Avaya Solution & Interoperability Test Lab

Application Notes for configuring IPC Unigy with Avaya Communication Server 1000 7.5 and Avaya Aura® Session Manager 6.1 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Communication Server 1000 via Avaya Aura® Session Manager, for turret users on IPC to reach users on Avaya Communication Server 1000 and on the PSTN.

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 IPC Unigy to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

IPC Unigy (hereafter referred to as Unigy) is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Communication Server 1000 7.5 (hereafter referred to as CS1000) via Avaya Aura® Session Manager, for turret users on IPC Unigy to reach users on Avaya Communication Server 1000 and on the PSTN.

This solution covered CS1000 IP (UNIStim), Digital and/or PSTN users. SIP endpoints are currently not supported due to an issue with blind transfer.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among Unigy turret users with CS1000 IP (UNIStim), Digital and/or PSTN users. Call controls were performed from various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the network connection to Unigy.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic calls, basic display, G.711, G.729, DTMF, hold/reconnect, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and attended conference.

The serviceability testing focused on verifying the ability of Unigy to recover from adverse conditions, such as disconnecting/reconnecting the network connection to Unigy.

2.2. Test Results

The objectives outlined in S**ection 2.1** were verified and met. All tests were executed and passed with the following observations.

- Blind transfer of a call from Unigy to an Avaya SIP endpoint fails. For example, Set A (Avaya) calls Set B (Unigy). Set B does a blind transfer to Set C (Avaya SIP end point). When Set C answers the call, Set A gets disconnected. Issue is not seen if Set C is a non SIP endpoint.
- Set A (Unigy) calls Set B (Avaya) with name and number restricted. Set B does an unattended transfer to Set C (Unigy). Set C sees the Calling Line Identification (CLID) of Set B rather than Set A. This is because Avaya CS1000 design does not support CLID update while doing a transfer to a third party system.
- Set A (Avaya) calls Set B (Unigy) which is setup so that all calls forward to Set C (Avaya) which is setup so that all calls forward to a voice mail system. Set A is leaving a

voice mail to Set B mailbox and not to the mailbox for Set C. This is the CS1000 design intent since original call from Set A was made to Set B.

- Set A (Avaya) calls Set B (Unigy) which has calls forward if busy to Set C's (Avaya) voice mail. Set A hears the voice mail greeting right away with no ringing indication.
- Set A (Unigy) calls Set B (Unigy) which has calls forward if busy to an invalid extension on Avaya CS1000. As per design call fails however the line on Set A freezes and has to be force cleared. Unigy design is investigating this issue.
- Set A (Unigy) calls Set B (Avaya) which has calls forward on no answer to Set C (Unigy) which has all calls forward to a PSTN number. Even though Unigy documentation claims to use the UDP protocol only, during diversions like the example mentioned above, it changes the protocol to TCP. Therefore, for calls to be successful, Avaya Aura® Session Manager needs to be configured for both UDP and TCP protocols when integrating with the Unigy system. Details of the configuration are explained in **Section 6**.
- Set A (Unigy) calls Set B (Unigy). Set B does a blind transfer to Set C (Unigy) which has calls forward on no answer to a voice mail system. The call between Set A and the voice mail system is active however there is no speech path and Set A cannot hear any mail box greetings or commands. Issue has been raised with Avaya CS1000 design.
- Uncheck PRACK in Unigy system so that Unigy users can access the Avaya Call Pilot voice mail system that is hosted on the Avaya CS1000 system.
- G.722 codec is not supported and therefore should not be configured on Unigy.
- A packet rate of 20ms is to be used with G.711 and G.729 codecs.

2.3. Support

Technical support on IPC Unigy can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in **Figure 1** below, the Unigy configuration consists of the Media Manager, Converged Communication Manager, and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

Unigy, CS1000 and Avaya Aura® Session Manager are connected to each other through the lab network. SIP trunks are used from Unigy to Avaya CS1000 via the Avaya Aura® Session Manager, to reach users on CS1000 and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between Unigy and CS1000. During compliance testing, extension ranges 58xxx were associated with CS1000 users and 35xxx were associated with the Unigy turret users. Avaya Call Pilot DN is 58888 and the PSTN number is 96139655570.

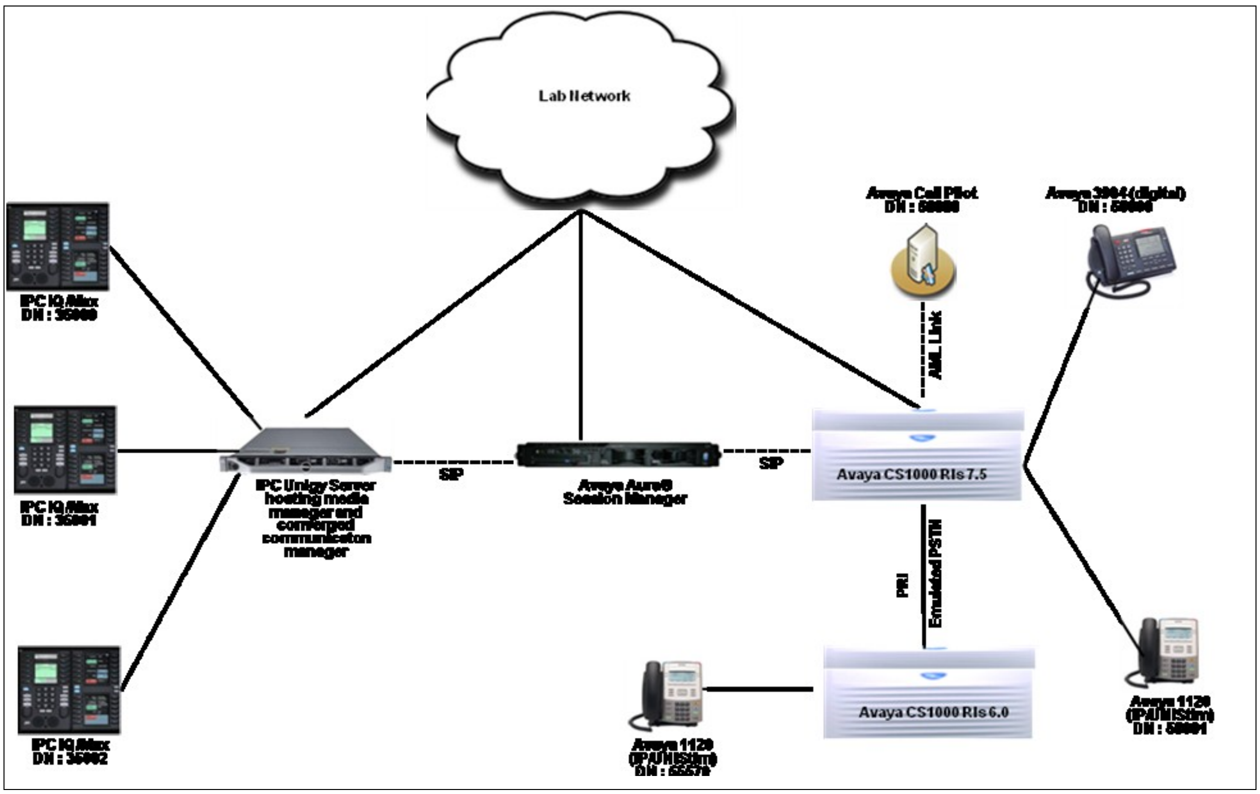

Figure 1: Compliance Test Setup in the lab

4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000	7.50.17
Avaya Communication Server 1000 (for emulated PSTN)	6.0
Avaya Call Pilot (600r)	5.00.41
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya Digital user (3904)	NA
Avaya IP (UNIStim) user (1120)	0624C8A
IPC Unigy • Media Manager • Converged Communication Manager • Turrets (IQ/Max)	 01.00.00.04.0003 01.00.00.04.0003 01.00.00.04.0003

5. Configure Avaya CS1000

This section provides the procedures for configuring the Avaya CS1000 system. The procedures include the following areas:

- Logging into the Element Manager via Unified Communications Manager.
- Configuring the SIP Signaling Gateway.
- Configuring a D-Channel.
- Configuring Routes and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Distant Steering Code.

Assumption is made here that the CS1000 users are already created and also the PRI Trunk between CS1000 7.5 and CS1000 6.0 is configured for emulated PSTN setup during compliance testing. For configuration details of the CS1000 refer to **Section 10[1]**.

5.1. Logging into Element Manager via Unified Communication Manager

To login to the Unified Communications Manager (UCM) open an IE browser and type in the IP address of the UCM in the URL (not shown). **Figure 2** below shows the login screen of the UCM. Enter the **User ID** and **Password** credentials and click on **Log In** to continue.

Figure 2: UCM Login Screen

From the UCM main screen as shown in **Figure 3** below, click on the Element **EM on cppm1**. This is the element which is configured to access the Element Manager (EM) for the CS1000 Call Server.

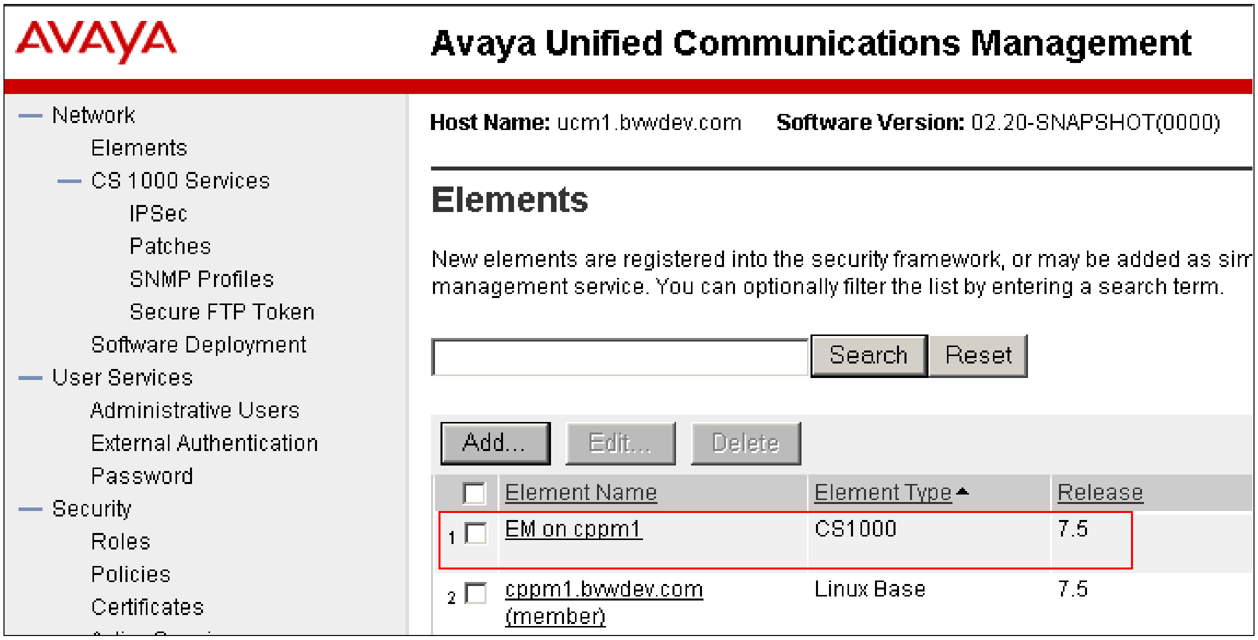

Figure 3: UCM Main Screen

5.2. Configuring the SIP Signaling Gateway

This section describes the configuration required on the SIP Signaling Gateway present on the CS1000 so that CS1000 can communicate with the Avaya Aura® Session Manager via SIP Trunks. Assumption is made here that the IP Telephony node is already added.

To access the Node in the EM left navigator screen, navigate to **IP Network > Nodes: Servers, Media Cards** as shown in **Figure 4** below.

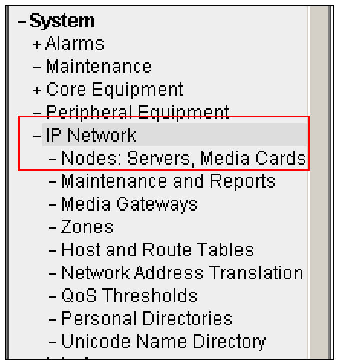

Figure 4: EM Screen showing navigation tree to Nodes

During compliance testing Node **551** was already created. Click on this Node as shown in **Figure 5** below.

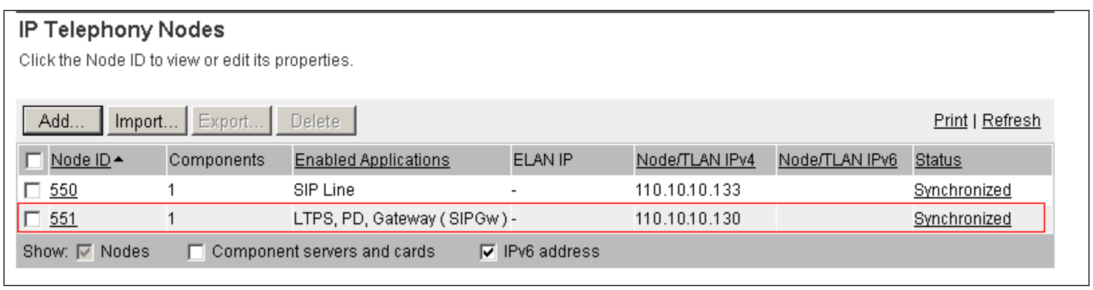

Figure 5: Accessing the Node

Open the SIP Signaling Gateway configuration by clicking on **Gateway (SIPGw)** as shown in **Figure 6** below.

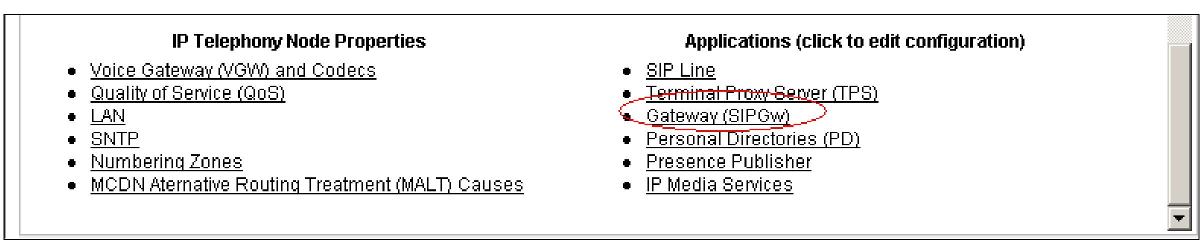

Figure 6: Accessing the SIP Signaling Gateway

In the **General** tab, select the values as shown in **Figure 7** below. A **SIP domain name** of **sip.ipc.com** was chosen since this is the domain name that will be configured on the Avaya Aura® Session Manager. Similarly, **cppm1** was configured as the **Gateway endpoint name**.

