from the drop down menu.
Retain default values for all other fields.



Scroll down to edit the **Remote Capabilities** of the D-Channel that is seen under the **Basic options (BSCOPT)** section. Click on **Edit** button as shown in the screen below.



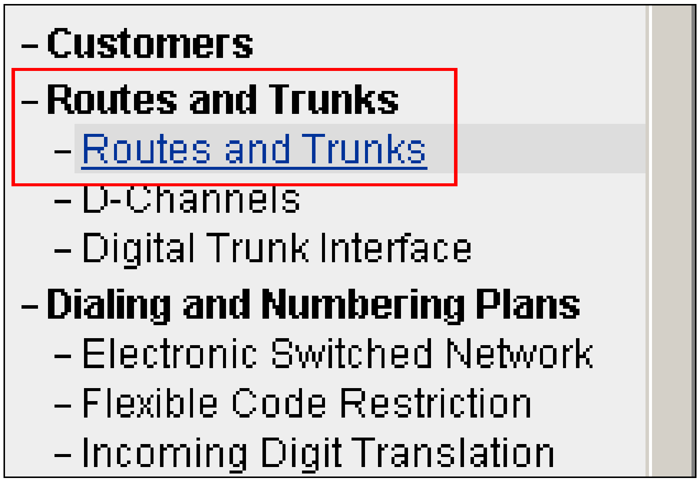
Enable the **Message waiting interworking with DMS-100 (MWI)** and **Network name display method 2 (ND2)** options. Click on **Return - Remote Capabilities** button (not shown) to return back to the main screen.



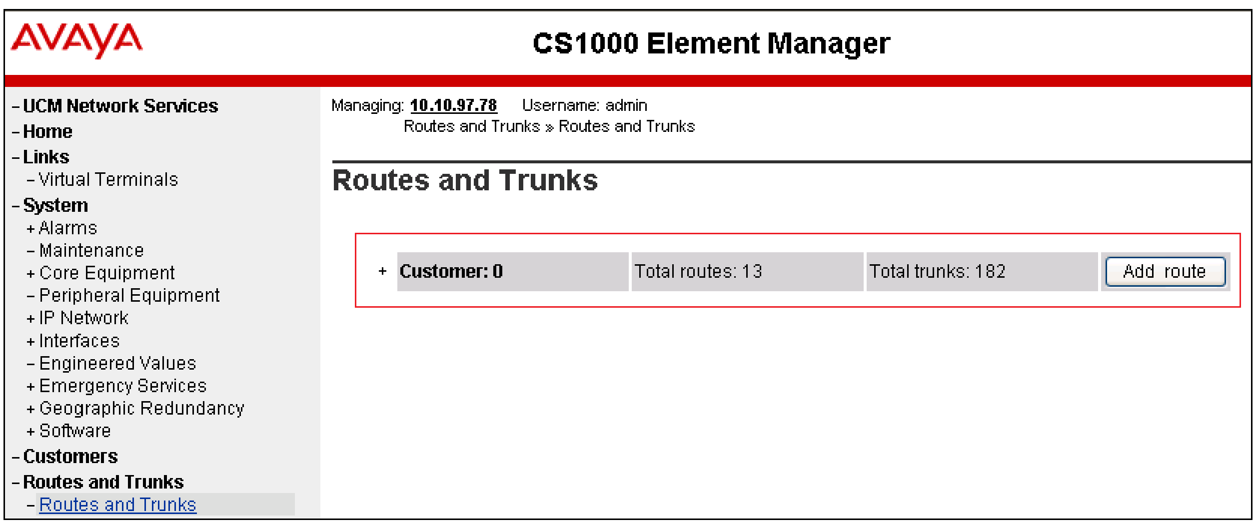
Click on the **Submit** button (not shown) to complete the D-channel configuration.

5.7. Configuring Route and Trunks

This section explains the configuration of the SIP route and trunks which will be used by Communication Server 1000 to communicate with Session Manager. To add a new route, navigate to **Routes and Trunks → Routes and Trunks** from the EM left hand navigator window as shown in screen below.



From the **Routes and Trunks** screen as shown below click on **Add route** button to start configuring a new route.



During compliance testing route 1 was added. The next three screens below shows the configuration for route 1 used during compliance testing.

- **Route data block (RDB) (TYPE)**: *RDB*
- **Customer number (CUST)**: *00*
- **Route number (ROUT)**: *1*
- **Designator field for trunk (DES)**: A descriptive name.
- **Trunk type (TKTP)**: *TIE*
- **Incoming and outgoing trunk (ICOG)**: Select *Incoming and Outgoing (IAO)* from the drop down menu.
- **Access code for the trunk route (ACOD)**: An available Directory number from the system.
- **The route is for a virtual trunk route (VTRK)**: Enable the box.
- **Zone for codec selection and bandwidth management (ZONE)**: A number configured in the system as explained in **Section 5.4**.
- **Node ID of signaling server of this route (NODE)**: *511*; this is the same node added in **Section 5.2**.
- **Protocol ID for the route (PCID)**: Select *SIP (SIP)* from the drop down menu.
- **Integrated services digital network option (ISDN)**: Enable the box.
- **D channel number (DCH)**: *1*; this is the same D channel added in **Section 5.6**.
- **Interface type for route (IFC)**: Select *Meridian M1 (SL1)* from the drop down menu.
- **Private network identifier (PNI)**: A value configured in the system.
- **Call type for outgoing direct dialed TIE route (CTYP)**: Select *Coordinated Dialing Plan (CDP)* from the drop down menu.
- **Calling number dialing plan (CNDP)**: Select *Coordinated dialing plan (CDP)* from the drop down menu.
- **Signaling arrangement (SIGO)**: Select *Standard (STD)* from the drop down menu.
- **Route class (RCLS)**: Select *Route Class marked as external (EXT)* from the drop down menu.

Retain default values for other fields.

Click on the **Submit** button (not shown) to complete the configuration.

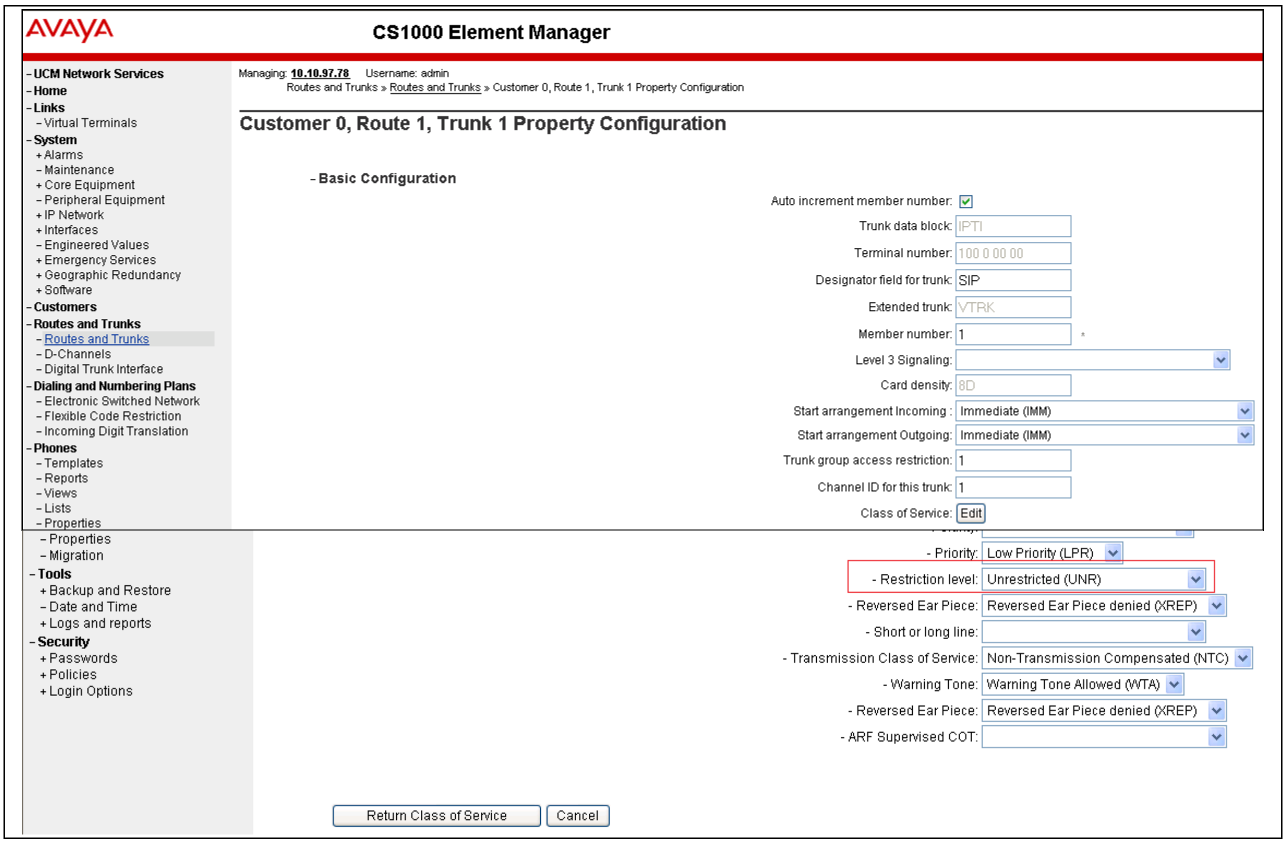

AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
- Tools
+ Backup and Restore
- Date and Time
+ Logs and reports
- Security
+ Passwords
+ Policies
+ Login Options
Managing: 10.10.97.78 Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 1 Property Configuration
Customer 0, Route 1 Property Configuration
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 00
Route number (ROUT) : 1
Designator field for trunk (DES) : SIP
Trunk type (TKTP) : TIE
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 8001 *
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) : 00002 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 511 (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) :
- Enable Shared Bandwidth Management for the route (SBWM) :
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) : 1 (0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 00001 (0 - 32700)
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- - Trunk route optimization (TRO) :
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Coordinated Dialing Plan (CDP)
- Insert ESN access code (INAC) :
- Integrated service access route (ISAR) :
- Display of access prefix on CLID (DAPC) :
- Mobile extension route (MBXR) :
- Mobile extension outgoing type (MBXOT) : National number (NPA)
- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) : Coordinated dialing plan (CDP)
- Network Options
Electronic switched network pad control (ESN) :
Signaling arrangement (SIGO) : Standard (STD)
Route class (RCLS) : Route Class marked as external (EXT)
Off-hook queuing (OHQ) :
Off-hook queue threshold (OHQT) : 0
Call back queuing (CBQ) :
Number of digits (NDIG) : 2
Authcode (AUTH) :

After the route has been configured, trunks can be added that belongs to this route. The two screens below shows the configuration of the trunks that was used during compliance testing.
Auto increment member number: Enable this box.
Trunk data block: *IPTI*
Terminal number: An available terminal number from the system.
Designator field for trunk: A descriptive name.
Extended trunk: *VTRK*
Member number: *1*; this is the starting member number of the trunk.
Start arrangement Incoming: Select *Immediate (IMM)* from the drop down menu.
Start arrangement Outgoing: Select *Immediate (IMM)* from the drop down menu.
Class of Service: Click on the **Edit** button.

