Avaya Solution & Interoperability Test Lab

Application Notes for IPC System Interconnect Alliance 16.02 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 System Interconnect Alliance 16.02 to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

IPC System Interconnect Alliance is a trading communication solution. In the compliance testing, IPC System Interconnect Alliance 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 Alliance 16.02 to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

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

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among Alliance turret users with Communication Server 1000 SIP, 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 Alliance.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

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

2.2. Test Results

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

- Alliance does not support G.722 codec negotiation.
- Alliance sets intermittently show all zeroes in the Calling Line ID (CLID) display while making outgoing calls to a PSTN set.
- Alliance Set A calls Alliance Set B invoking suppressed CLID. Set B is Forward No Answer to Avaya Set C. Set C sees Set B number in the CLID display when the set is ringing however when Set C answers the call, Set B CLID disappears.
- Alliance Set A calls Alliance Set B invoking suppressed CLID. Set B is forward no answer to PSTN. PSTN sees Set B number in the CLID display when the set is ringing and even after answering the call.

- Alliance Set A calls Avaya Set B which has calls forward no answer to Alliance Set C which has all calls forward to a PSTN number. Even though Alliance document claims to use UDP protocol only, during diversions like the example mentioned above, it changes protocol to TCP. Therefore for calls to be successful, Avaya Aura® Session Manager needs to be configured for both UDP and TCP protocols while integrating with Alliance system. Detail configuration is explained in **Section 6**.

2.3. Support

Technical support on IPC Alliance 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, Alliance configuration consists of the IPC Alliance MX, IPC System Center, IPC Enterprise SIP Server and Turrets.

Alliance, Communication Server 1000 and Avaya Aura® Session Manager are connected to each other through the lab network. SIP trunks are used from Alliance to Avaya Communication Server 1000 via the Avaya Aura® Session Manager, to reach users on Communication Server 1000 and on the PSTN. Communication Server 1000 is connected to Call Pilot (for voicemail) using proprietary Application Module Link (AML).

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Alliance and Communication Server 1000. During compliance testing, extension ranges 58xxx were associated with Communication Server 1000 users and 35xxx were associated with the Alliance turret users. Avaya Call Pilot pilot DN is 58888 and the PSTN number is 96139655570.