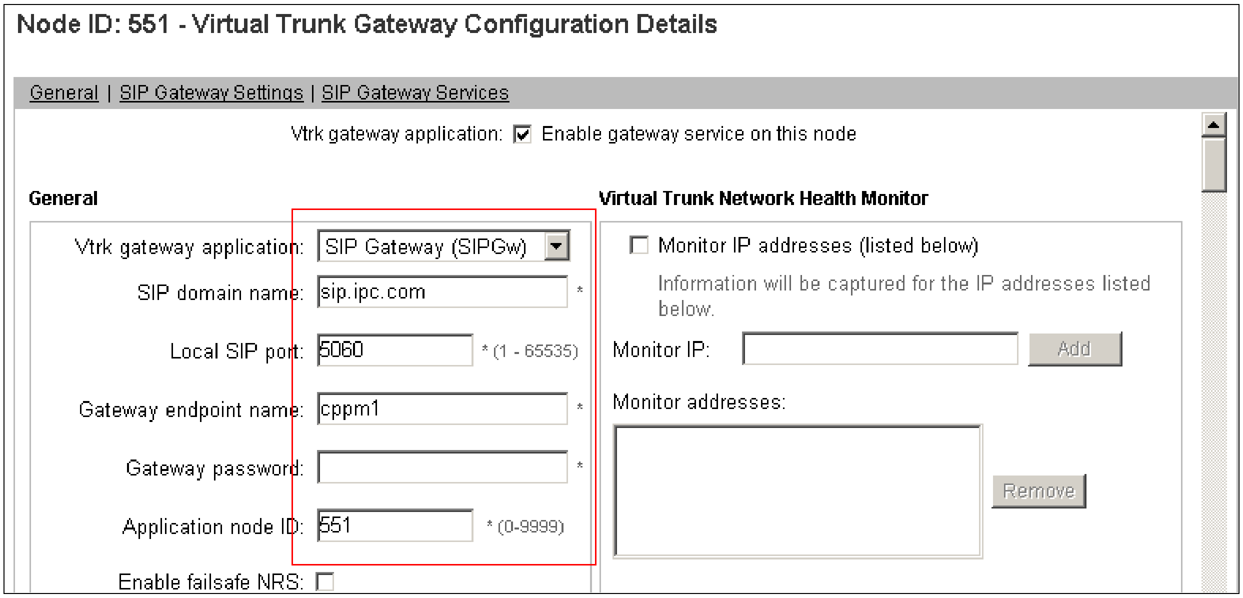

Figure 7: SIPGw General tab Configuration

Under the **Proxy or Redirect Server** section, enter the IP address of the Avaya Aura® Session Manager and select **UDP** as the Transport protocol as shown in **Figure 8** below. Leave the remaining values at their default settings. During compliance testing **110.10.10.198** was the IP address of the Avaya Aura® Session Manager.

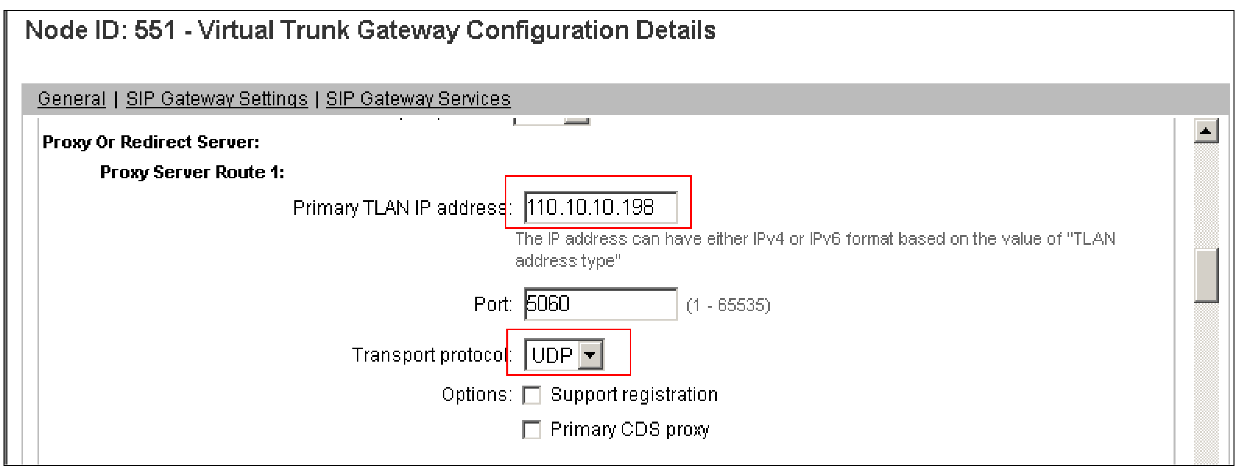

Figure 8: Proxy or Redirect Server Configuration

In the **SIP URI Map** section, enter the values as shown in **Figure 9** below. These values need to be matched if integration is to be successful between Unigy and CS1000, since Unigy is only able to understand the values below in its SIP messaging properties.

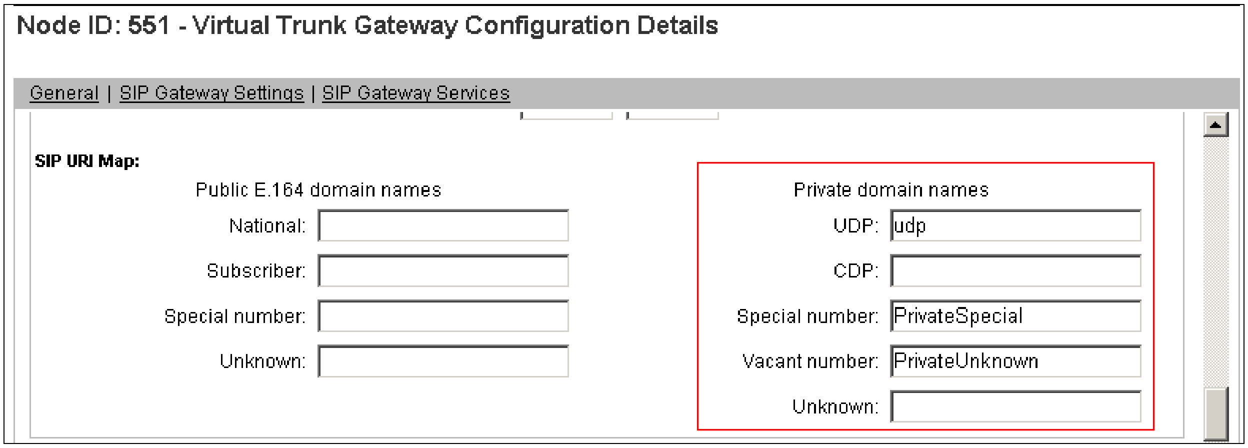

Figure 9: SIP URI Map Configuration

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

5.3. Configuring D-Channel

This section explains the configuration of a D-Channel for SIP Trunking. From the EM navigation screen, navigate to **Routes and Trunks > D-Channels** as shown in **Figure 10** below.

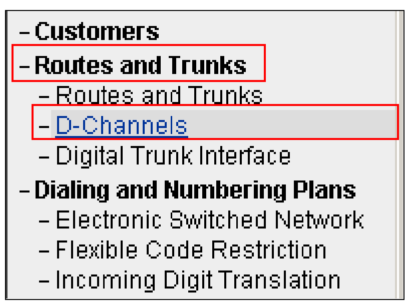

Figure 10: EM Screen showing navigation tree to D-Channels

Choose a D-Channel number to add as shown in **Figure 11** below. During compliance testing D-Channel number **10** was selected. Click on **to Add** to continue.

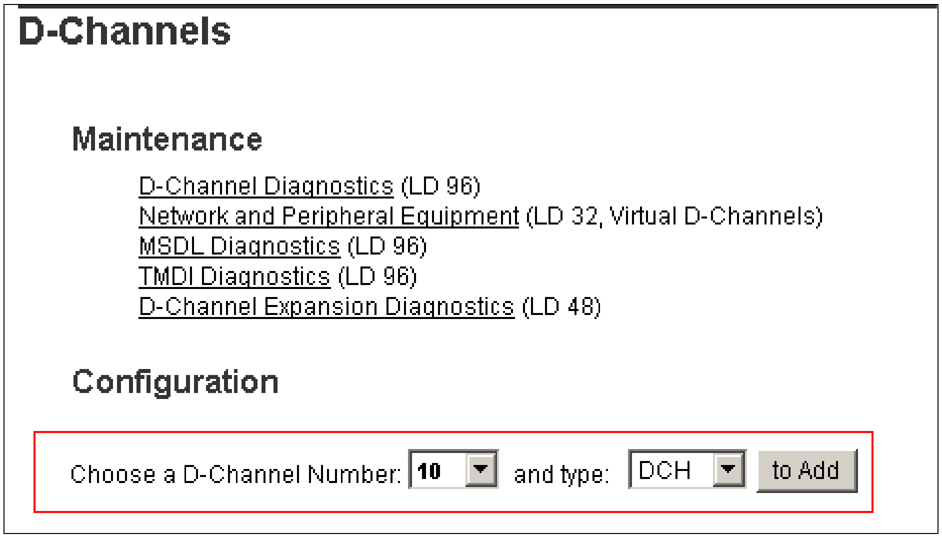

Figure 11: Adding D-Channel

Configure the **Basic Configuration** values for the D-Channel as shown in **Figure 12** below.

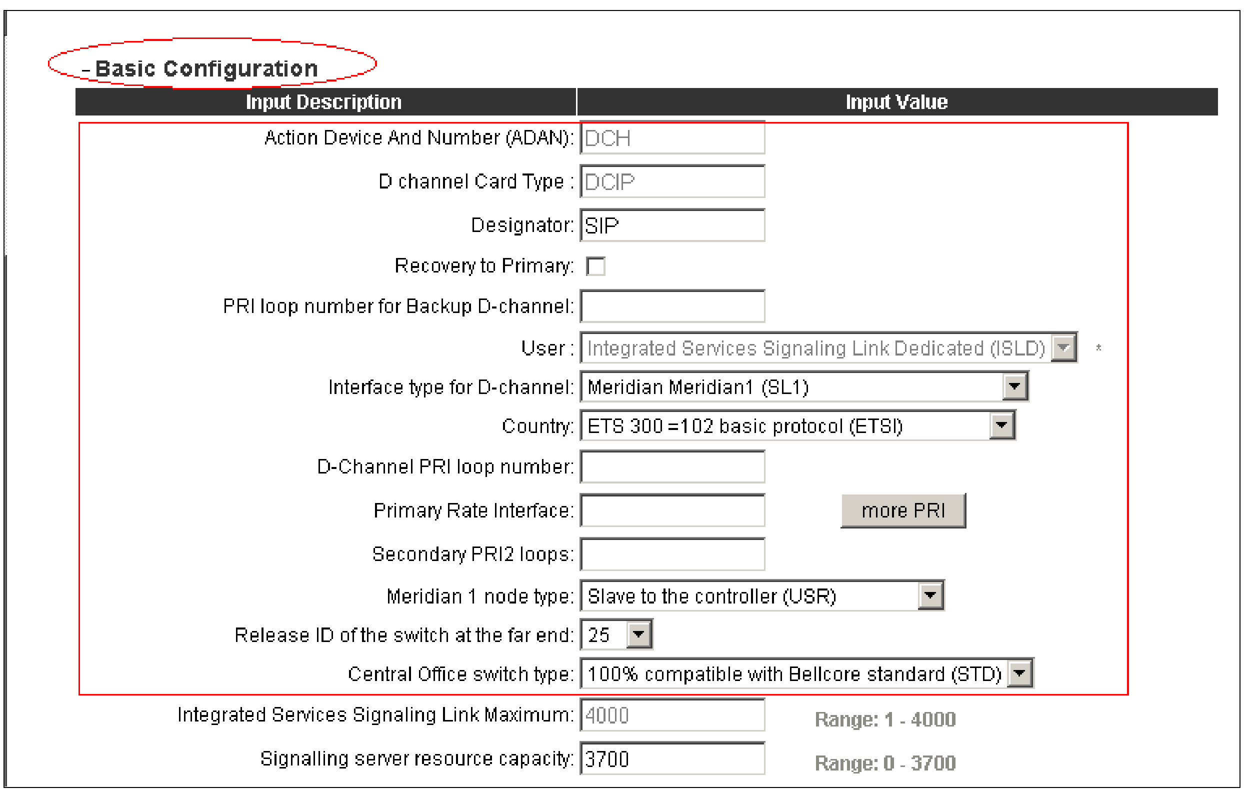

Figure 12: D-Channel Basic Configuration

To edit the **Remote Capabilities** of the D-Channel, click on the **Edit** button as shown in **Figure 13** below.

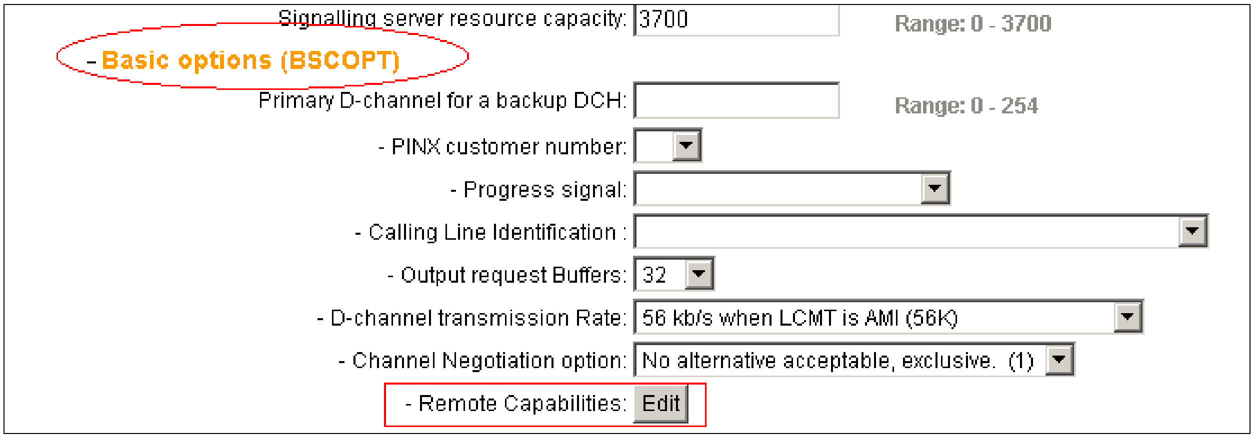

Figure 13: Editing Remote Capabilities Screen

Select the boxes for the desired Remote Capabilities as shown in **Figures 14** below. Click on **Return - Remote Capabilities** button to return back to the main screen to complete the D-Channel configuration.

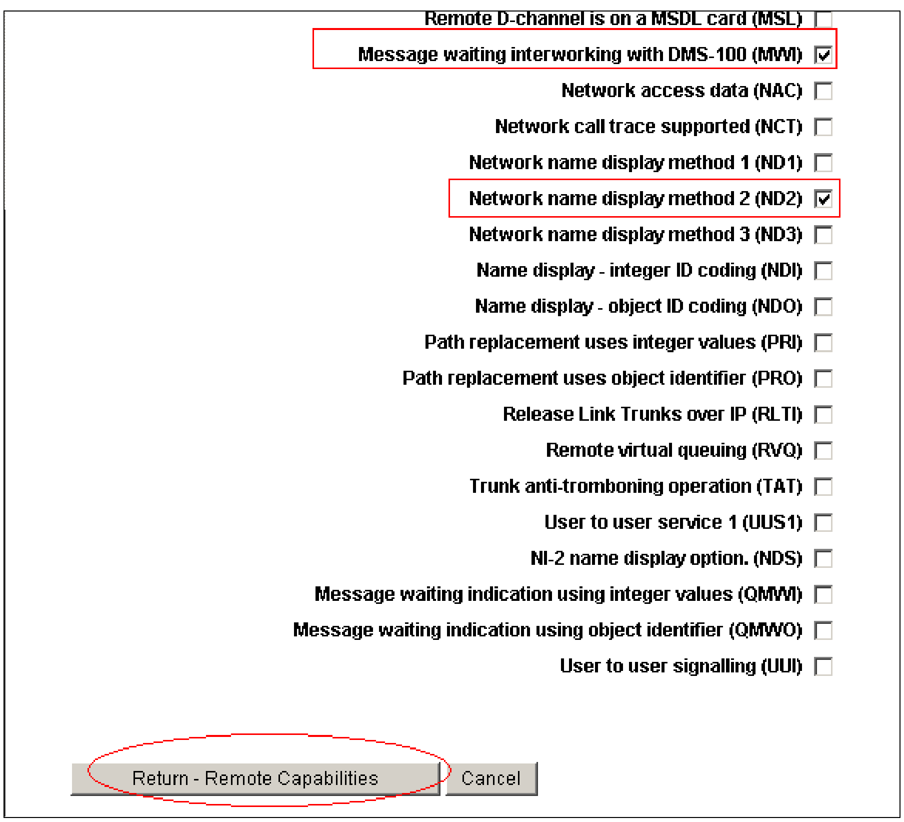

Figure 14: Remote Capabilities Values

5.4. Configuring Routes and Trunks

This section explains the configuration of the SIP routes and trunks which will be used by CS1000 and Unigy to communicate between them. To add a new route, navigate to **Routes and Trunks > Routes and Trunks** from the EM left hand navigator window as shown in **Figure 15** below.