- **Restriction level**: Select *Unrestricted (UNR)* from the drop down menu.

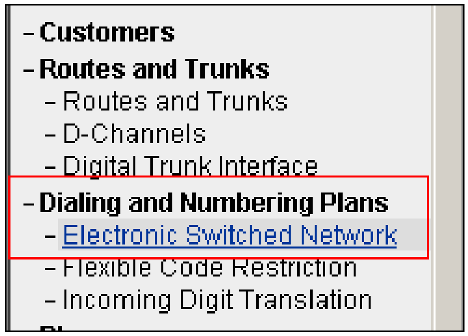
Retain default values for other fields.

Click on **Return Class of Service** button to return to the main page of trunks configuration. Click on **Save** button (not shown) to complete the trunks configuration.

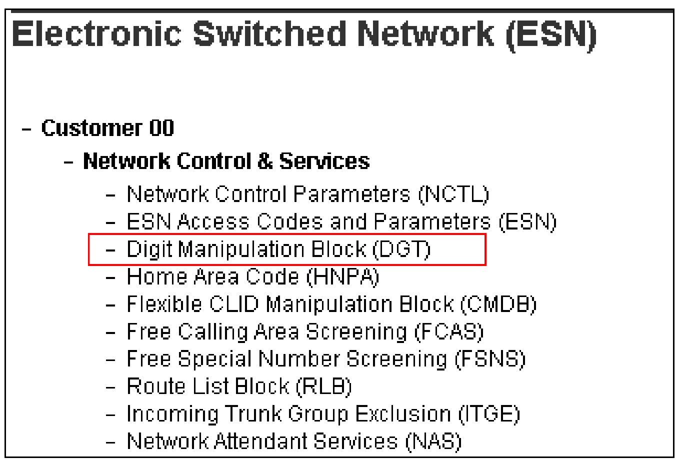


5.8. Configuring Digit Manipulation Block

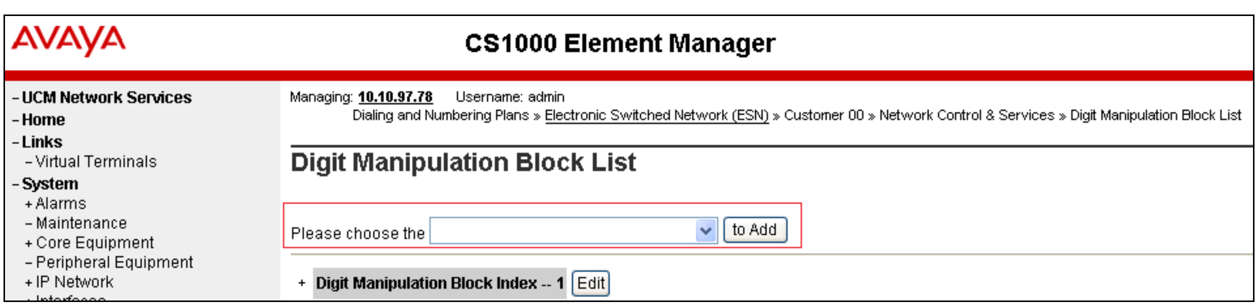
This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown below.



Click on **Digit Manipulation Block (DGT)** option as shown below.

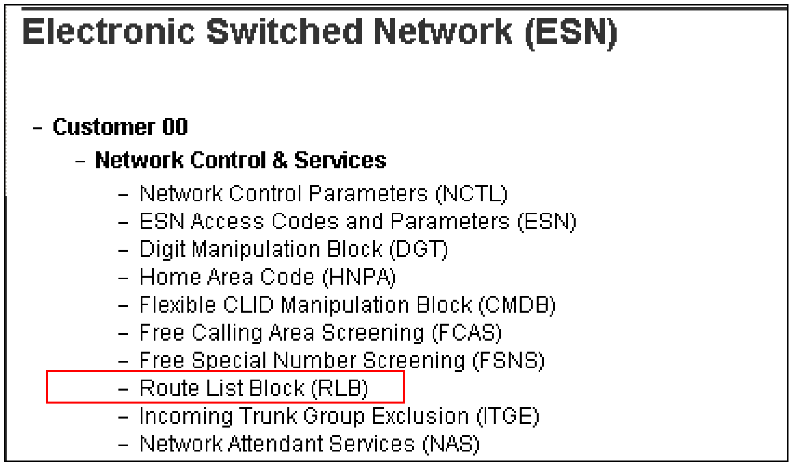


Screen below shows the **Digit Manipulation Block List** page where users can add a digit manipulation block index by selecting an available one from the drop down menu. During compliance testing **Digit Manipulation Block Index -- 0** was used which is already added in the Communication Server 1000 system by default.

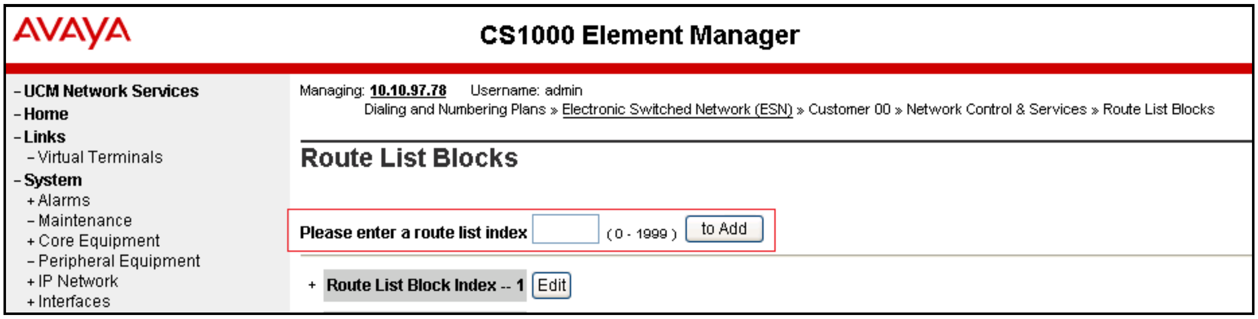


5.9. Configuring Route List Block

This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.8**. Click on **Route List Block (RLB)** option as shown below.

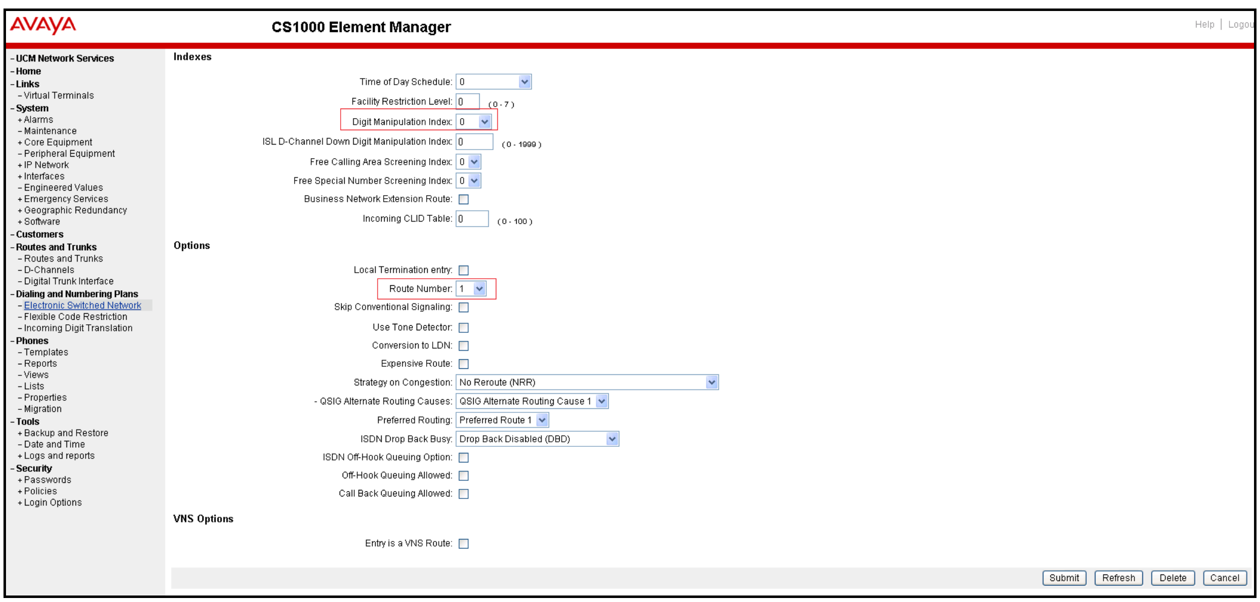


To add a route list index, enter a valid number in the **Please enter a route list index** box and click on **to Add** button as shown in the screen below. During compliance testing a route list block index of 1 was added.



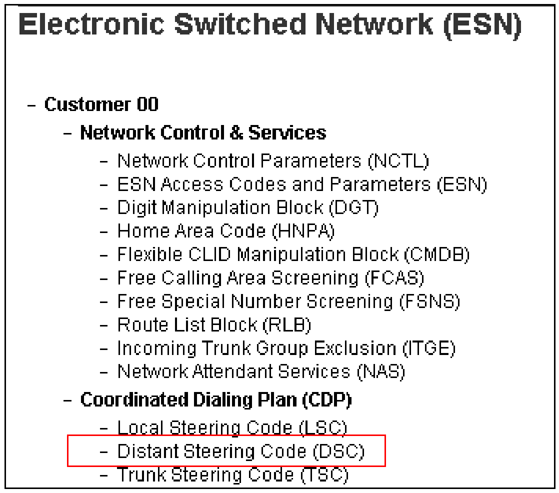
Screen below shows the values configured for the route list index block 1 added during compliance testing.
Digit Manipulation Index: Select *0* from the drop down menu. This was configured in **Section 5.8**.
Route Number: Select *1* from the drop down menu. This was configured in **Section 5.7**.
Retain default values for other fields.

Click on **Submit** to complete the configuration.

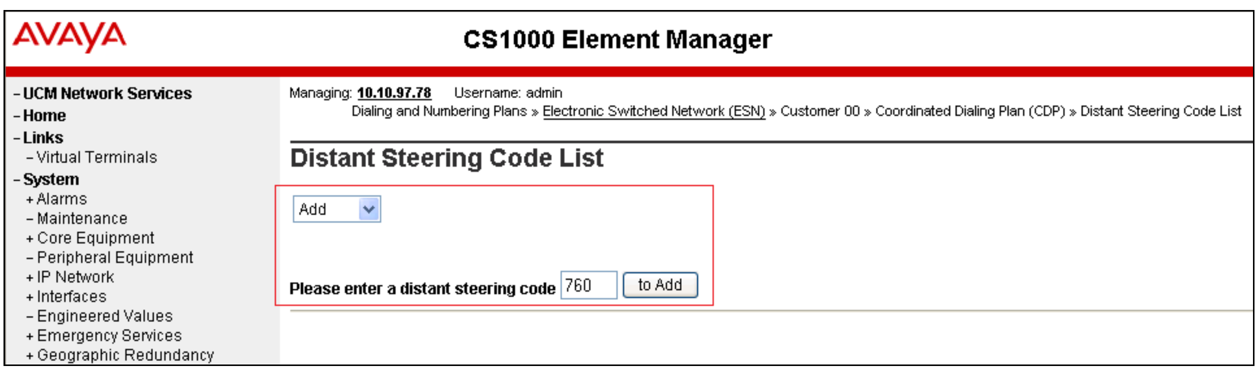


5.10. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.8**. Click on **Distant Steering Code (DSC)** option as shown below.

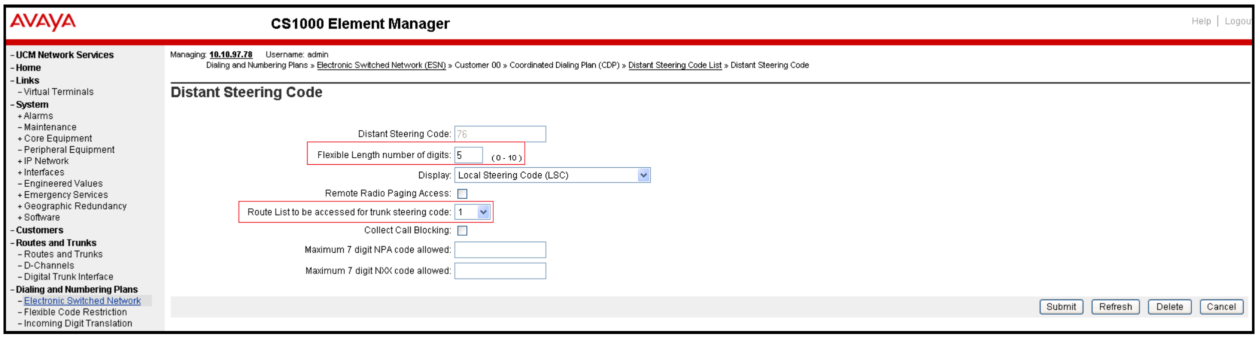


To add a distant steering code, select **Add** from the drop down menu and enter an available distant steering code in the **Please enter a distant steering code** box and click on **to Add** button to finish adding one as shown in the screen below. During compliance testing a code of **760** was added since the pilot number assigned to Infinity was 76000.



Screen below shows the values configured for the distant steering code of 760 added during compliance testing.
Enter the values as shown in screen below.
Flexible Length number of digits: *5*; since 76000 the number to dial Infinity is a 5 digit number.
Route List to be accessed for trunk steering code: Select *1* from the drop down menu. This was configured in **Section 5.9**.
Retain default values for other fields.

Click on **Submit** to complete the configuration.

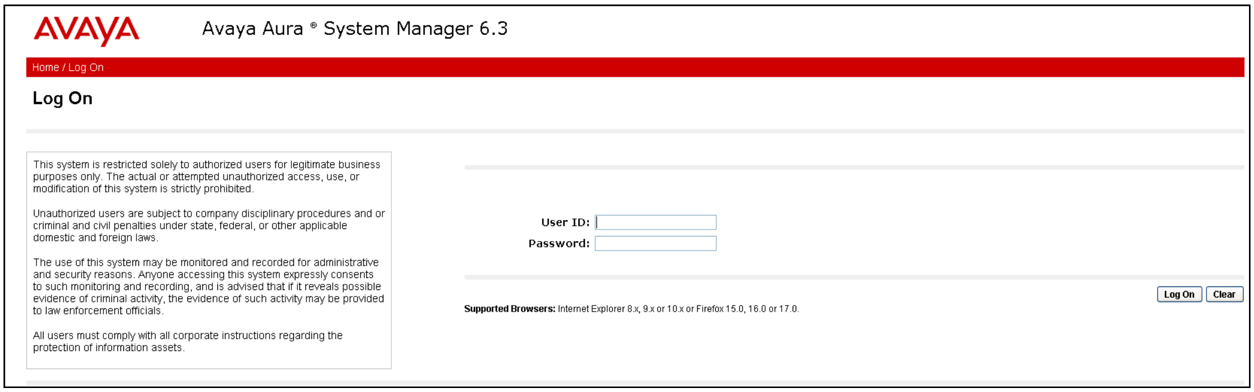


6. Configure Avaya Aura® Session Manager

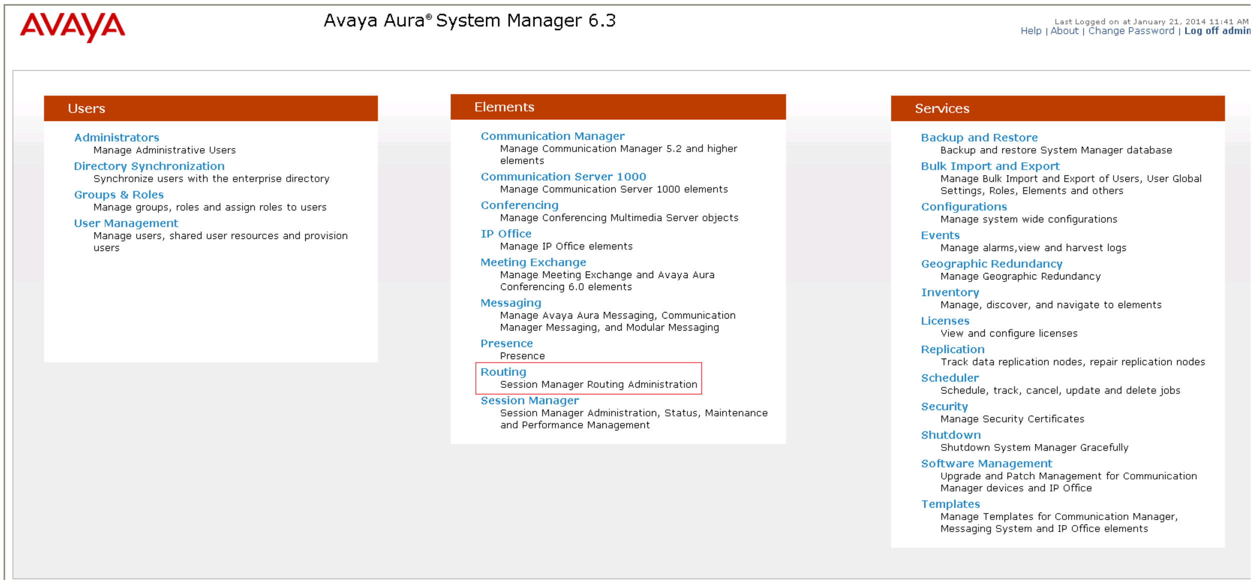
This section provides the procedures for configuring routing using Avaya Aura® System Manager. The procedures include the following areas:

For detail configuration details of Session Manager refer to **Section 10**

Session Manager is administered via Avaya Aura® System Manager Web interface. In a browser, navigate to **https//:<hostname>/** and login with appropriate credentials. Use the hostname or IP Address of the System Manager server in the URL.



All navigation is performed by clicking links in the navigation links on the System Manager landing page as shown in the screen below. Click on the **Routing** link to access Session Manager Routing Administration.



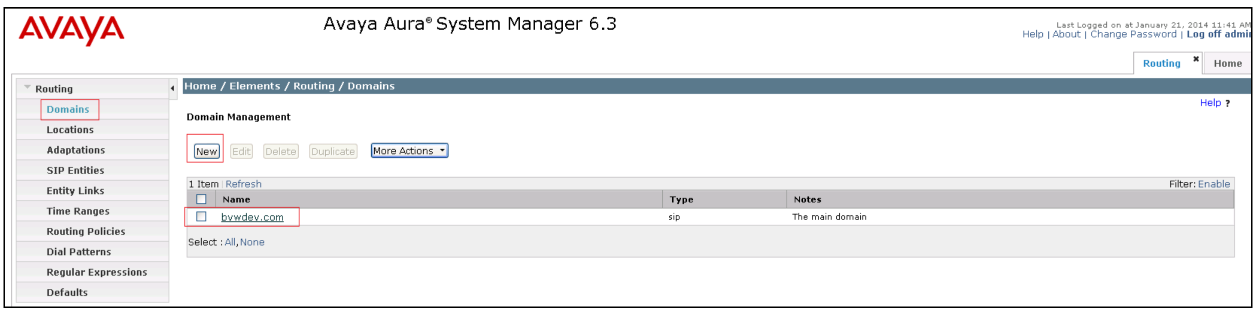
6.1. Configure Session Manager Details

Administration for the solution required the following steps:

- Add a Domain
- Add a Location
- Add a SIP Entity
- Add an Entity Link
- Create a Routing Policy
- Create a Dial Pattern

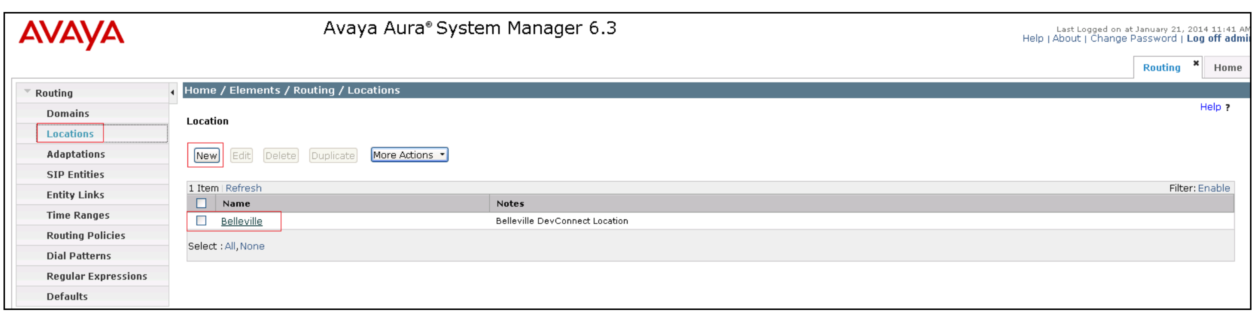
6.1.1. Add a Domain

To add a domain, select **Domains** from the left hand window of the **Routing** screen and click on **New**. Configure a domain name and click on **Commit** (not shown) to complete adding a domain. Screen below shows a domain name of **bvwdev.com** that was added during compliance testing. Additional domains can be added in a similar fashion.