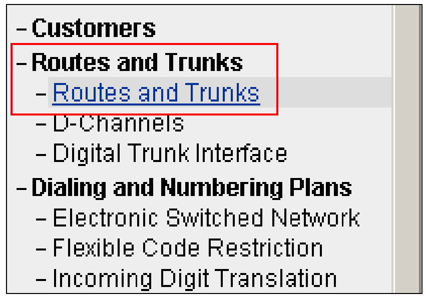

Figure 15: EM Screen showing navigation tree to Routes and Trunks

From the Routes and Trunks screen click on the **Add route** button to start configuring a new route as shown in **Figure 16** below.

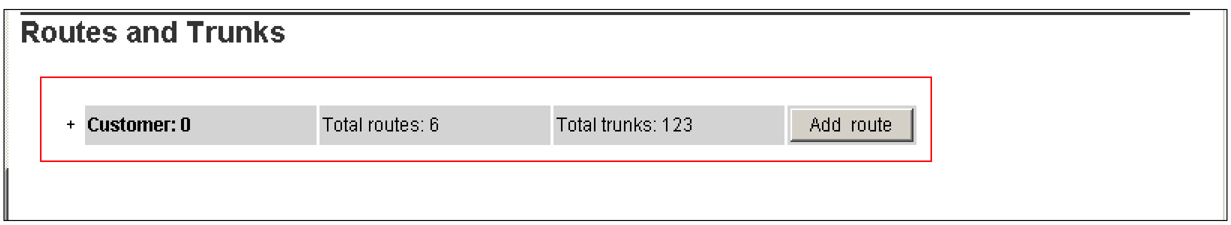

Figure 16: Adding a new Route

During compliance testing **Route number 10** was added. Select the values from the drop down menu and configure the values as shown in **Figures 17a,** 17**b** and **17c** below.

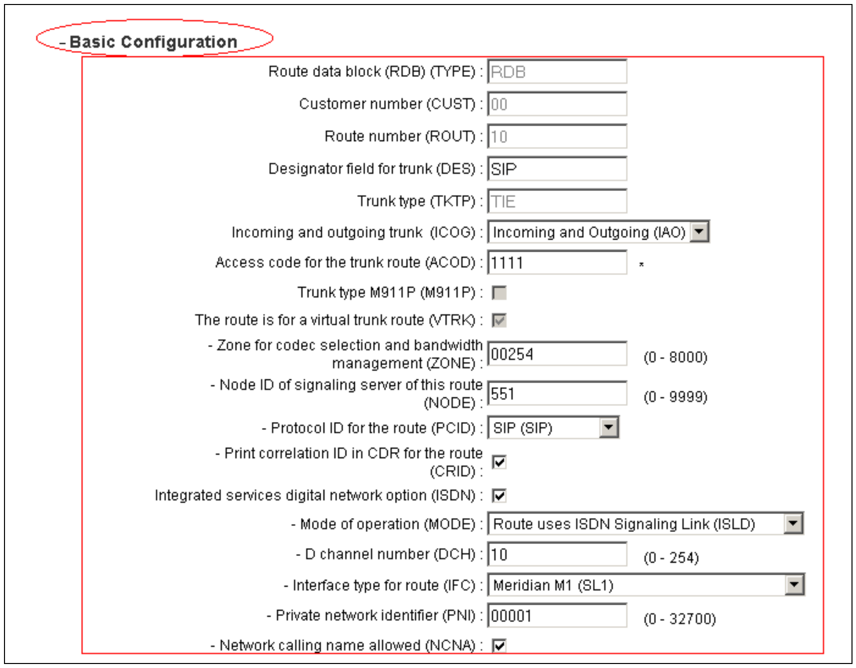

Figure 17a: Route Basic Configuration values

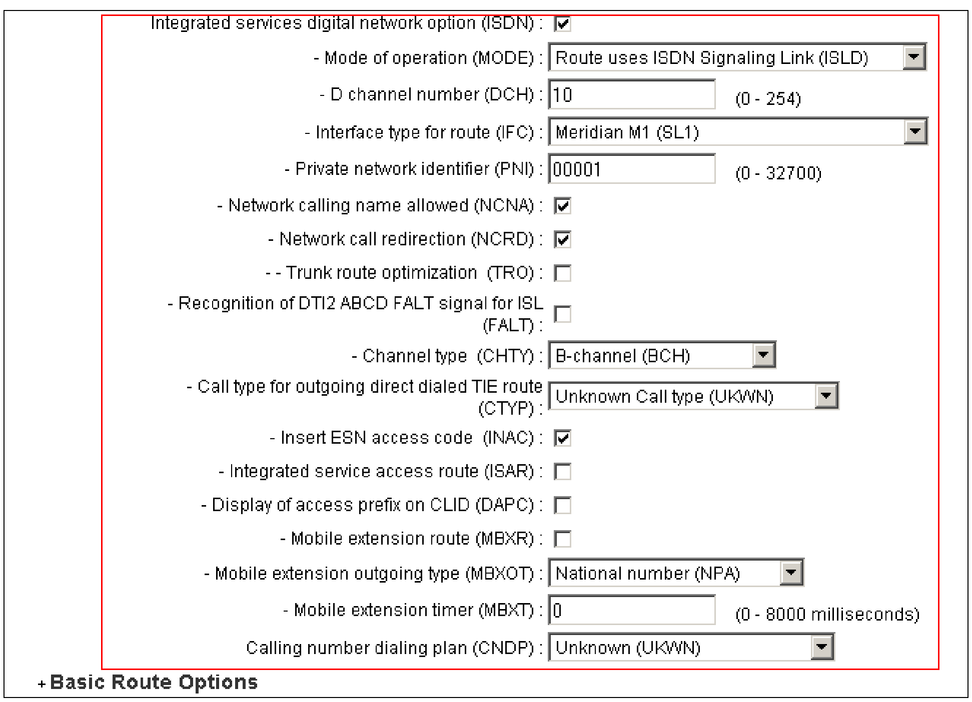

Figure 17b: Route Network Options values

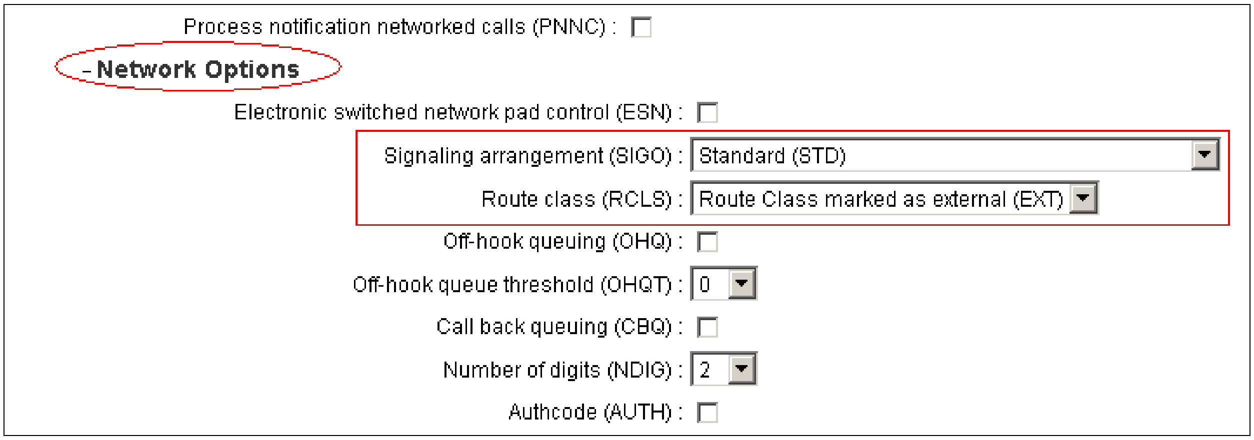

Figure 17c: Route Network Options values

Configure the trunk values as shown in **Figure 18** below. During compliance testing the **Terminal number** used was **100 1 00 00** since it is a virtual trunk. Click on the **Edit** button to configure the required **Class of Service** for the trunks.

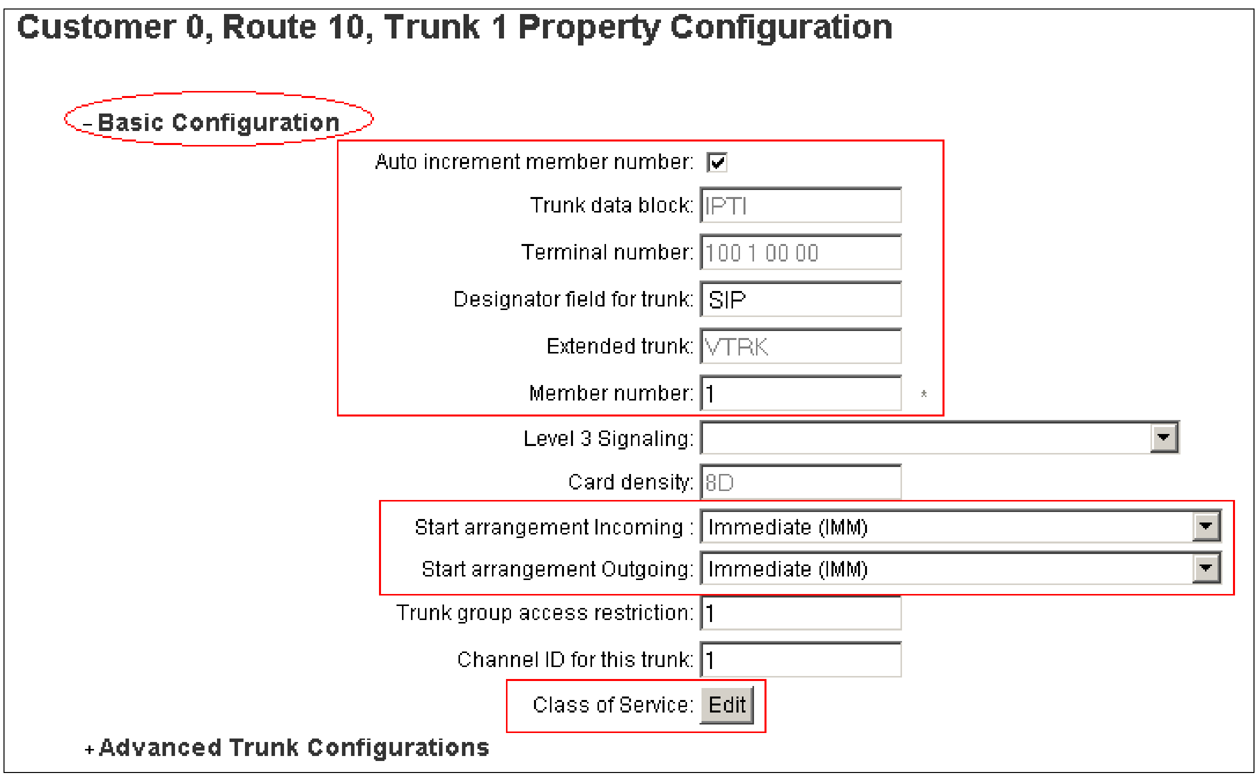

Figure 18: Trunk Properties

Figure 19 shows the **Class of Service** values selected for the compliance testing from the drop down menu. Click on **Return Class of Service** button to complete the trunks configuration.

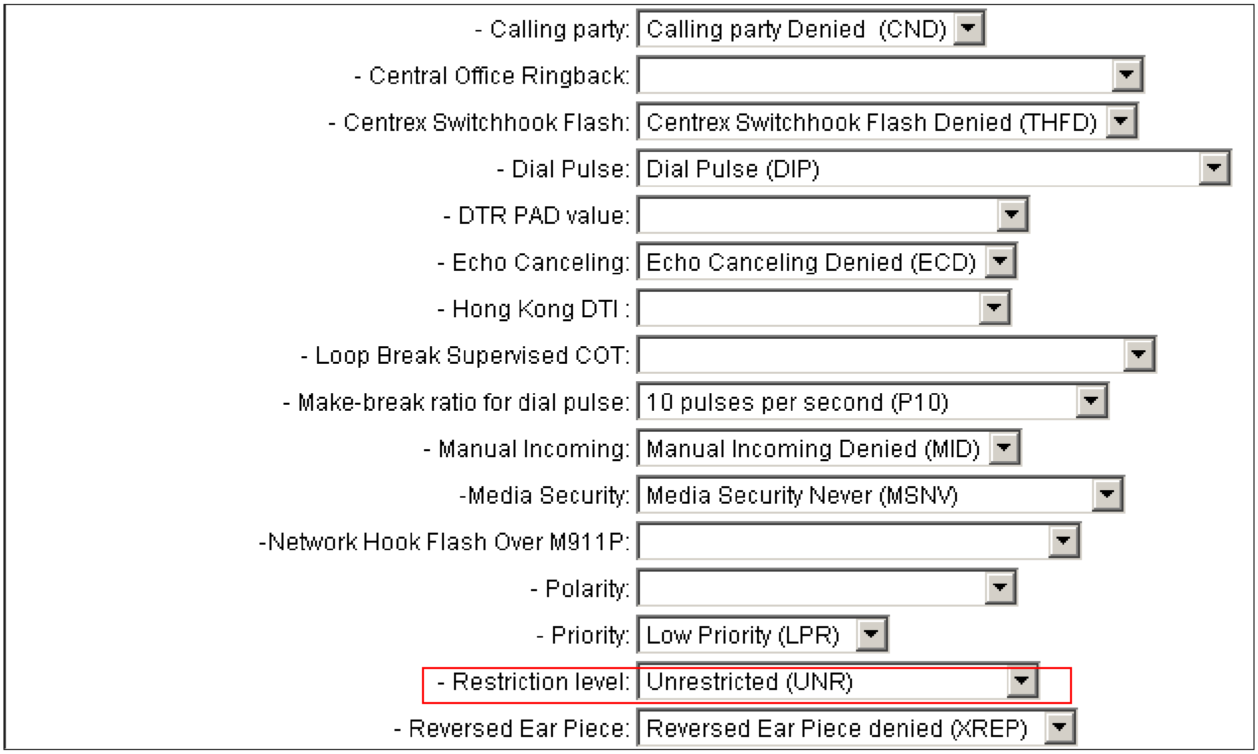

Figure 19: Trunk Class of Service

5.5. Configuring Digit Manipulation Block

This section explains the digit manipulation block that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans** > **Electronic Switched Network** as shown in **Figure 20** below.

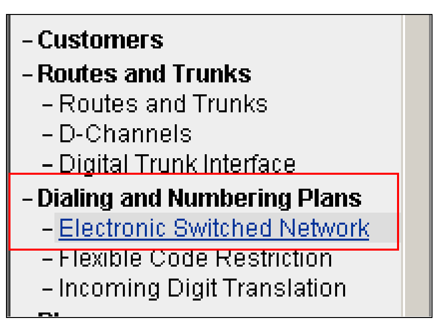

Figure 20: EM Screen showing navigation tree to Electronic Switched Network

Click on the **Digit Manipulation Block (DGT)** option as shown in **Figure 21** below.

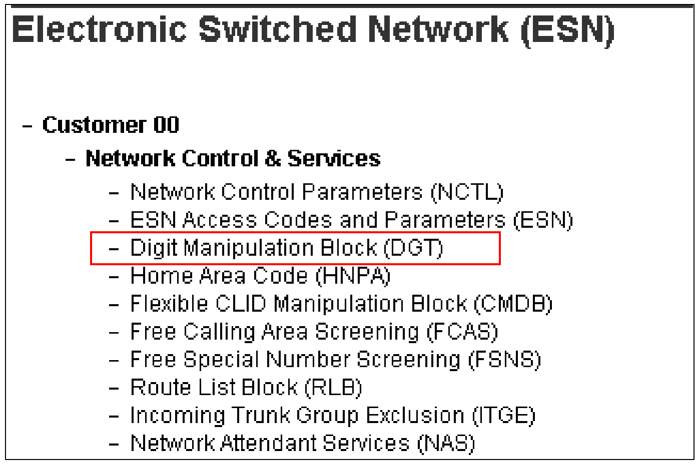

Figure 21: Accessing Digit Manipulation Block

Figure 22 below shows the Digit Manipulation Block Index users can add. However, during compliance testing **Digit Manipulation Block Index** of **0** was used which is already added in the CS1000 system by default.

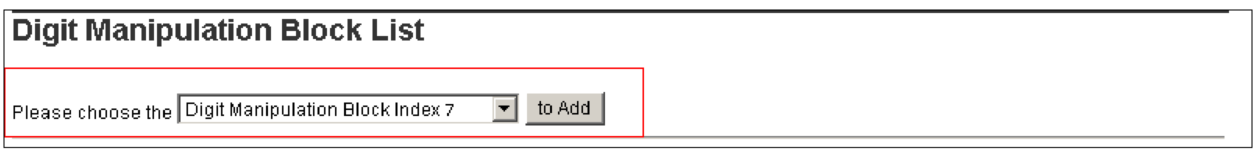

Figure 22: Adding a Digit Manipulation Block Index

5.6. Configuring Route List Block

This section explains the route list block that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** above. Click on **Route List Block (RLB)** option as shown in **Figure 23** below.

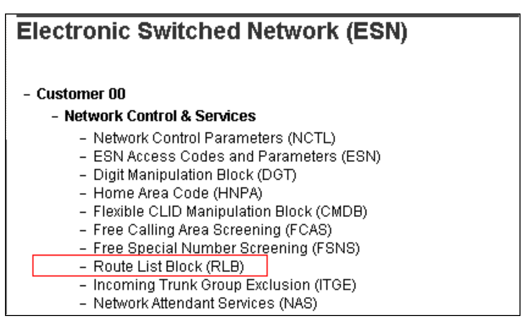

Figure 23: Accessing Route List Block

Start adding a **route list index** as shown in **Figure 24** below. During compliance testing, list index **10** was added. Click on **to Add** to continue.

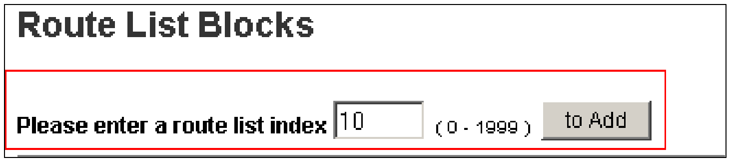

Figure 24: Adding Route List Index

Click on **Edit** for **Data Entry Index 0** as shown in **Figure 25** below.

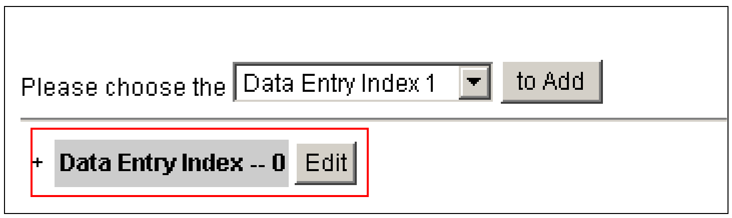

Figure 25: Adding Data Entry Index

Figure 26 below shows the values configured for the index block used during compliance testing. A **Route Number** of **10** and **Digit Manipulation Index** of **0** were selected as per the configuration explained in **Sections 5.4** and **5.5** respectively. Click **Submit** (not shown) to complete the configuration.

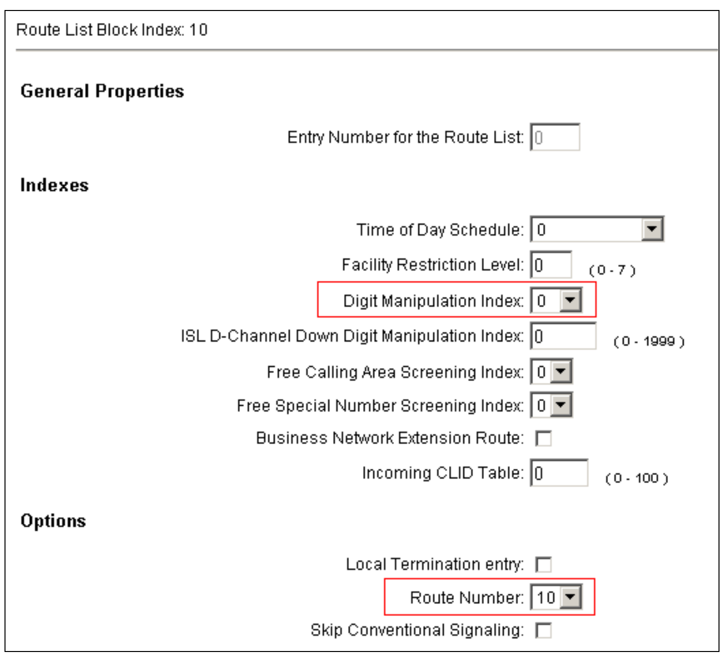

Figure 26: Route List Block properties

5.7. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** above. Click on the **Distant Steering Code (DSC)** option as shown in **Figure 27** below.

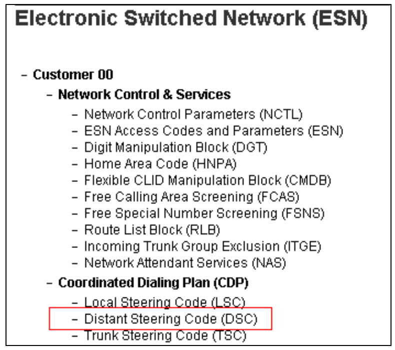

Figure 27: Accessing Distant Steering Code

From the drop down menu select **Add** and enter a distant steering code to add as shown in **Figure 28** below. During compliance testing a code of **350** was added since the Unigy extension range started with 350xx. Click on **to Add** to continue.

Figure 28: Adding a Distant Steering Code

Enter the values as shown in **Figure 29** below. Note that the **Route List to be accessed for trunk steering code** value selected is **10** based on the configuration explained in **Section 5.6** above. Click on **Submit** to complete the configuration.

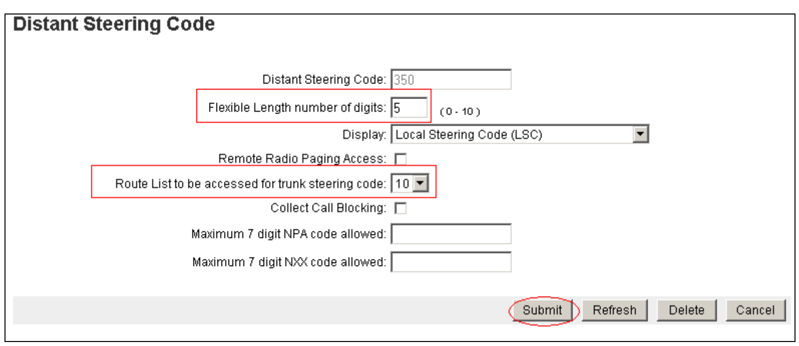

Figure 29: Distant Steering Code properties

6. Configure Routing using Avaya Aura® System Manager

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

- Logging into the Avaya Aura® System Manager.
- Adding a Domain.
- Adding a Location.
- Adding SIP entities.
- Adding Routing Policies.
- Adding Dial Patterns.

6.1. Logging into the Avaya Aura® System Manager

This section explains the steps to launch the login screen of System Manager, and then access the Network Routing Policy.

To launch the System Manager Login screen, start an IE browser and type the IP address of System Manager in the URL (not shown). **Figure 30** below shows the Log On Screen. Type the required **User ID** and **Password** credentials and click **Log On** to continue.

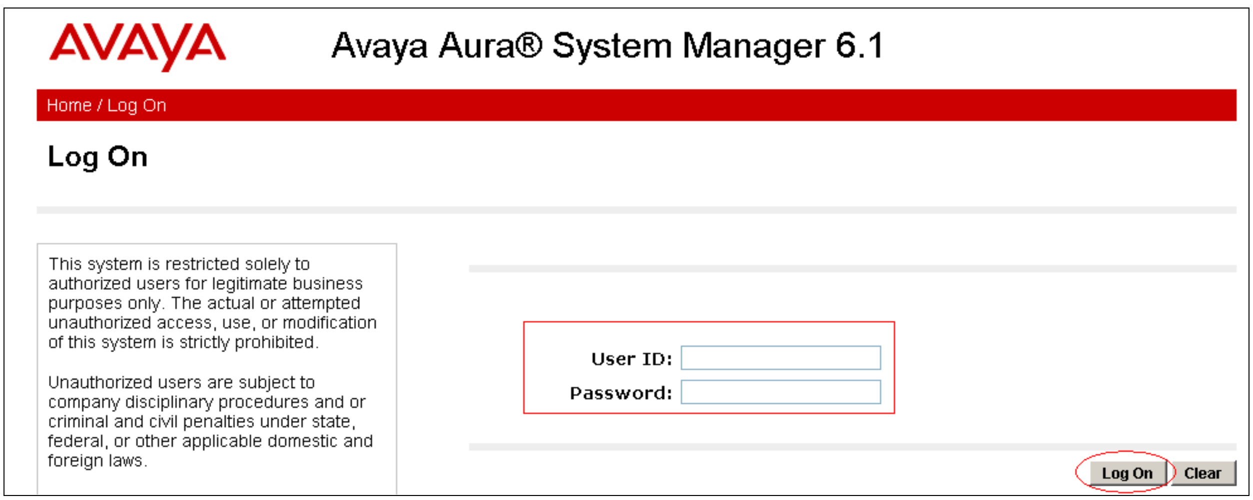

Figure 30: Avaya Aura® System Manager Login Screen

From the main screen of System Manager access the Network Routing Policy by selecting **Routing** as shown **in Figure 31** below.

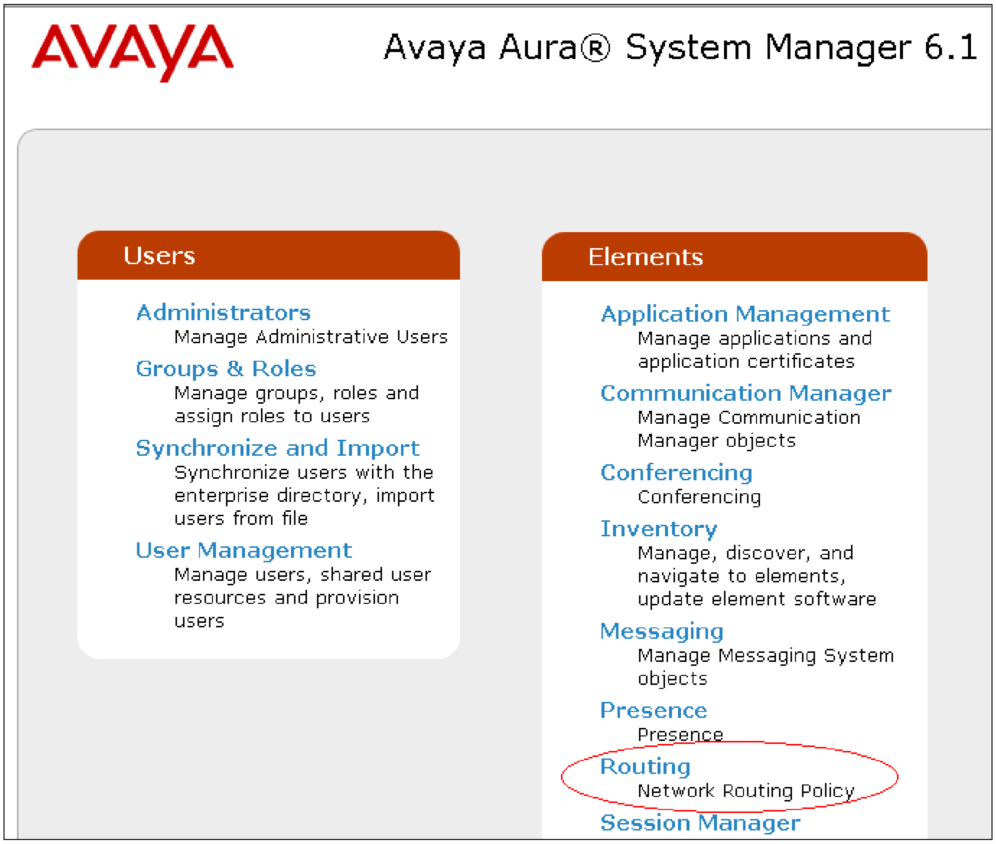

Figure 31: Avaya Aura® System Manager Main Screen

6.2. Adding a Domain

To add a domain, select **Domains** from the left hand window of the Routing screen and click on **New** (not shown). Configure the Domain in the **Name** field as shown in **Figure 32** below and click on **Commit** to complete adding a domain. During compliance testing a domain name of **sip.ipc.com** was used. Additional domains can be added in a similar fashion.

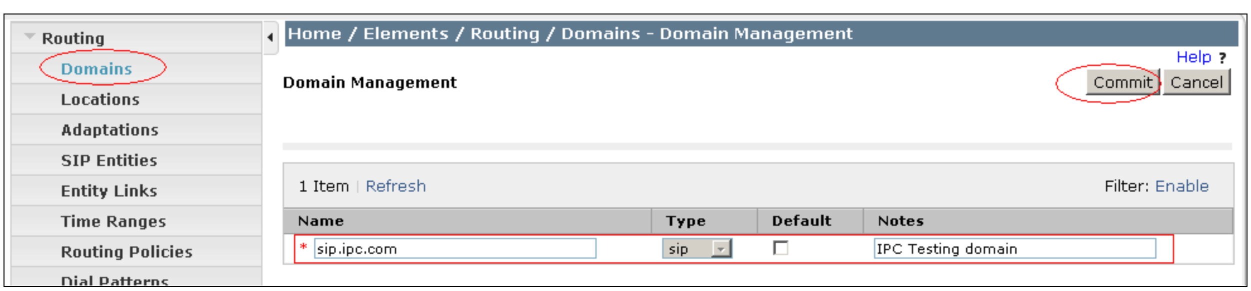

Figure 32: Domain Management

6.3. Adding a Location

To add a location, select **Locations** from the left hand window of the Routing screen and click on **New** (not shown). Configure the Location **Name** as shown in **Figure 33** below and click on **Commit** to add the Location. During compliance testing a location name of **Belleville,Ont,Ca** was used. Click on **Commit** to complete adding a location. Additional locations can be added in a similar fashion.