6.1.2. Add a Location

To add a location, select **Locations** from the left hand window of the **Routing** screen and click on **New**. Configure a location name and click on **Commit** (not shown) to complete adding a location. Screen below shows a location name of **Belleville** that was added during compliance testing. Additional locations can be added in a similar fashion.

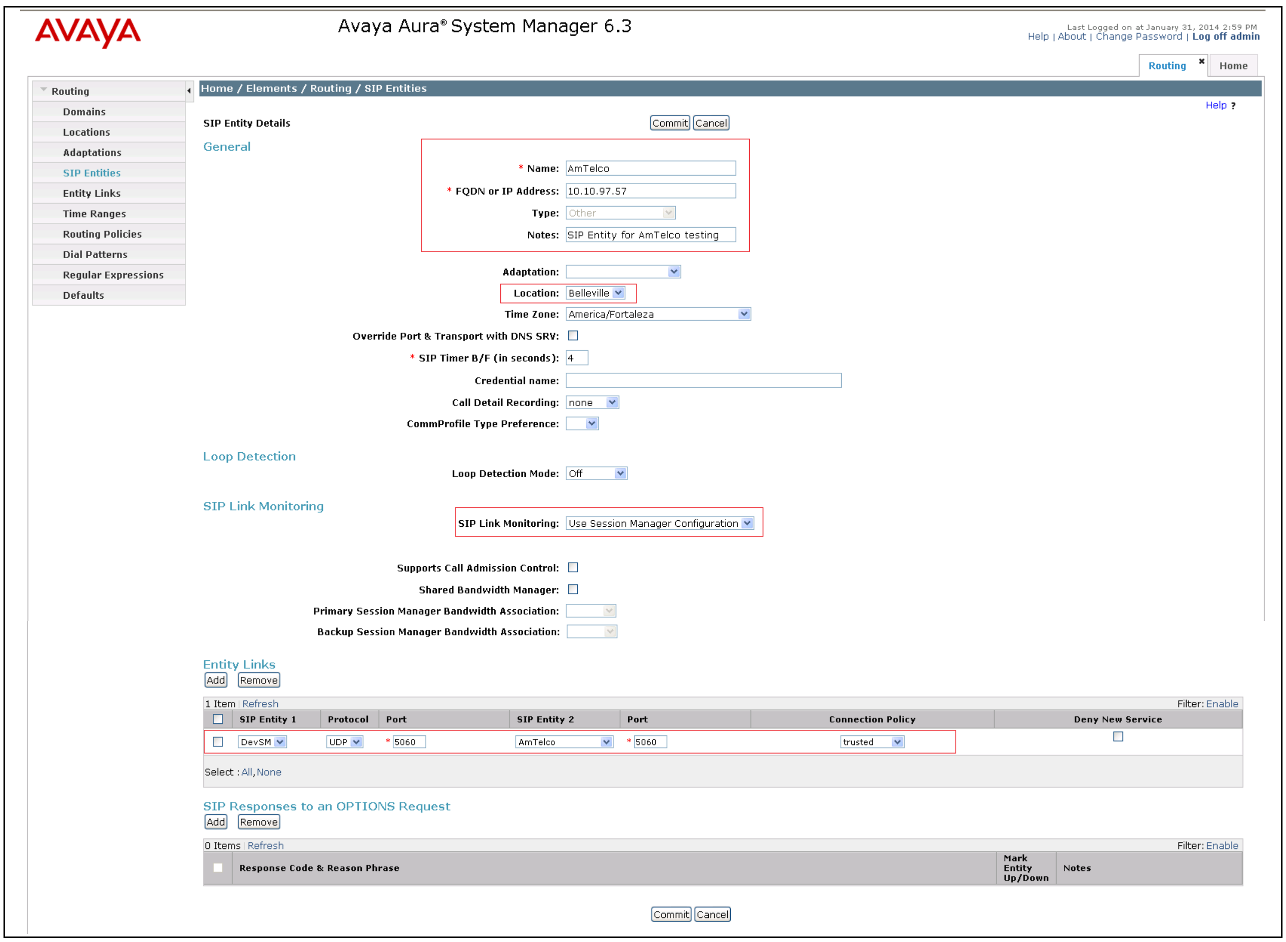


6.1.3. Add a SIP Entity

To add a SIP entity, select **SIP Entities** from the left hand window of the Routing screen and click on **New** (not shown). On the SIP Entity Details screen shown below which appears when the New button is pressed, enter the following values.

Name: Enter a descriptive name for the entity (*AmTelco*).
FQDN or IP Address: *10.10.97.57* was the address used by the Infinity server during compliance testing.
Type: Select *Other* from the drop down menu.
Notes: Useful for quick glance identification on other screens.
Location: Select *Belleville* from the drop down list.
SIP Link Monitoring: Select *Link Monitoring Enabled* from the drop down menu**.** The Infinity Server does support keep-alive messages and therefore we can use link monitoring.
Entity Links: This was added in a subsequent edit to the Entity record using the **Add** button but is described here for brevity purposes**.** See **Section 6.1.4** for how the Entity Link was created.
Retain default values for other fields.

Click **Commit** to complete the entries on this screen.

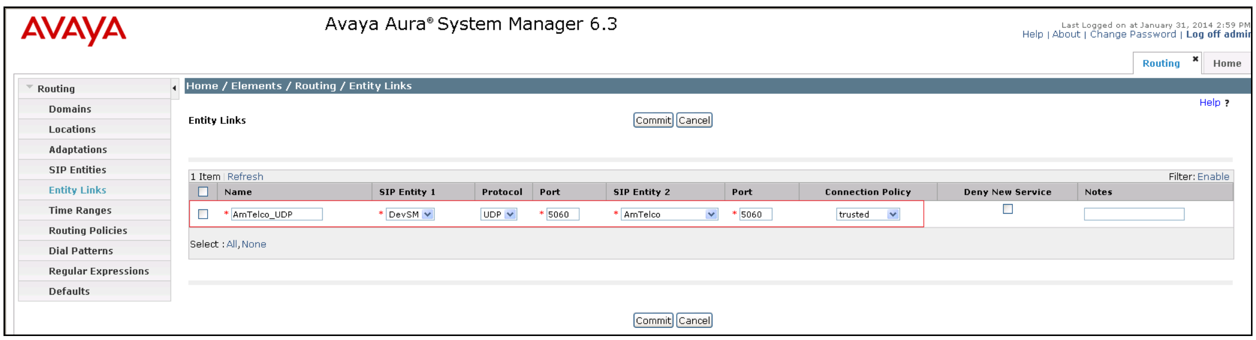


6.1.4. Add Entity Links

To add an Entity Link, select **Entity Links** from the left hand window of the Routing screen and click on **New** (not shown). On the **Entity Links** screen shown below which appears when the New button is pressed, enter the following values.

Name: *AmTelco_UDP* - A Descriptive name for the Entity Link.
SIP Entity 1: Select *DevSM* from the drop down menu **–** This is the existing Session Manager SIP Entity.
SIP Entity 2: Select *AmTelco* from the drop down menu – This is the newly created SIP entity in **Section 6.1.3**.
Protocol: Select *UDP* from the drop down menu**.**
Port: *5060* – Port 5060 is the standard listen port for the UDP SIP transport protocol.
Retain default values for other fields.

Click **Commit** to save the entries.



6.1.5. Create a Routing Policy

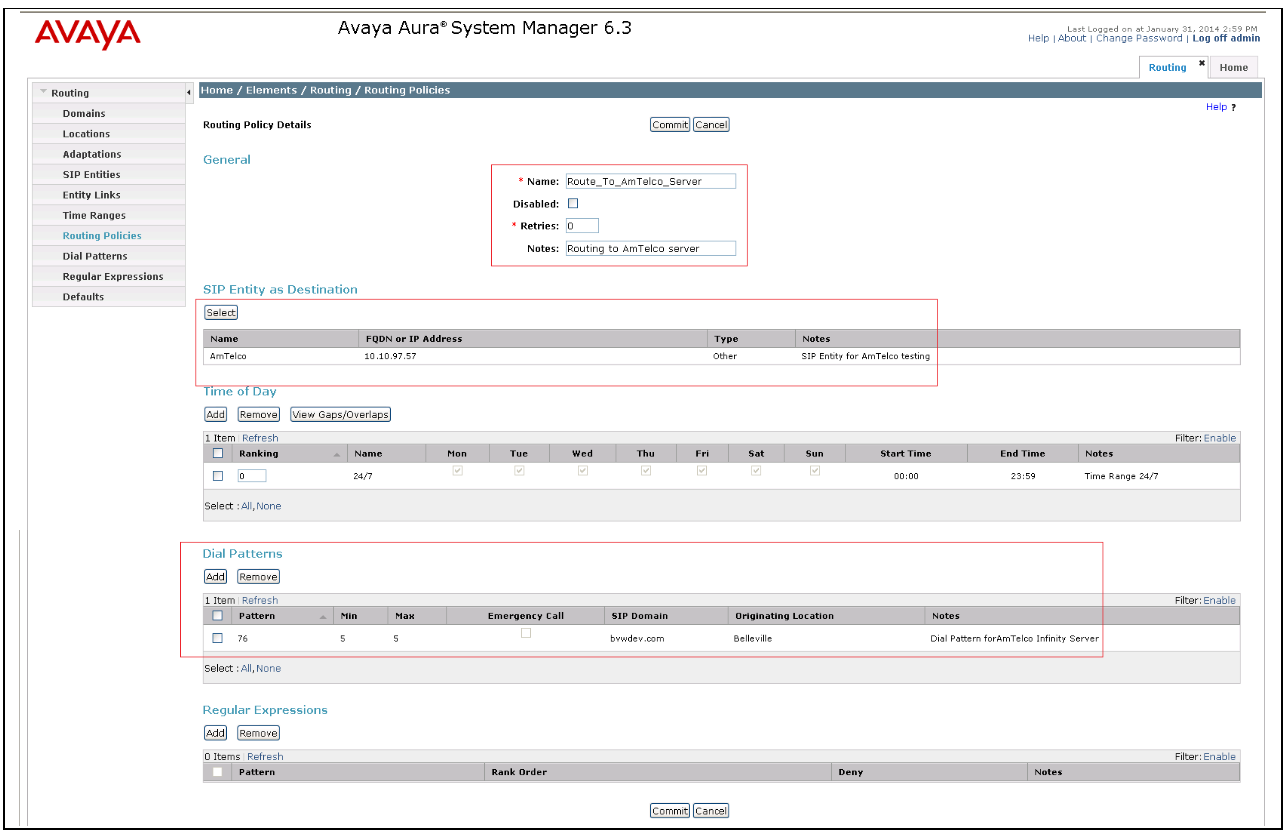
Routing Policies require definition of a Routing Policy, and definition of Dial Patterns. A new Routing Policy is created first, leaving the Dial Pattern undefined, then a Dial Pattern is defined, then the Dial Pattern is applied to the Routing Policy.