Figure 33: Location Details

6.4. Adding SIP Entities

This section explains the adding of SIP entities to Session Manager, Unigy System and the CS1000 system routing. To add SIP Entities, select **SIP Entities** from the left hand window of the Routing screen and click on **New** (not shown).

Figures 34a and **34b** show the SIP Entity Details for the Session Manager routing. The **FQDN or IP Address** of **110.10.10.198** is the IP address of the Session Manager. Also note that both **TCP** and **UDP** protocols need to be selected for the Entity Links and Ports to **IPC** and **sip.ipc.com** respectively, since Unigy System changes protocols for various diversions. If only the **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

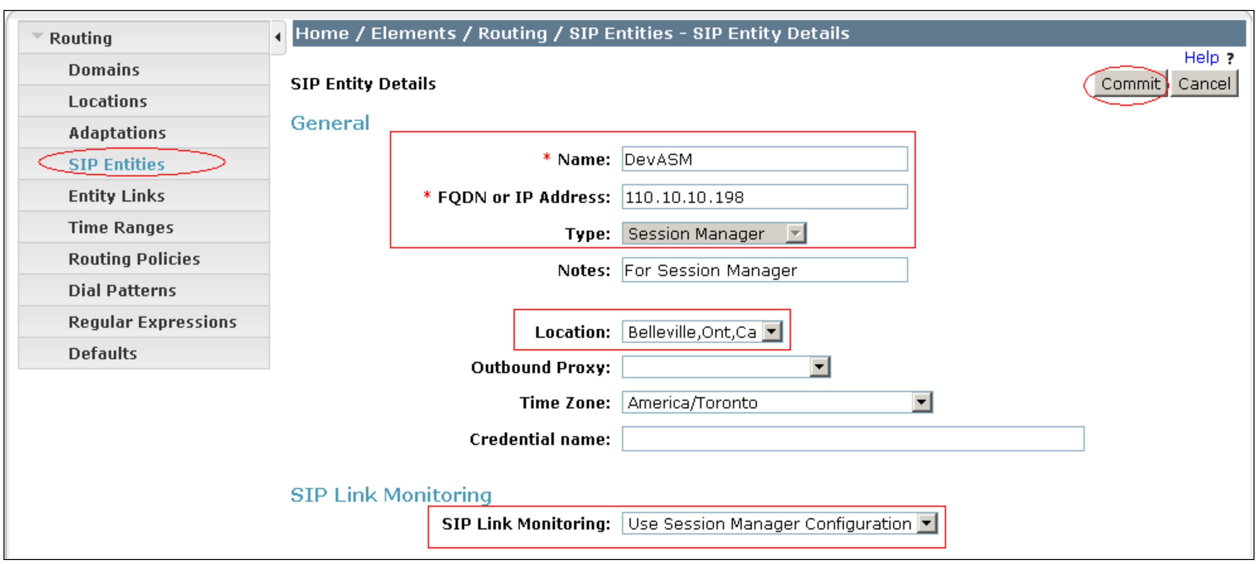

Figure 34a: SIP Entity Details for Session Manager

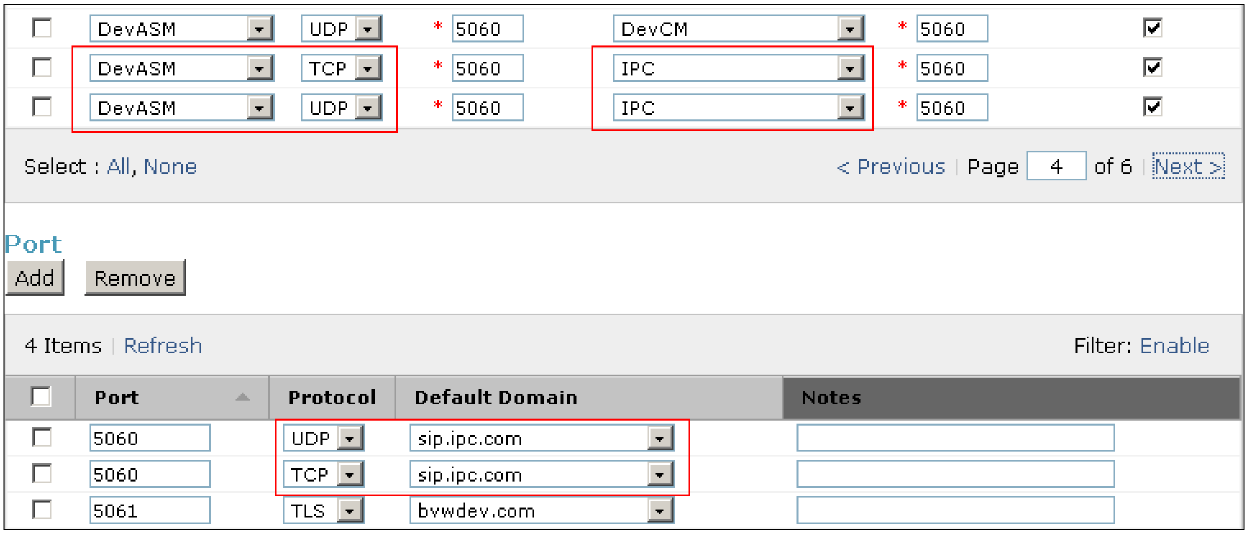

Figure 34b: SIP Entity Details for Session Manager (cont'd)

Figures 35a and **35b** show the SIP Entity Details for the Unigy System routing. The **FQDN or IP Address** of **110.10.10.226** is the IP address of the Unigy System. Also note that both **TCP** and **UDP** protocols need to be selected in the Entity Links section for **IPC** since Unigy System changes protocols for various diversions. If only **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

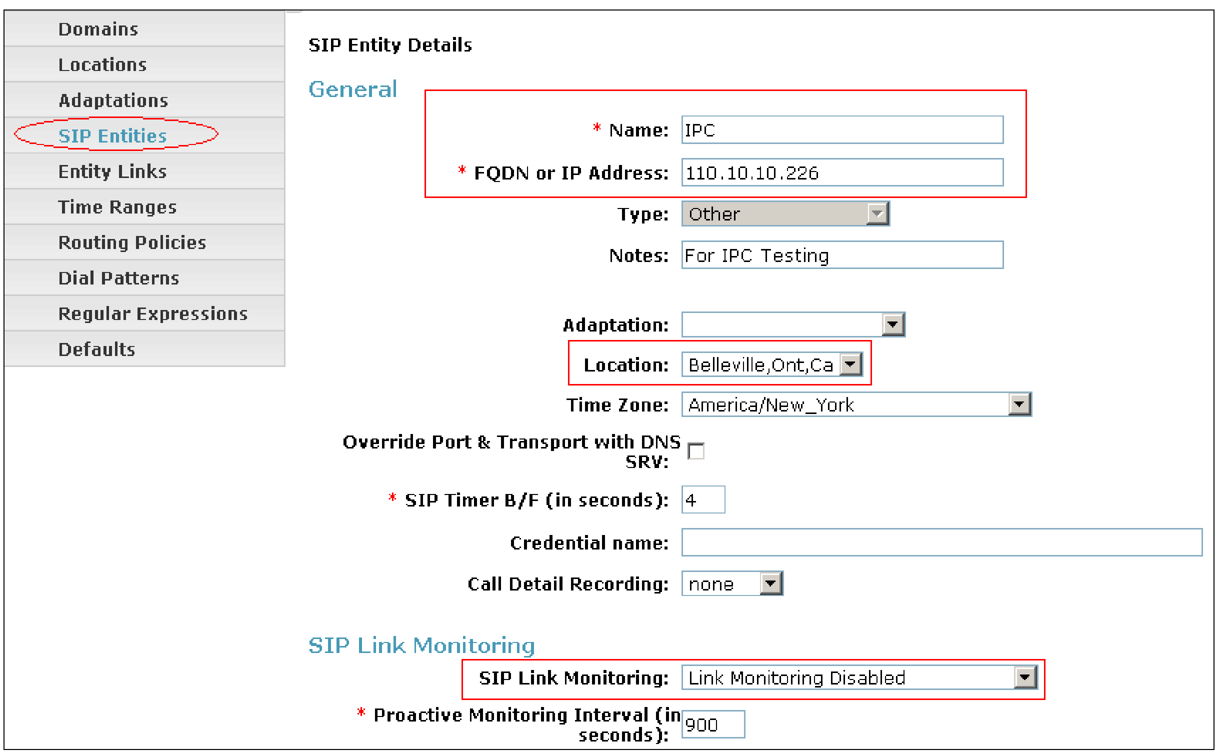

Figure 35a: SIP Entity Details for Unigy System

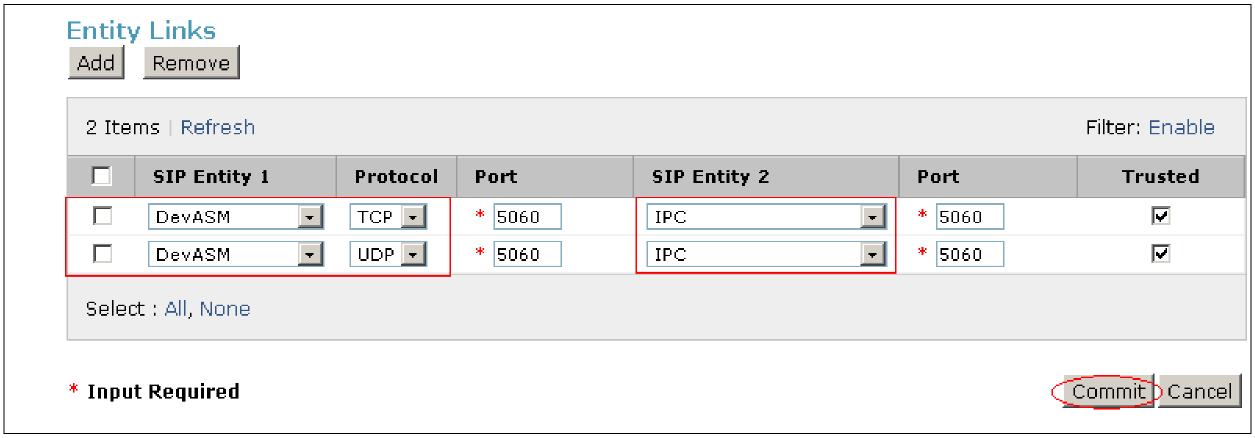

Figure 35b: SIP Entity Details for Unigy System (cont'd)

Figures 36a and **36b** show the SIP Entity Details for the CS1000 System routing. The **FQDN or IP Address** of **110.10.10.130** is the Node IP address of the SIP Signaling Gateway of the CS1000 System. Also note that both **TCP** and **UDP** protocols need to be selected in the Entity Links secton for **cppm1** since Unigy System changes protocols for various diversions. If only **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

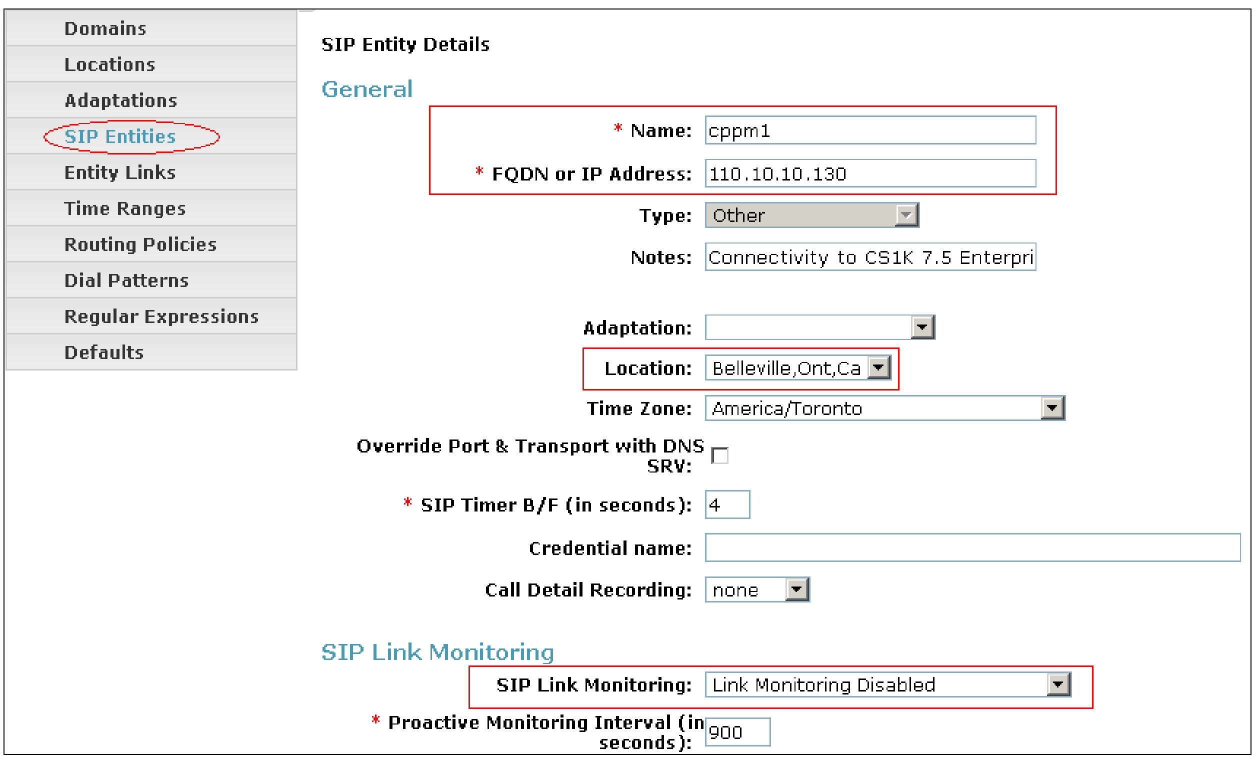

Figure 36a: SIP Entity Details for CS1000 System

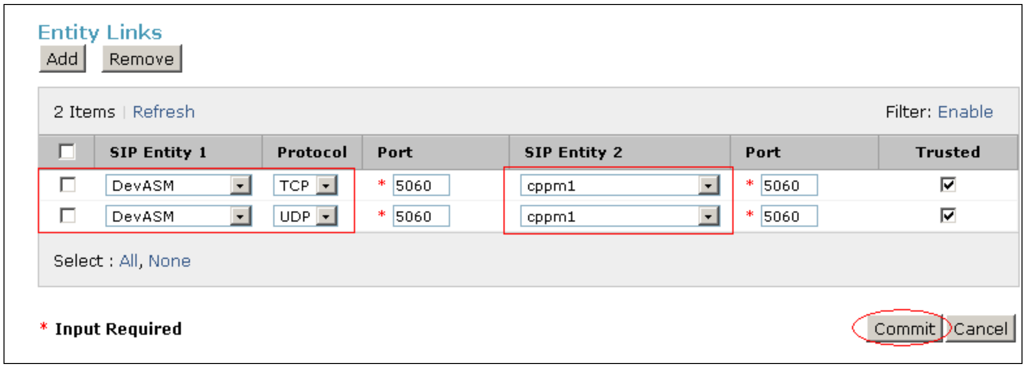

Figure 36b: SIP Entity Details for CS1000 System (cont'd)

6.5. Adding Routing Policies

This section explains the Routing Policy configuration for the Unigy and CS1000 Systems. To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown).