To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown). On the **Routing Policy Details** screen shown below which appears when the New button is pressed, enter the following values.

Name and **Notes** as desired for the policy.
Click the **Select** button to select the **SIP Entity as Destination** (not shown). The *AmTelco*SIP Entity was selected as the Destination.
Retain default values for other fields.

Click **Commit** to save the entries.

Note that the **Dial Patterns** shown below was added when the **Dial Pattern** was defined in **Section 6.1.6** but is shown here for brevity.

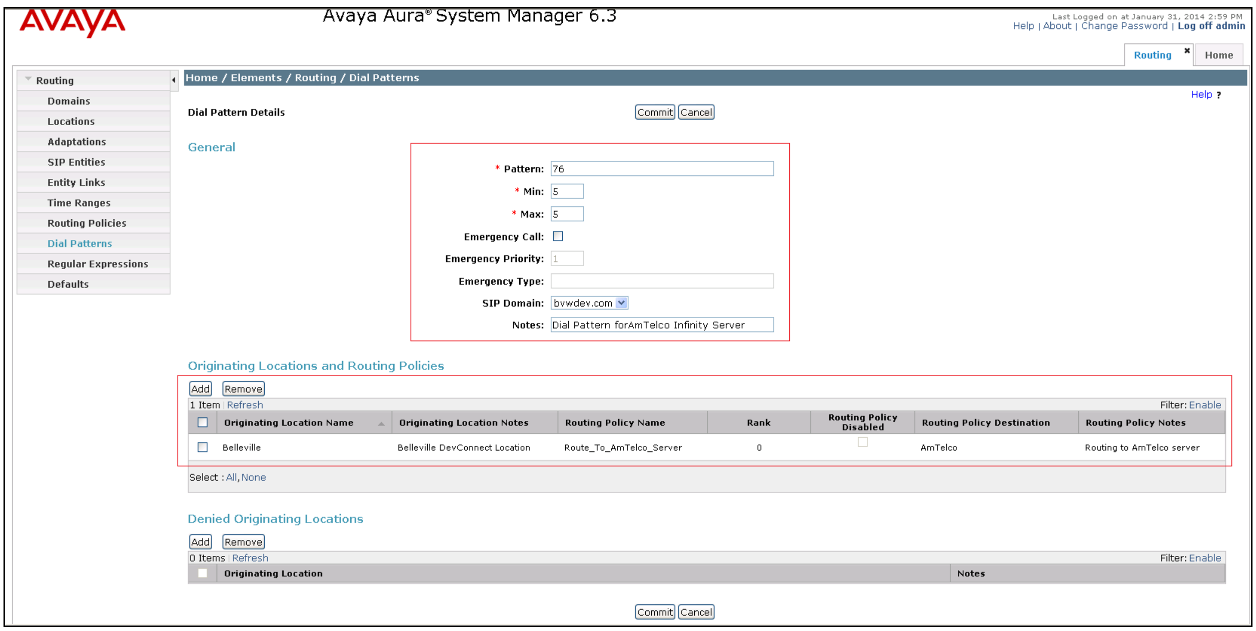


6.1.6. Create Dial Pattern

To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown). On the **Dial Pattern Details** screen shown below which appears when the New button is pressed, enter the following values.

Pattern: *76* – Pilot number to reach the Infinity Server was defined as 76000 during compliance testing.
Min and Max: *5* – The number of digits in the dialed number to match.
SIP Domain: Select *bvwdev.com* from the drop down menu – The SIP Domain was configured in **Section 6.1.1**.
Originating Locations and Routing Policies: See the next page for details of this step.
Retain default values for other fields.

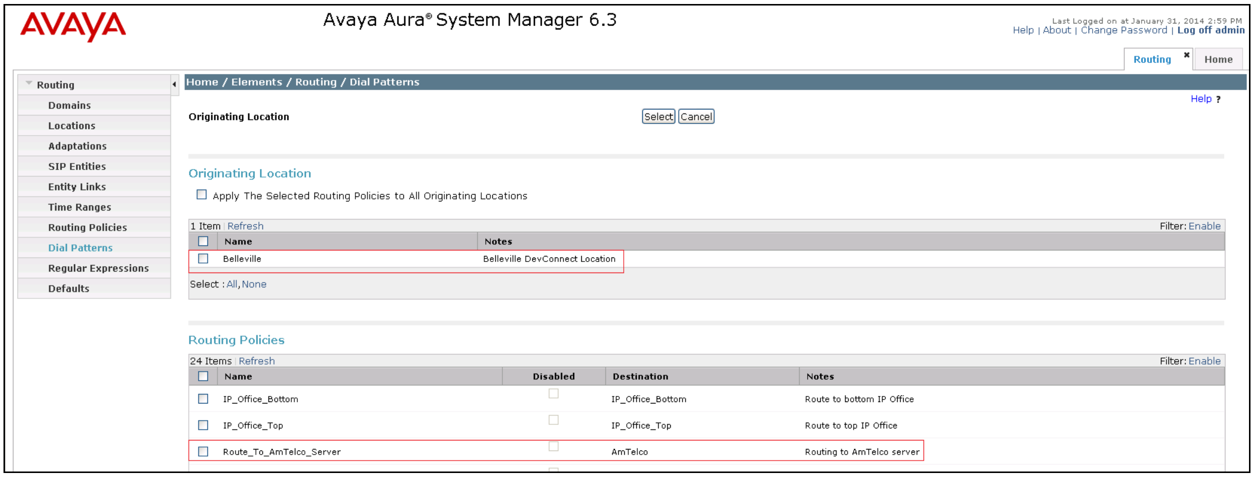
Click on the **Commit** button to save the entries after the step on the following page is completed.



When the **Add** button is clicked on the **Originating Locations and Routing Policies** section for the **Dial Pattern Details** page, the screen shown below will appear.

The **Originating Location** can be defined as any location that originates a SIP request. In the compliance test, the location **Belleville** was used and therefore this option was selected.
The *Route_To_AmTelco_Server* policy defined in **Section 6.1.5** was selected in the **Routing Policies** section.

Click the **Save** button (not shown) to save these changes and return to the **Dial Pattern Details** page.



7. Configure Amtelco Infinity Intelligent SIP Attendant Console

This section provides the procedures for configuring Infinity. The procedures include the following areas:

- Launch Infinity Supervisor
- Administer billing number and board settings
- Administer SIP route
- Administer clients
- Administer system settings

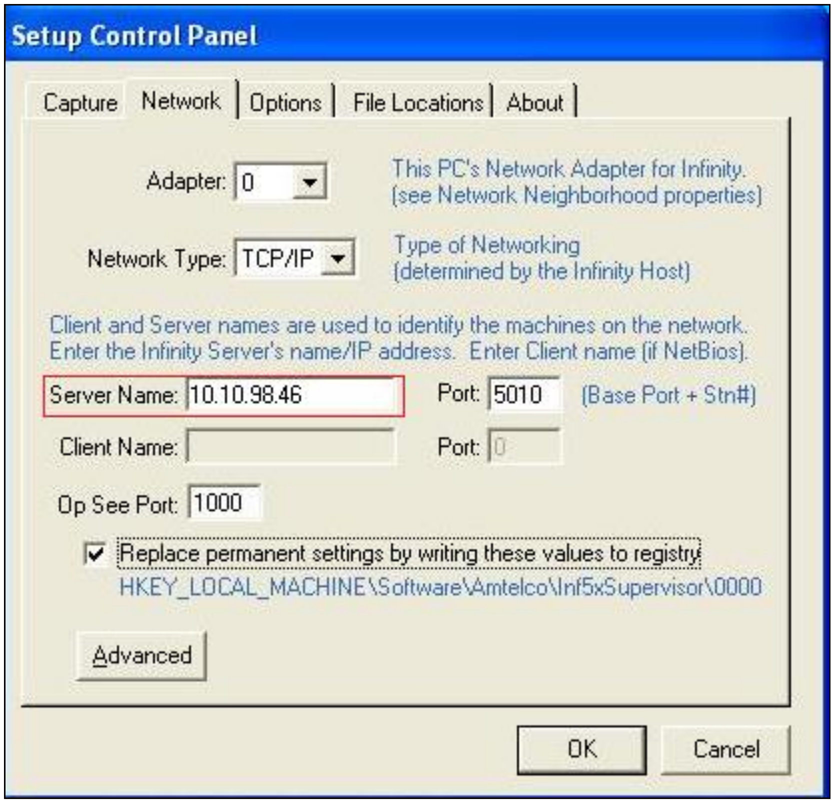
7.1. Launch Infinity Supervisor

From a PC running the Amtelco Infinity Supervisor application, select **Start → All Programs → AMTELCO → Infinity Supervisor** to display the **Infinity Supervisor Login** screen below.

Upon initial log in, prior to entering the credentials, press the **Ctrl** and **F12** key.

The **Setup Control Panel** screen is displayed. For **Server Name**, enter the IP address of the Infinity server that interfaces with attendants (SIP Card), in this case “10.10.98.46”. Retain the default values in the remaining fields. Click on the **OK** button.