Figures 37a and **37b** show the Routing Policy Details for the Unigy System. Select the Unigy System as the SIP Entity Destination and add the dial pattern associated with the Unigy System. A dial pattern can be added once it has been configured as explained in **Section 6.6** below. Click on **Commit** to complete adding a routing policy.

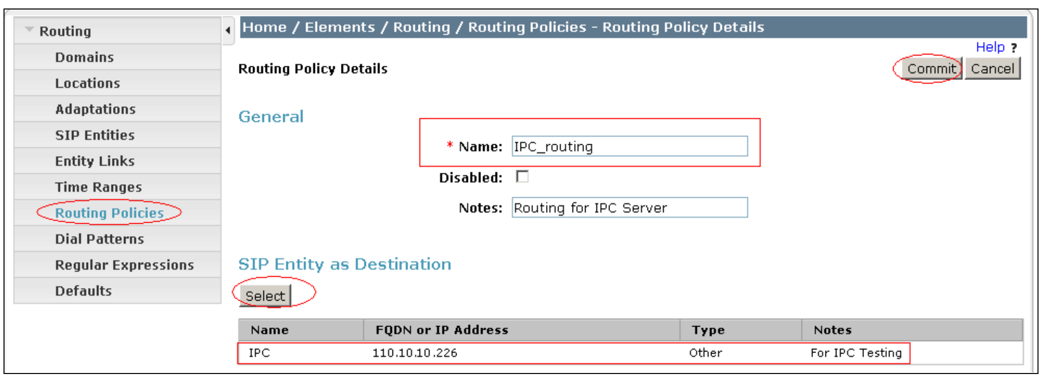

Figure 37a: Routing Policy Details for Unigy System

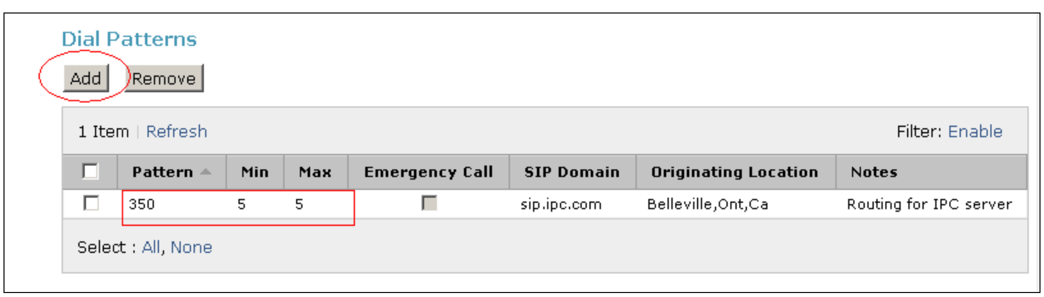

Figure 37b: Routing Policy Details for Unigy System (cont'd)

Figures 38a and **38b** show the Routing Policy Details for the CS1000 System. Select the CS1000 System as the SIP Entity Destination and add the dial pattern associated with the CS1000 System. A dial pattern can be added once it has been configured as explained in **Section 6.6** below. Click on **Commit** to complete adding a routing policy.

Additional routing policies can be configured as required in a similar fashion.

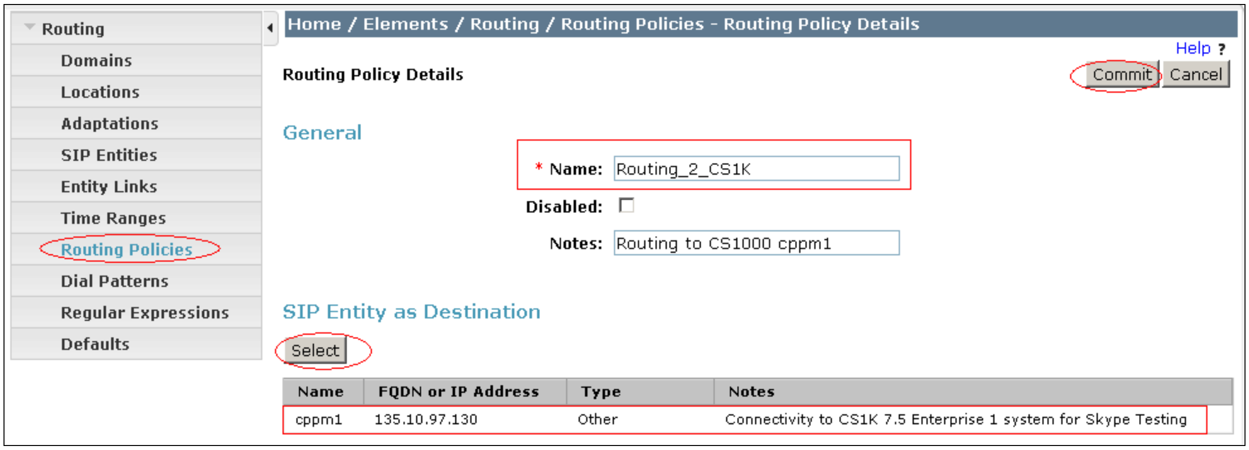

Figure 38a: Routing Policy Details for CS1000

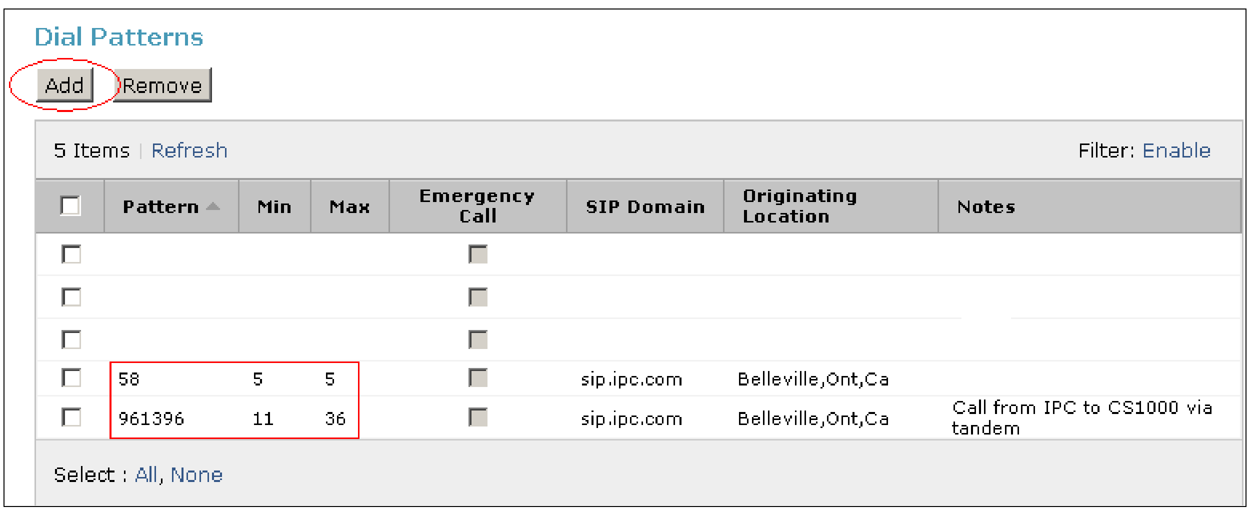

Figure 38b: Routing Policy Details for CS1000 (cont'd)

6.6. Adding Dial Patterns

This section explains the steps to add a dial pattern for the Unigy and CS1000 systems. To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown).

Figure 39 shows the Dial Pattern Details for the Unigy System. During compliance testing, the extension range on the Unigy System started with 350xx and therefore **350** is used in the **Pattern** field. The minimum and maximum size of the extension is defined as **5**. Add the **IPC routing** policy as configured in **Section 6.5** above. Click on **Commit** to complete adding the dial pattern. Additional dial patterns can be configured as required in a similar fashion.

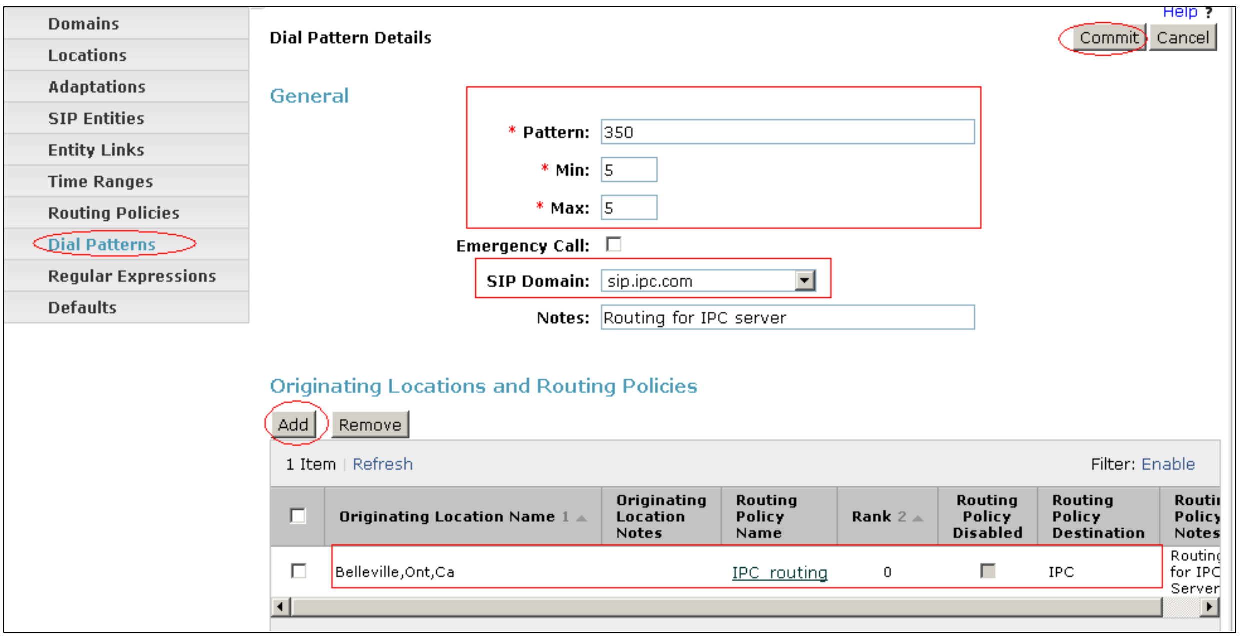

Figure 39: Dial Pattern Details

7. Configure IPC Media Manager

This section provides the procedures for configuring IPC Media Manager. The procedures include the following areas:

- Launch Unigy Management System.
- Administer SIP Trunks.
- Administer trunk groups.
- Administer route lists.
- Administer dial patterns.
- Administer route plans.
- Administer Codecs.

The configuration of Media Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes. For detailed administration and configuration information for the Unigy system refer to **Section 10 [2]**.

7.1. Launch Unigy Management System

Access the Unigy Management System web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Media Manager. Log in using the appropriate credentials.

The screen as shown in **Figure 40** below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

In the subsequent screen (not shown), click **Continue**.

Figure 40: Unigy Management System Login Screen

7.2. Administer SIP Trunks

The screen as shown in **Figure 41** below is displayed next. Select **Configuration > Site Configuration** from the top menu.

Figure 41: Unigy Management System Login Screen

Figures 42a and **42b** below show the **Site Configuration** information displayed in the left pane. Select **Trunks > SIP Trunks** and click the **"+"** icon in the lower left pane to add a new SIP trunk group. Click on the **Advanced** tab to configure the trunk. During compliance testing a SIP trunk by the name **SIP-Trunk-SM** was added with the required values as shown below. The IP address **110.10.10.198** is the IP address of the Avaya Aura® Session Manager. Values shown in the red box were used during compliance testing. Click on **Save** (not shown) to complete the configuration.

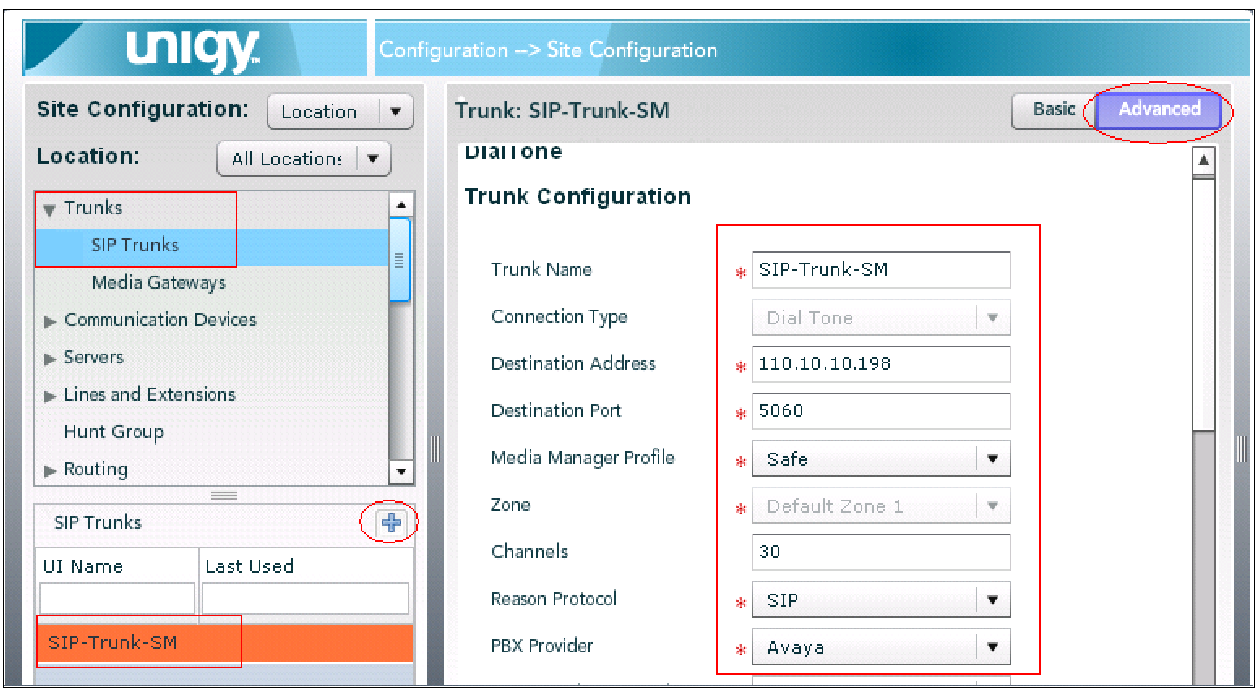

Figure 42a: Adding a SIP Trunk

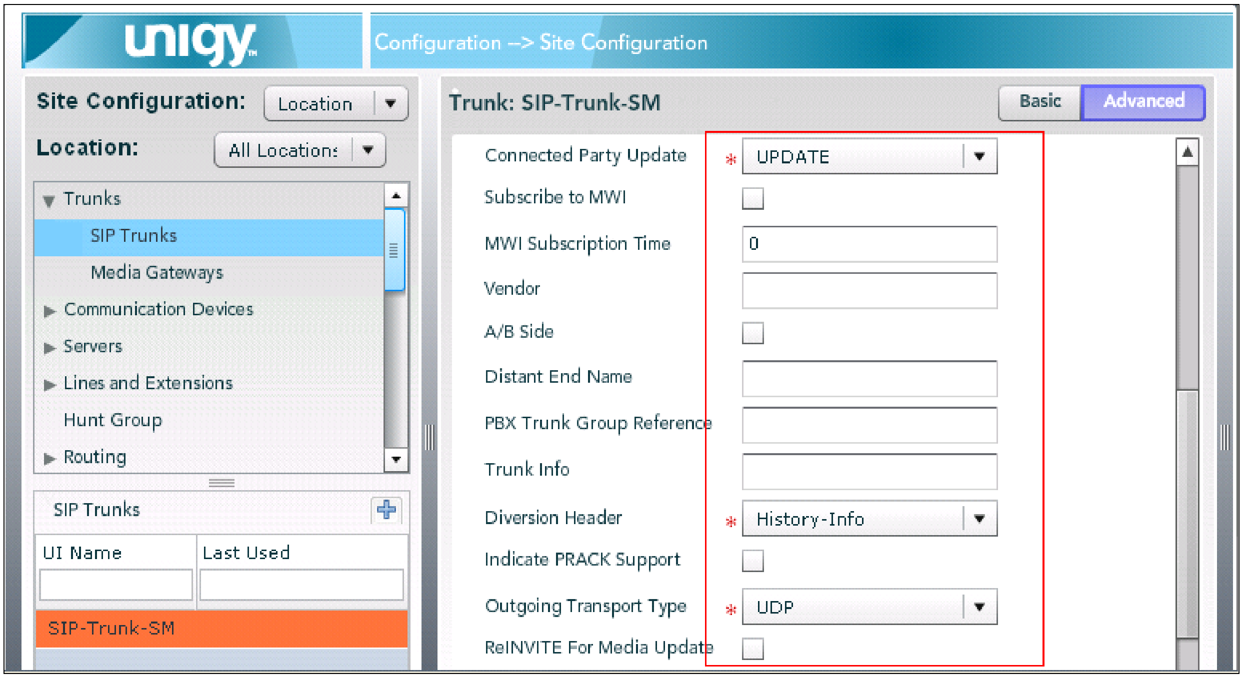

Figure 42b: Adding a SIP Trunk (cont'd)

7.3. Administer Trunk Groups

Select **Routing > Trunk Groups** in the left pane, and click the **"+"** icon in the lower left pane to add a new trunk group as shown in **Figure 43** below.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, leave the remaining values as default and click **Save** (not shown).

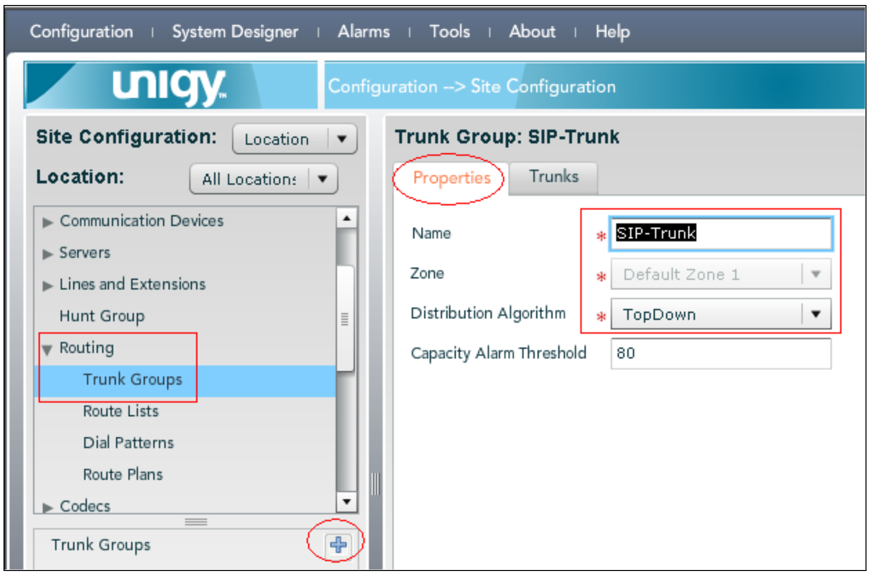

Figure 43: Adding Trunk Group

Select the **Trunks** tab in the right pane as shown in **Figure 44** below. The screen is updated with three panes. In the right pane, select the **Trunks** tab. In the listing, select and expand the applicable trunk (not shown) from **Section 7.2,** and drag the selection to the **Name** column in the middle pane as shown below. Click on **Save** (not shown) to complete the configuration.

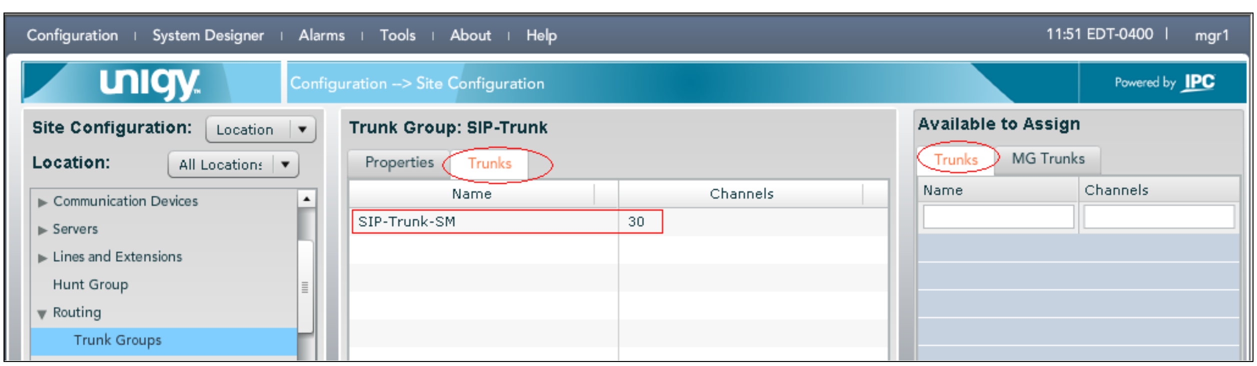

Figure 44: Adding Trunk Group (cont'd)

7.4. Administer Route Lists

Select **Routing** > **Route Lists** in the left pane, and click the **"+"** icon in the lower left pane to add a new route list as shown in **Figure 45** below.

The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration.

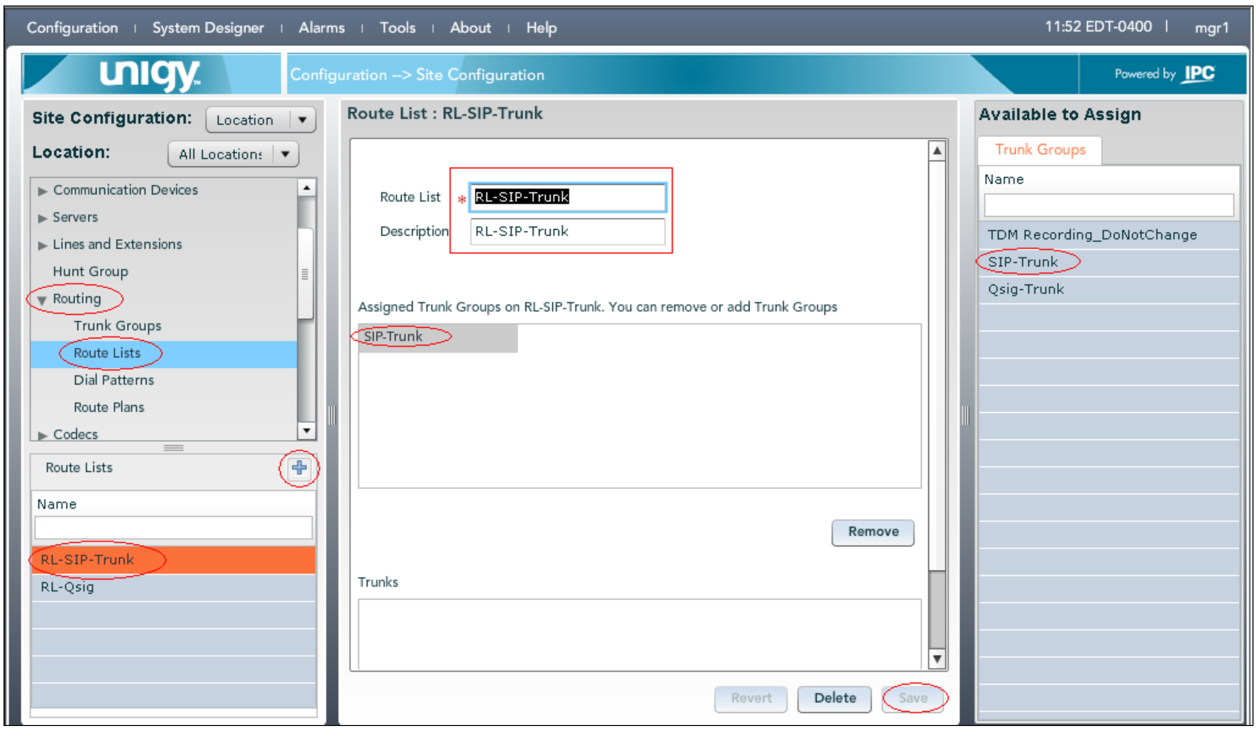

Figure 45: Adding Route List

7.5. Administer Dial Patterns

Select **Routing > Dial Patterns** in the left pane to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane as shown in **Figure 46** below.

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya CS1000 extensions, in this case **58$$$** with "$" matching to any digit. For **Call Classification**, select **External**. Click on **Save** to complete adding a dial pattern.

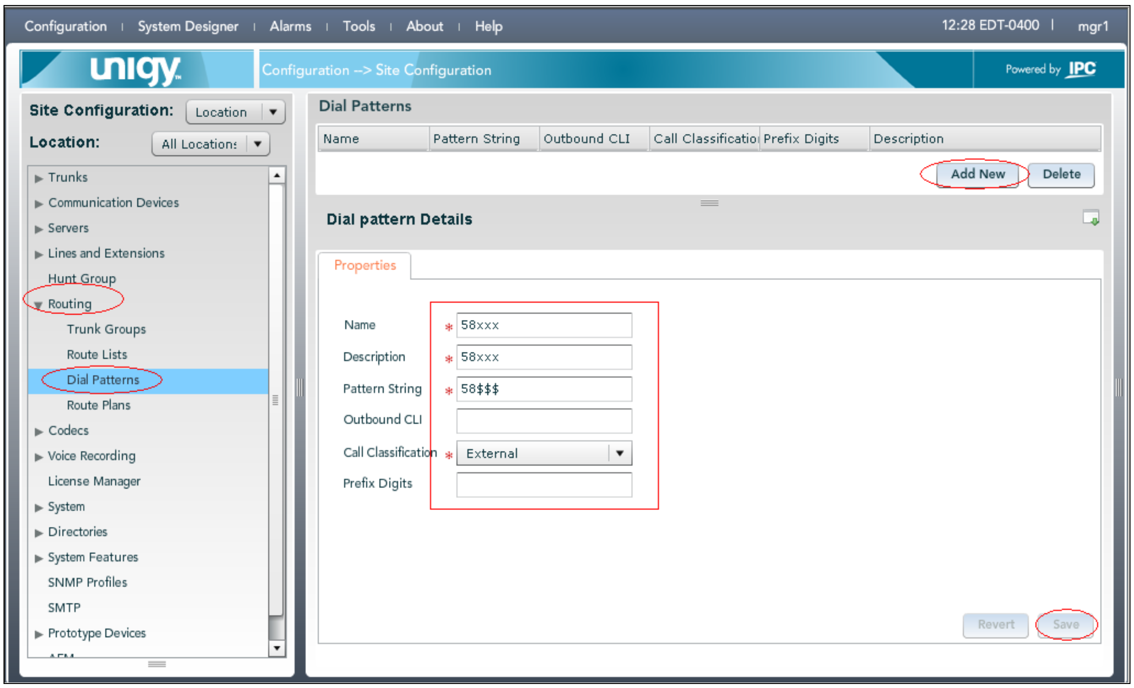

Figure 46: Adding a Dial Pattern

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Avaya CS1000. In the compliance testing, two dial patterns were created as shown in **Figure 47** below.

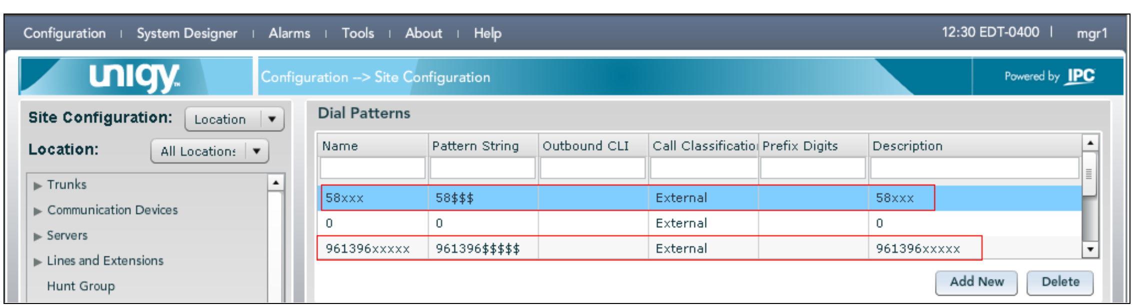

Figure 47: Extension and PSTN Dial Patterns

7.6. Administer Route Plans

Select **Routing > Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan as shown in **Figure 48** below.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and an optional **Description**. For **Calling Party**, enter * to denote any calling party from Unigy. For **Called Party**, select the dial pattern for the CS1000 users from **Section 7.5**. Select **Forward** for **Action**, and click on **Save**.

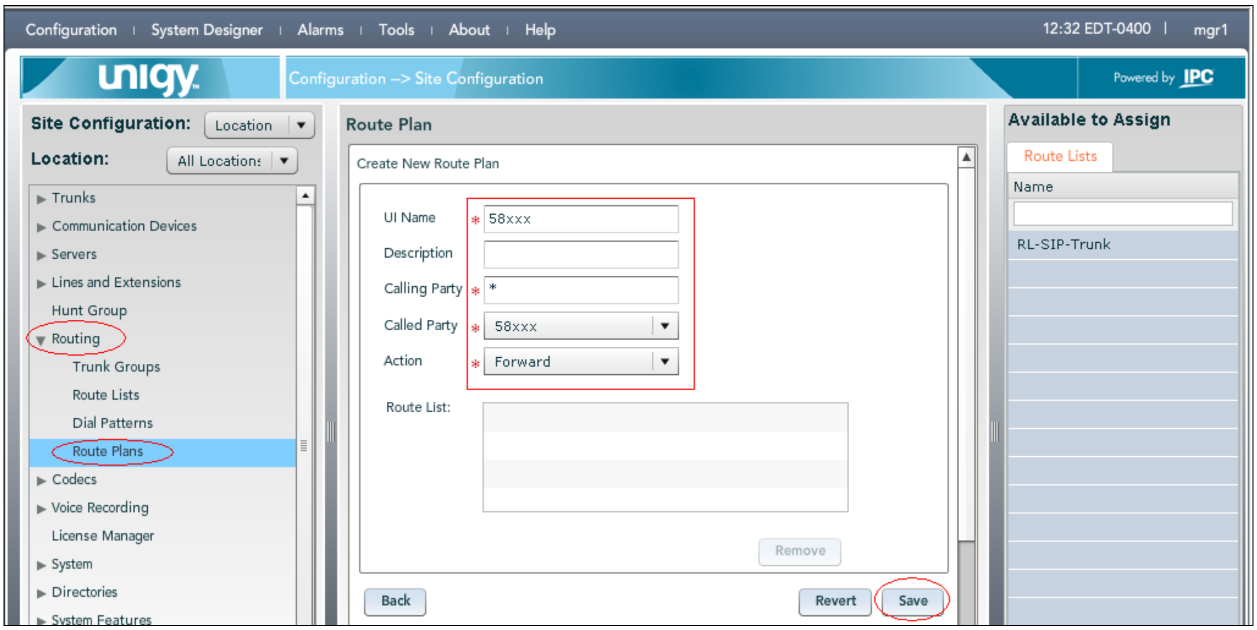

Figure 48: Creating a new Route plan

The screen is updated with the newly created route plan as shown in **Figure 49** below. Select the route plan, and click **Edit** toward the bottom of the screen (not shown).