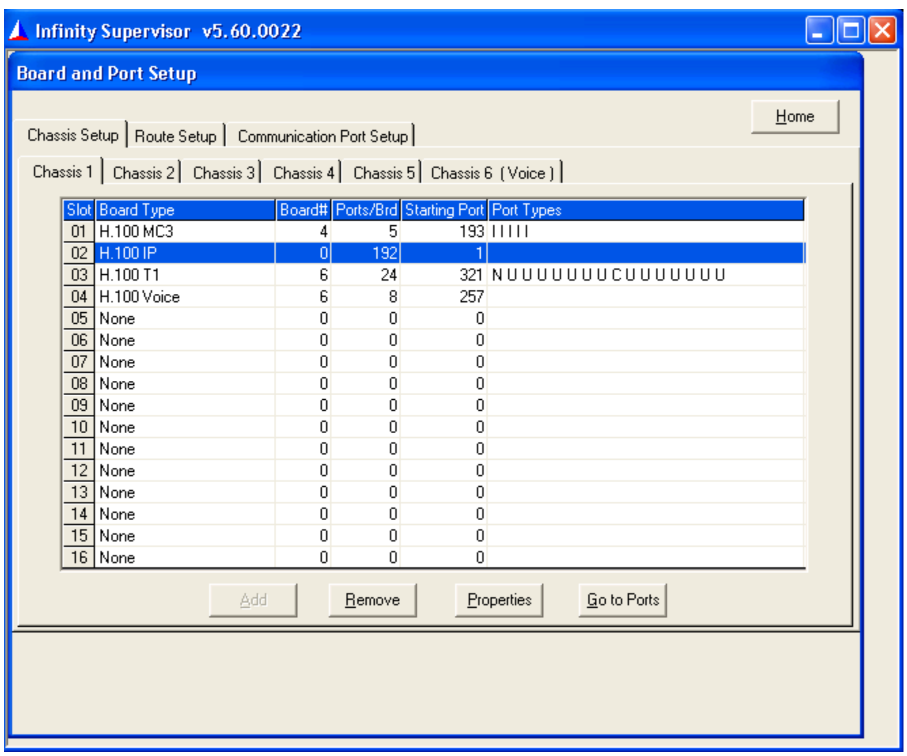
The **Infinity Supervisor Login** screen shown earlier is displayed again. Log in using the appropriate credentials.



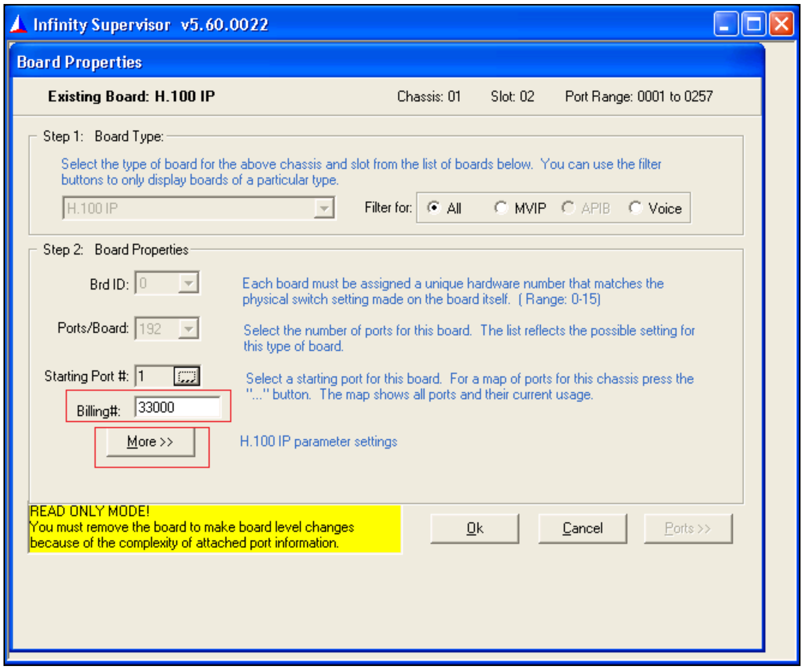
7.2. Administer Billing Number and Board Settings

The **Infinity Supervisor** screen is displayed next. Select **BOARDS and PORTS**.

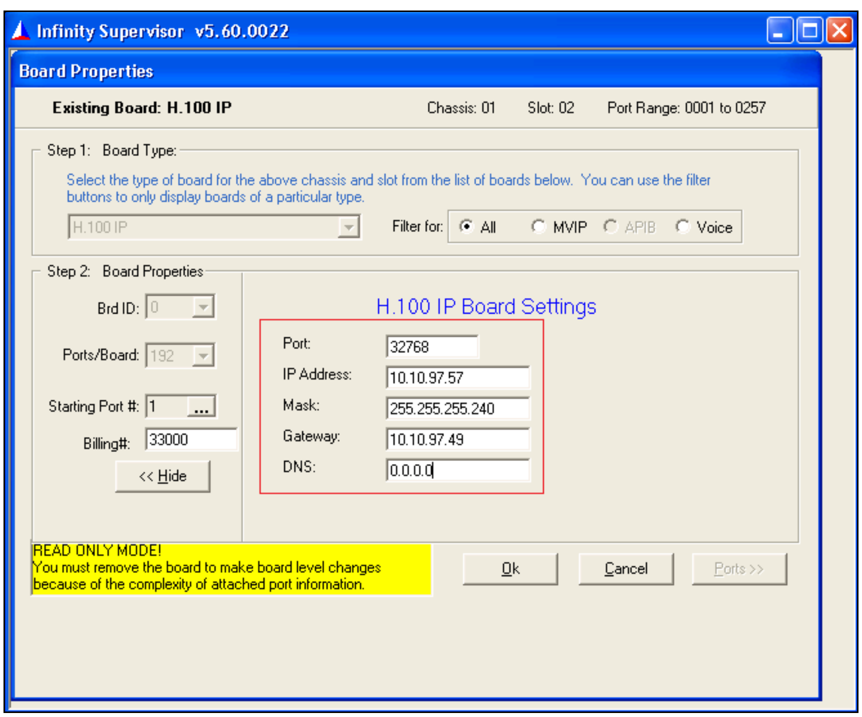
The **Board and Port Setup** screen pops up. Select the **H.100 IP** entry, and click **Properties**.



The **Board Properties** screen pops up next. For **Billing#,** enter the applicable number to use for outbound calls for billing purposes, and click **More**.



The **Board Properties** screen is updated with the **H.100 IP Board Settings** sub-section. For **Port**, enter "32768". Enter the pertinent network information (Server IP Address) for the remaining fields.

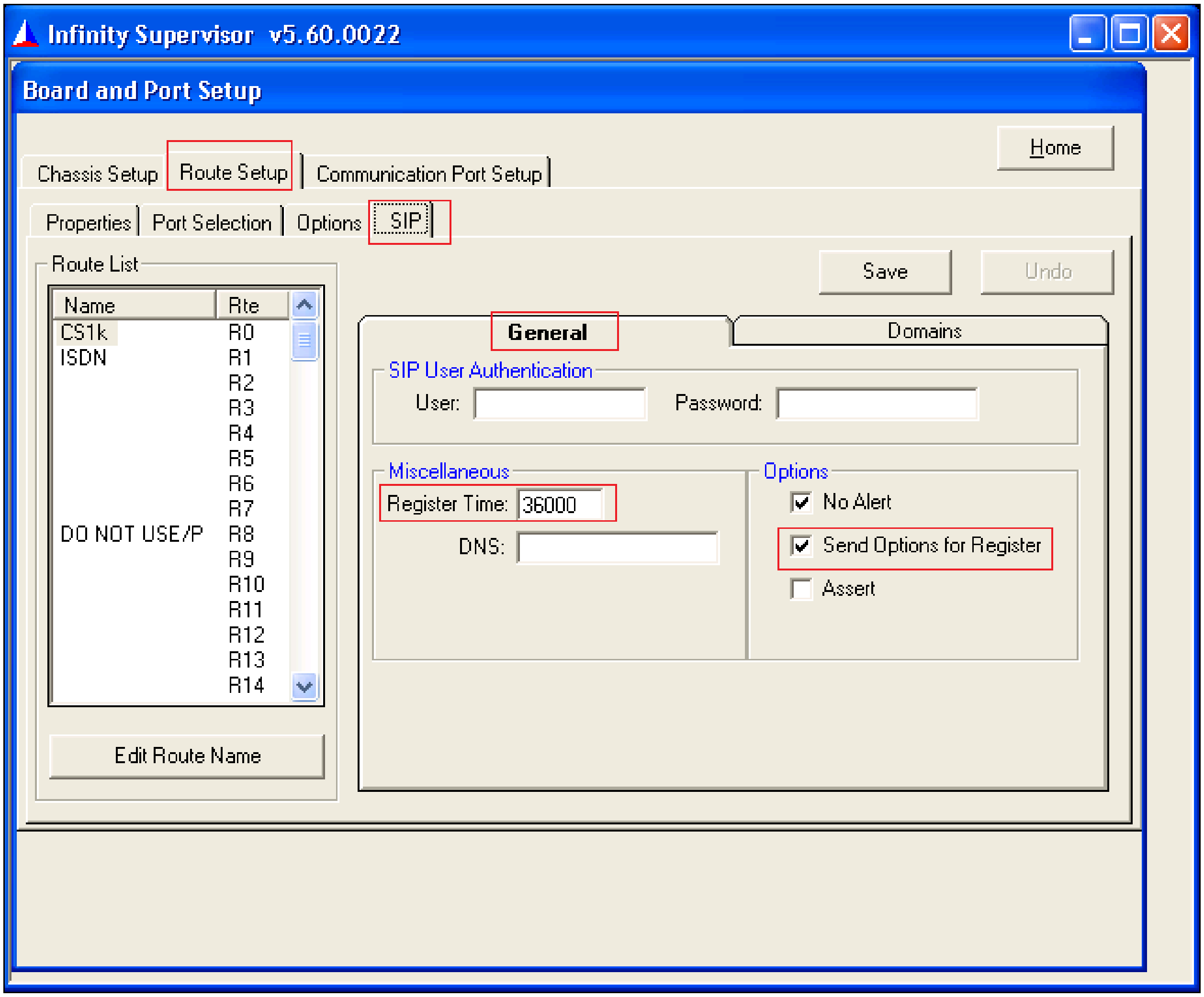


7.3. Administer SIP Route

The **Board and Port Setup** screen is displayed next. Select the **Route Setup → SIP** tab, followed by the **General** sub-tab.

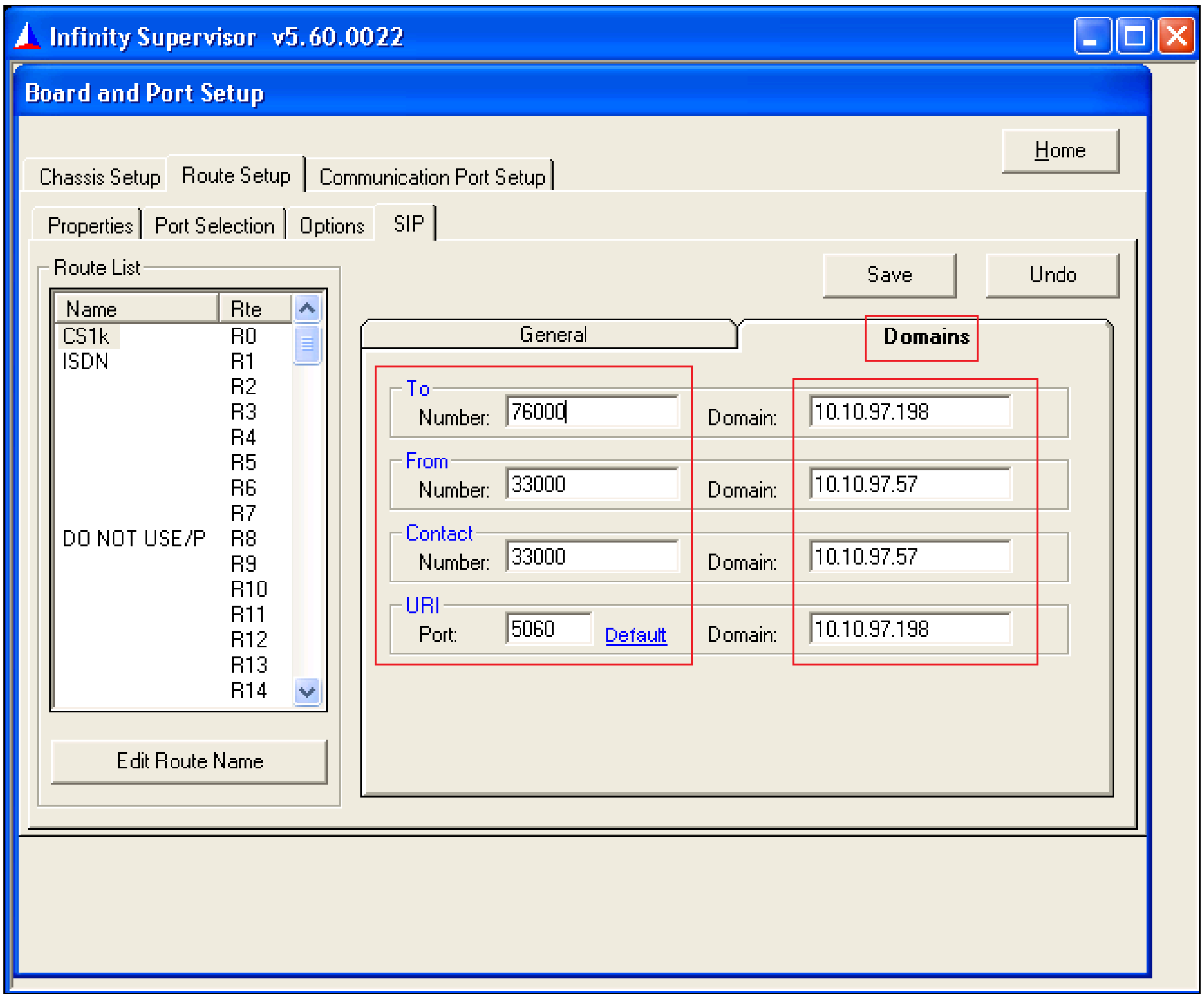
Under **Options**, check **Send Options for Register**.

For **Register Time**, enter a desired interval for the Options message. Retain default values for other fields.



Select the **Domains** sub-tab. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click on the **Save** button.

- **To Number:** 76000
- **To Domain:** IP address of Session Manager signaling interface.
- **From Number:** 33000
- **From Domain:** IP address of the IP board from **Section 7.2**.
- **Contact Number:** 33000
- **Contact Domain:** IP address of the IP board from **Section 7.2**.
- **URI Port:** Infinity SIP entity port number from **Section** Error! Reference source not found..
- **URI Domain:** IP address of Session Manager signaling interface.



7.4. Administer Clients

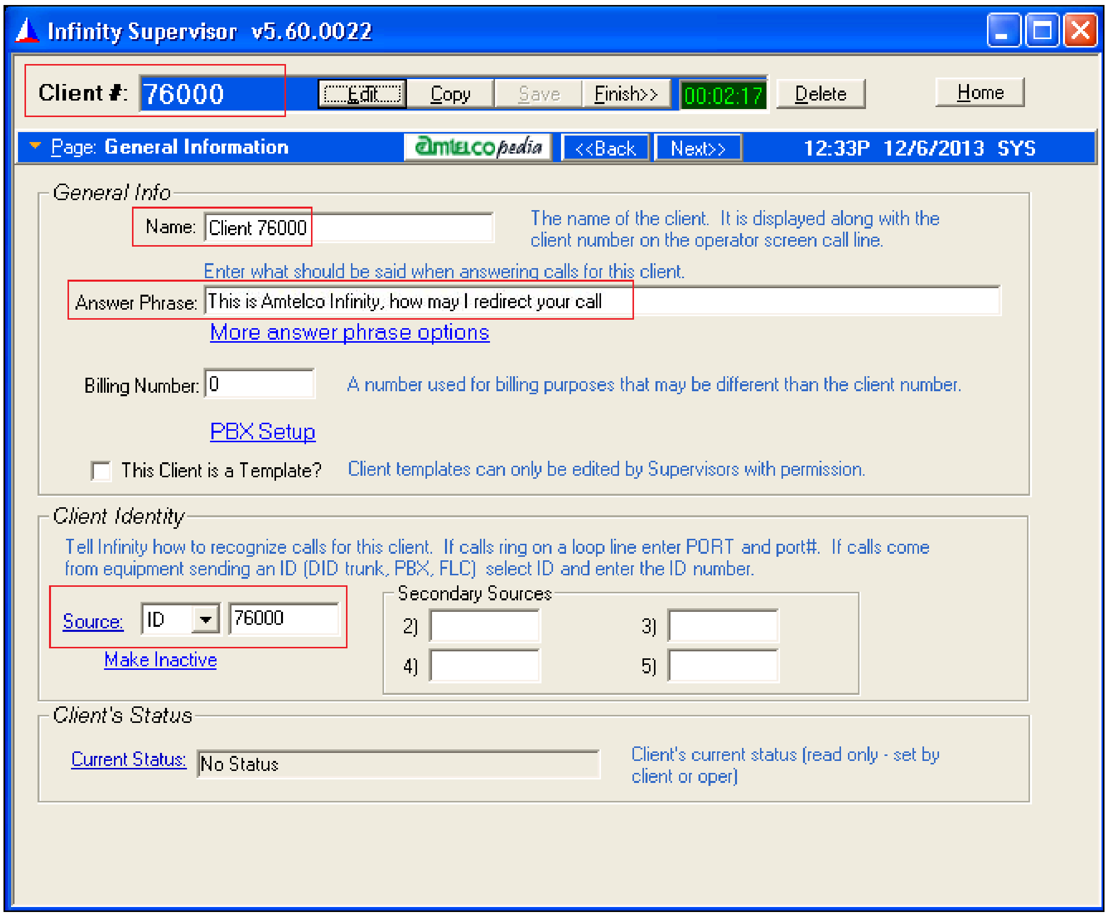
From the **Infinity Supervisor** screen shown below, select **CLIENT**.

Enter an available client number, in this case “76000” and click on **Edit** to configure the values. If there is no available client then a **Client not found** pop-up window appears (not shown) asking user to confirm adding a new client, click on the **Yes** button to confirm.

The screen is updated as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** Name to display to the attendant when answering calls to this client.
- **Answer Phrase:** Guidance phrase for what to say when answering calls to this client.
- **Source ID:** The phone number identification for this client.

Repeat this section to administer all needed clients. In this compliance testing, calls from the PSTN will be routed with digits 76000 to Infinity.



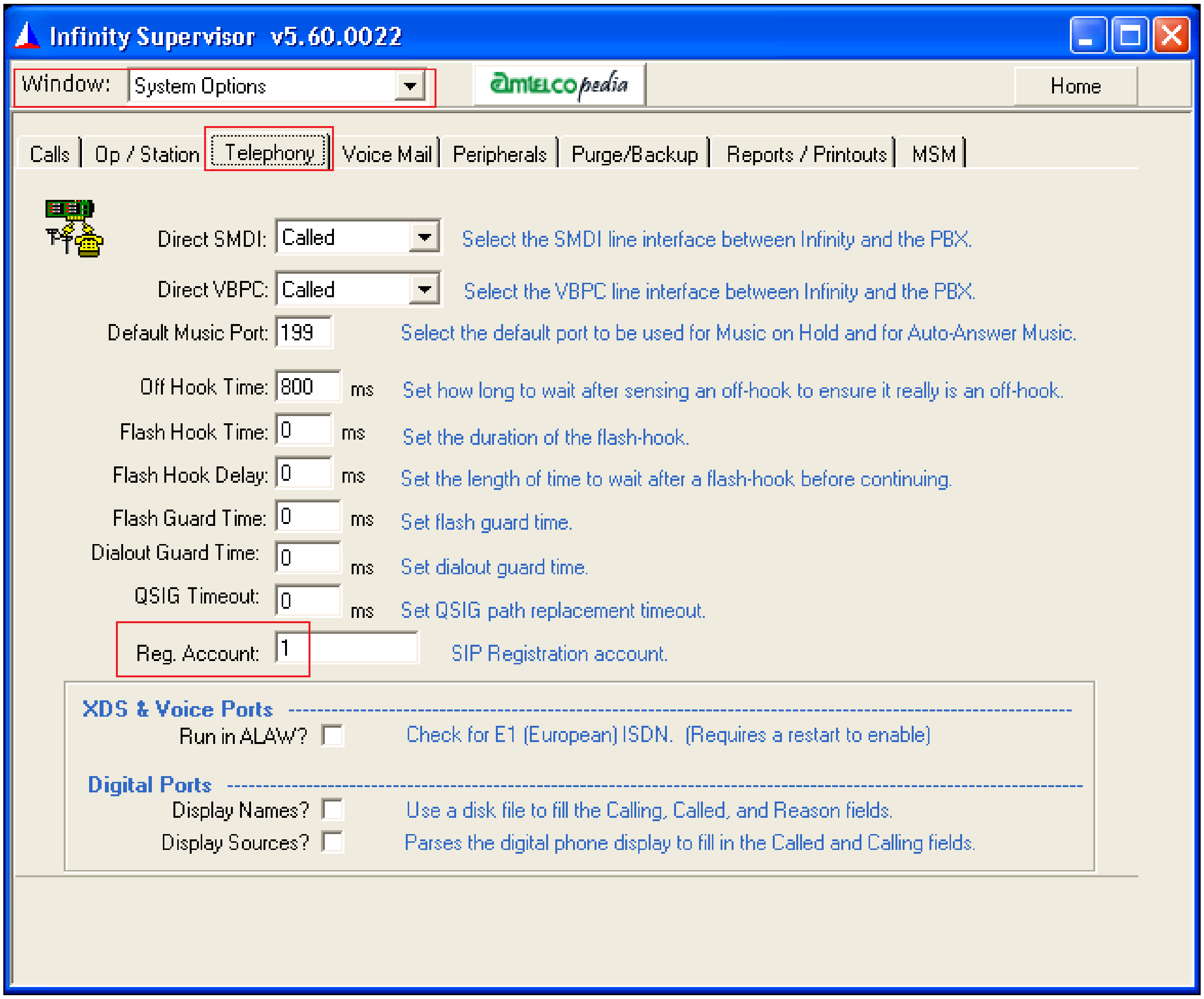
7.5. Administer System Settings

From the **Infinity Supervisor** screen shown below, select **SYSTEM SETTINGS**.