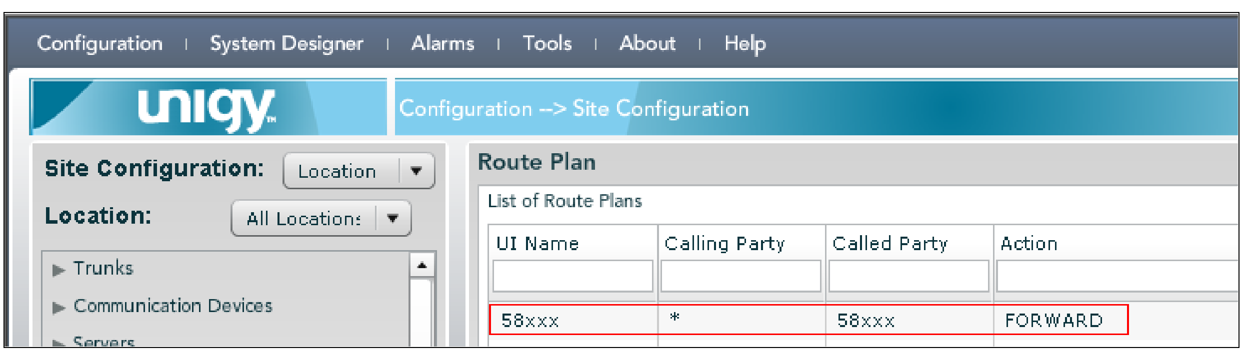

Figure 49: New Route Plan

The screen is updated with three panes again, as shown in **Figure 50** below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration**.**

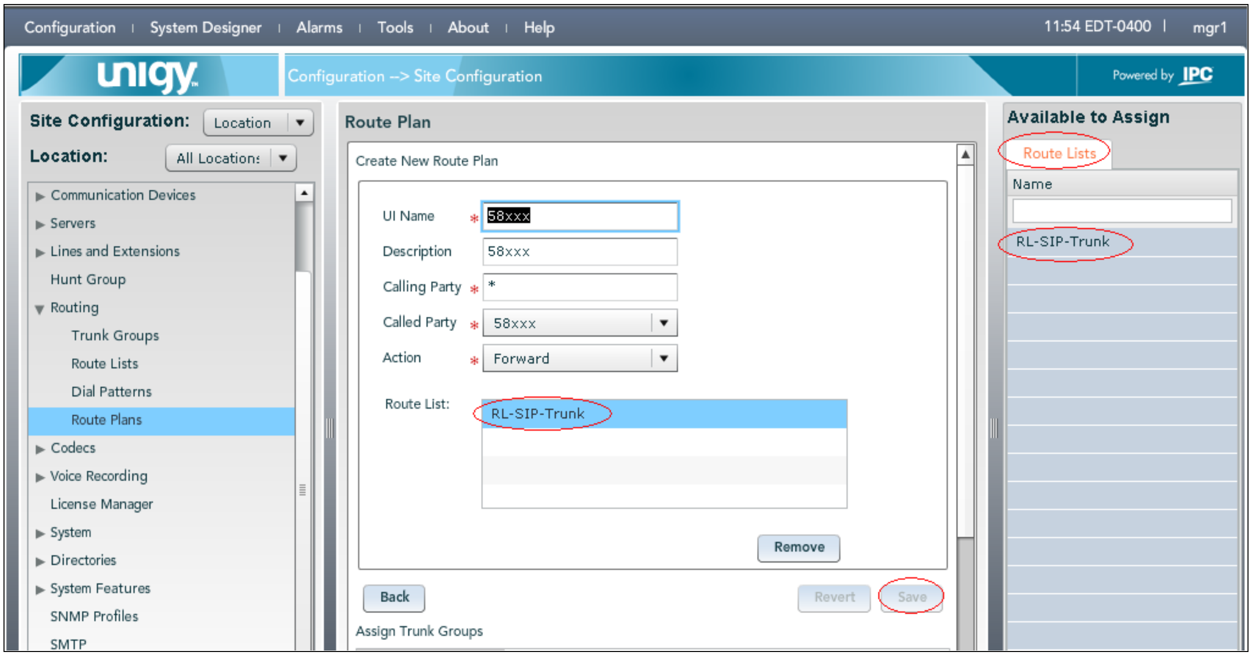

Figure 50: Adding Route List to Route Plan

Repeat this section to add another route plan for the PSTN. During compliance testing, two route plans were created as shown in **Figure 51** below.

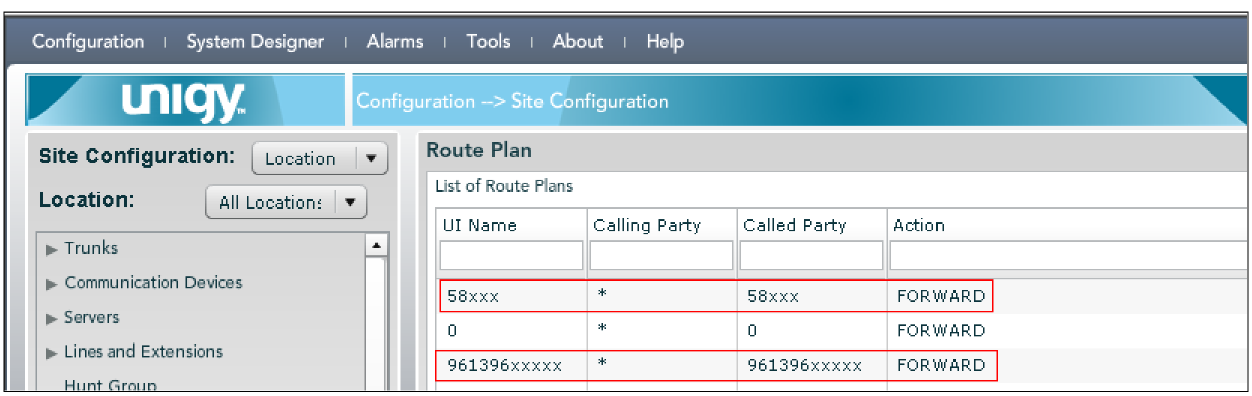

Figure 51: Extension and PSTN Route Plan

7.7. Administer Codecs

Select **Codecs > Codecs** in the left pane, and click the **"+"** icon in the lower left pane to add a new codec as shown in **Figure 52** below.

Enter a **Name** for the Codec, select a codec **Type** from the drop down and enter 20 for the **Packet Period.** Click on **Save** to complete the configuration. **Figure 52** below shows the G.711 u-law codec being added. Similarly another codec for G.729 can be added.

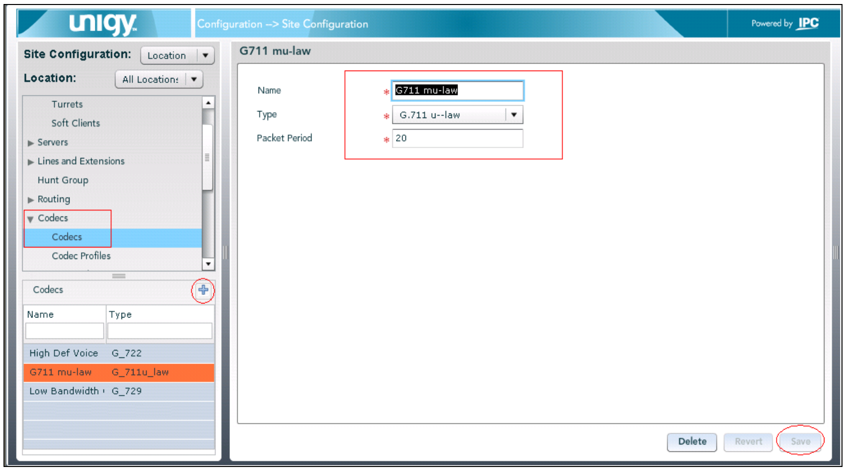

Figure 52: Adding a Codec

The two codecs added above will be used during compliance testing however they need to be included into a codec profile. Select **Codecs > Codec Profiles** and click on "+" to add a new profile. **Figure 53** below shows a profile that has been added during compliance testing called **Avaya-Codecs** and **G711 a-law** and **G.729** codecs has been added to this profile by dragging it into the middle pane from the right pane. Click on **Save** to complete this configuration.

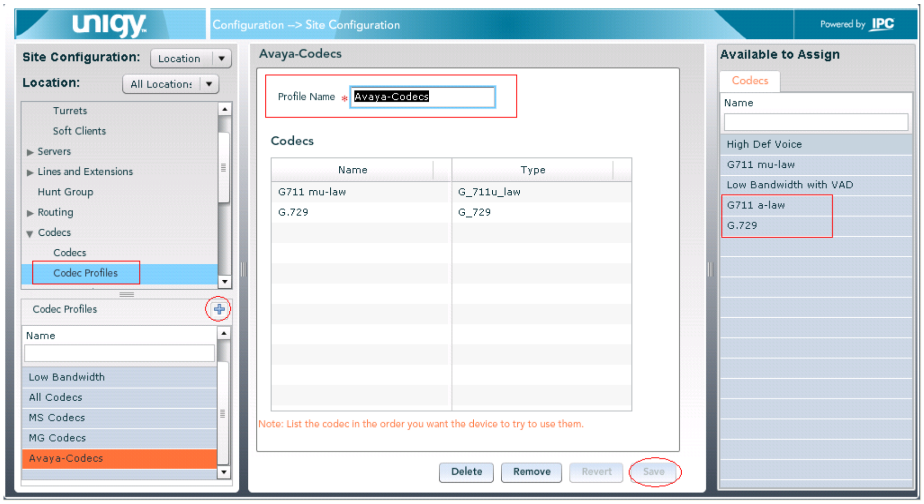

Figure 54: Creating a Codec Profile

The created Codec profile needs to be added at the Turret and User level. To include this profile in a turret, select **Communication Devices > Turrets** as shown in **Figure 55** below. Select a turret and in the **VOIP Parameters** tab select the created codec profile from the drop down seen under the **CODEC Profile** field. Click on **Save** to complete this configuration.

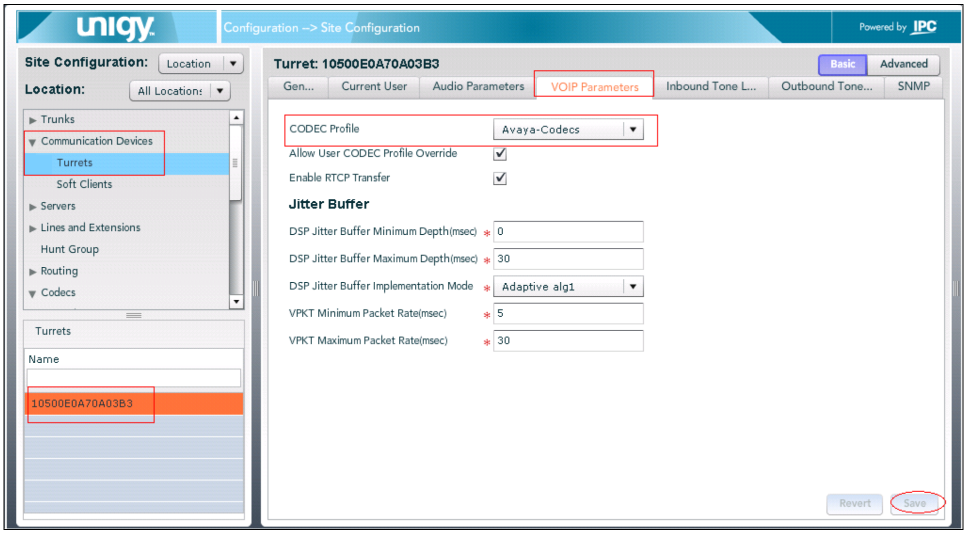

Figure 55: Selecting CODEC Profile for a Turret

To include this profile in a user, navigate to **System Designer > End User Configuration**. Select a user and access the **Trader Features** tab. Select the required profile from the drop down of the **CODEC Profile** field as shown below. Click on **Save** to complete the configuration.

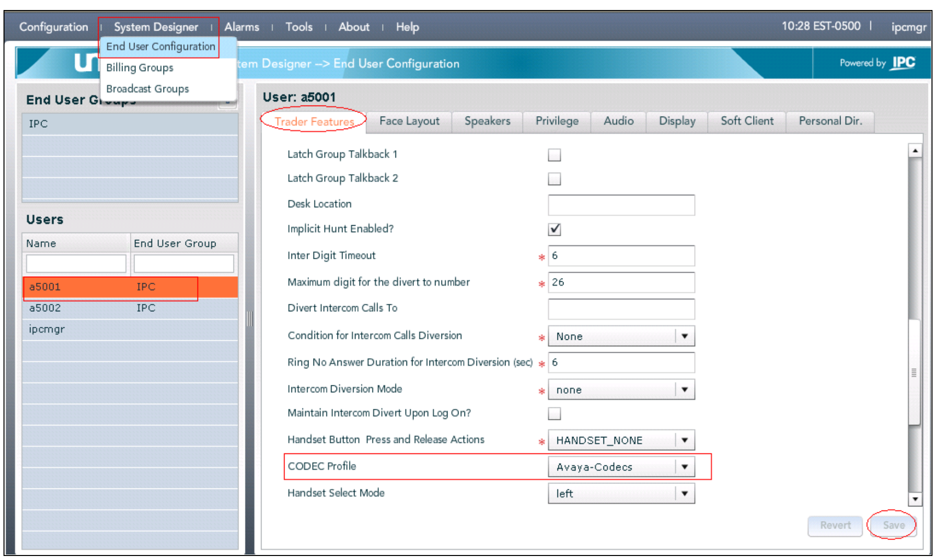

Figure 56: Selecting CODEC Profile for a User

Note that after configuring the Codecs, the turrets will need to be rebooted.

8. Verification Steps

The following tests were conducted to verify the solution between the CS1000 and Unigy system:

- All basic call features operate successfully between CS1000 and Unigy users.
- Connection between Unigy System and Avaya Aura® Session Manager is successfully established when the Ethernet connection is disconnected and connected back to the Unigy System.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy to successfully interoperate with Avaya Communication Server 1000 7.5 using SIP trunks. All executed test cases have passed and met the objectives outlined in **Section 2** along with the observations as noted in **Section 2.2**. The Unigy System is considered compliant with Avaya CS1000 Release 7.5 using Avaya Aura®.

10. Additional References

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

1. *CS1000 7.50 Administering and System Programming documents*, available at http://support.avaya.com.

2. *Unigy 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

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.