The screen below is displayed. For **Window**, select **System Options** from the drop-down list.

Select the **Telephony** tab, and enter a valid account number for **Reg. Account**.

Reboot the Infinity server.



8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Infinity.

8.1. Verify Avaya Communication Server 1000

On Communication Server 1000, verify the status of the DCH by the **stat dch** command. Verify that the DCH is in **OPER EST** and **ACTV** status as shown below.

```
.stat dch
DCH 001 : OPER          EST    ACTV   AUTO          DES : SIP
```

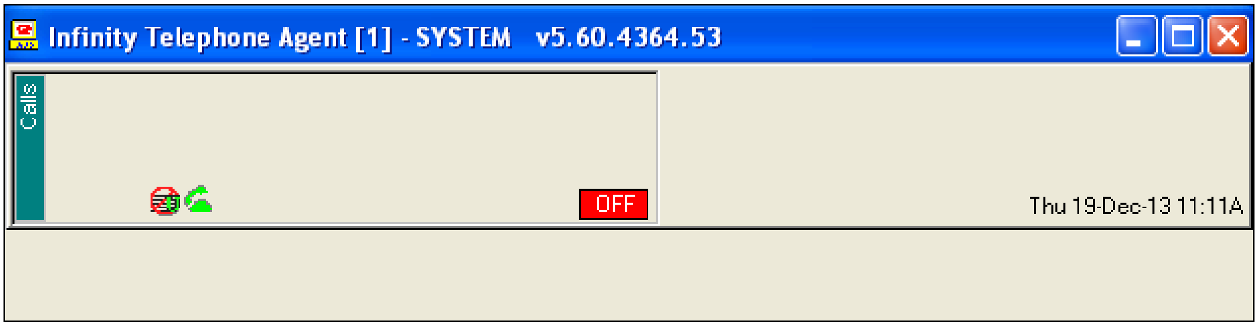
8.2. Verify Avaya Aura® Session Manager

Navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** and select the Communication Server 1000 SIP Entity (not shown). Verify the **Link Status** is ***Up***. Repeat the procedure above selecting the AmTelco Infinity server SIP Entity (not shown), and verify the **Link Status** is ***Up***.

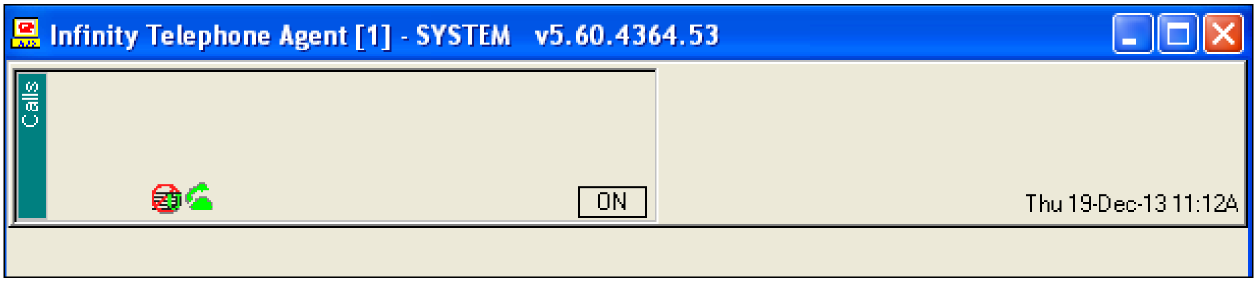
8.3. Verify Infinity Intelligent SIP Attendant Console

From an attendant PC running the Amtelco Infinity Telephone Agent application, select **Start** → **All Programs** → **AMTELCO** → **Infinity Telephone Agent** to display the **Infinity Telephone Agent** screen below. Log in using the appropriate credentials.

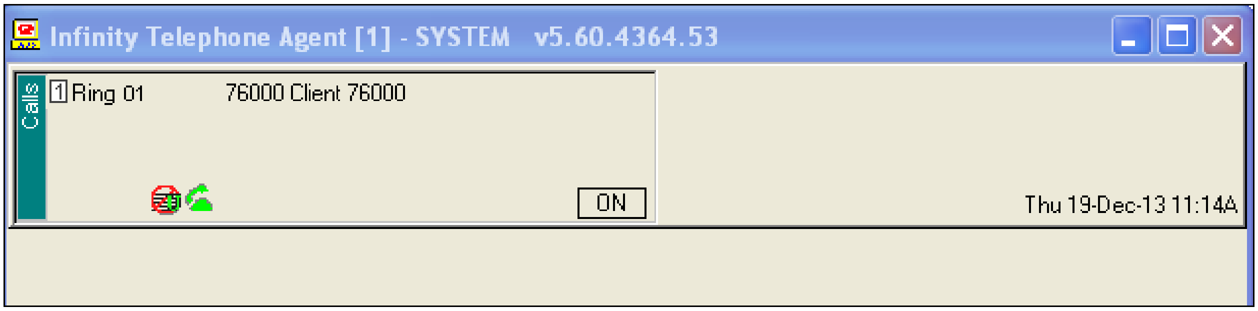
The screen below is displayed next. Click **OFF** to toggle into available.



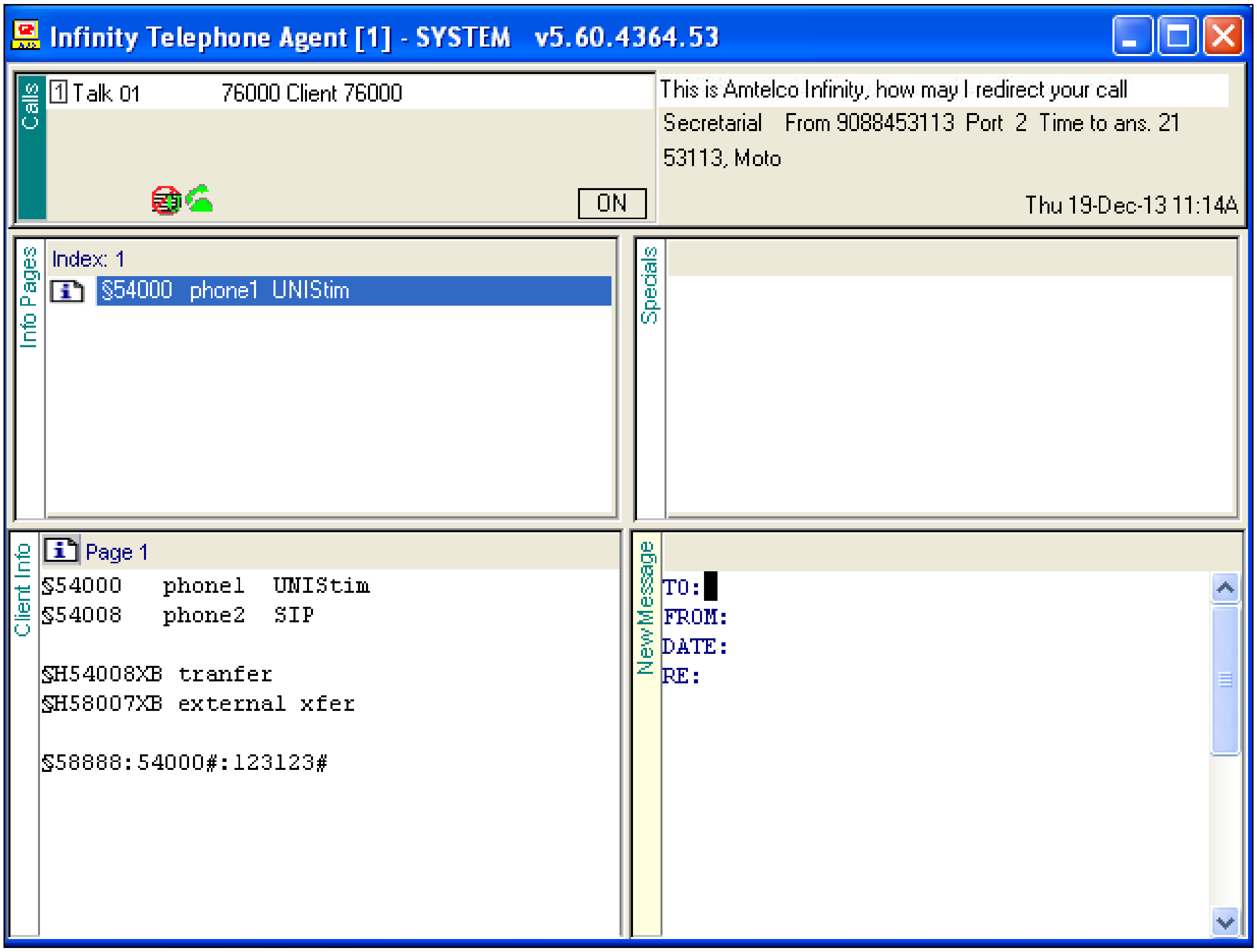
Verify the status is updated to **ON**, as shown below.



Make an incoming call from the PSTN to reach Infinity. Verify that an available attendant hears the alerting tone, and that the attendant screen is updated showing the alerting call. Also verify that the display information reflects the proper client ID and name from **Section 7.4**.



Press **F1** to answer the call. Verify that the attendant is connected to the PSTN with two-way talk paths, and that the screen is updated with the proper guidance phrase from **Section 7.4**.



9. Conclusion

These Application Notes describe the configuration steps required for Amtelco Infinity Intelligent SIP Attendant Console to successfully interoperate with Avaya Aura® Session Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

Avaya
Communication Server 1000E Installation and Commissioning, March 2013, Release 7.6, NN46041-310
Element Manager System Reference – Administration - Avaya Communication Server 1000, March 2013, Release 7.6, NN43001-632.
Co-resident Call Server and Signaling Server Fundamentals - Avaya Communication Sever 1000, March 2013, Release 7.6, NN43001-509.
Unified Communications Management Common Services Fundamentals - Avaya Communication Server 1000, March 2013, Release 7.6, NN43001-116.
Administering Avaya Aura® System Manager, October 2013, Release 6.3.
ISDN Primary Rate Interface Installation and Commissioning - Avaya Communication Server 1000, March 2013, Release 7.6, NN43001-301.
Administering Avaya Aura® Session Manager, October 2013, Release 6.3, Document Number 03-603324.

Amtelco
Product information for Amtelco Infinity can be found at http://www.amtelco.com/.

Infinity Supervisor Reference Guide, Version 232M072, November 2012, available at http://service.amtelco.com.

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.