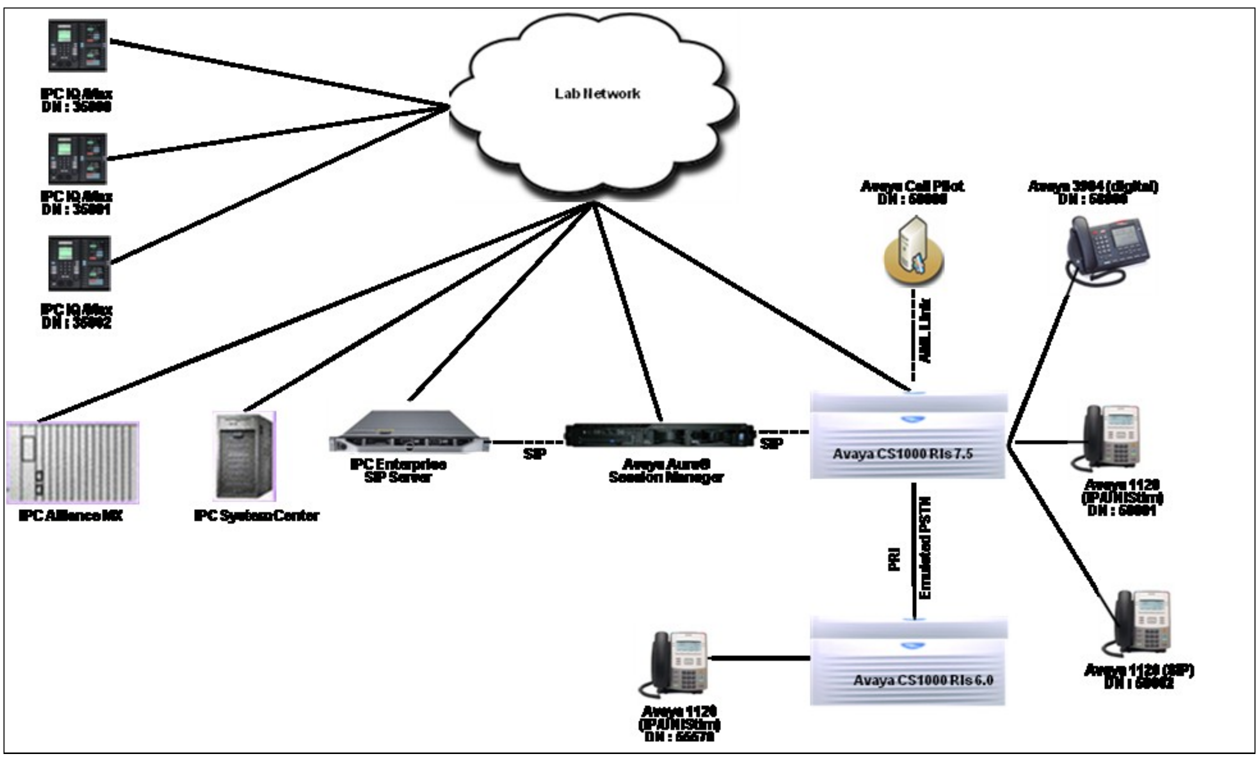

Figure 1: Compliance Test Setup in the lab

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 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 1120E IP Deskphone (UNIStim)	0624C8A
Avaya 1120E IP Deskphone (SIP)	04.01.13.00
IPC System Interconnect • SipProxy • Alliance MX • Enterprise SIP Server (ESS) • System Center o SIPX Line Card • Turrets	 2.00.01-14b 16.02.01.00.0007-1 16.02.01.00.0007-1 16.02.01.00.0007-1 16.02.01.00.0007-1

5. Configure Avaya Communication Server 1000

This section provides the procedures for configuring Avaya Communication Server 1000 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 Route and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Distant Steering Code.

Assumption is made here that the Communication Server 1000 users are already created during compliance testing. Assumption is also made that mailboxes are created in Call Pilot for Turrets. For detail configuration details of the Communication Server 1000 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 Communication Server 1000 Call Server.

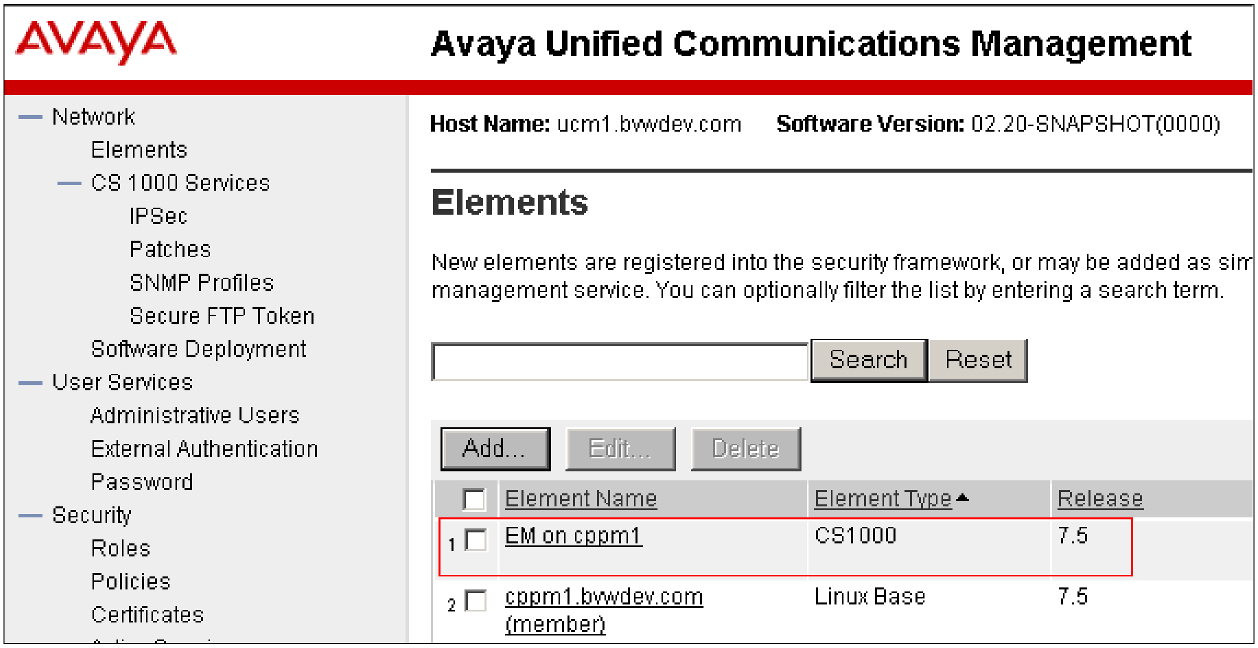

Figure 3: UCM Main Screen

5.2. Configuring the SIP Signaling Gateway

This section describes the configuration required on the SIP Signaling Gateway present on the Communication Server 1000 so that Communication Server 1000 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.

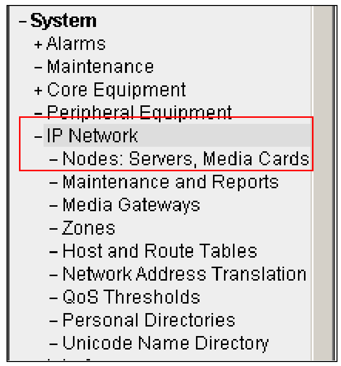

Figure 4: EM Screen showing navigation tree to Nodes

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

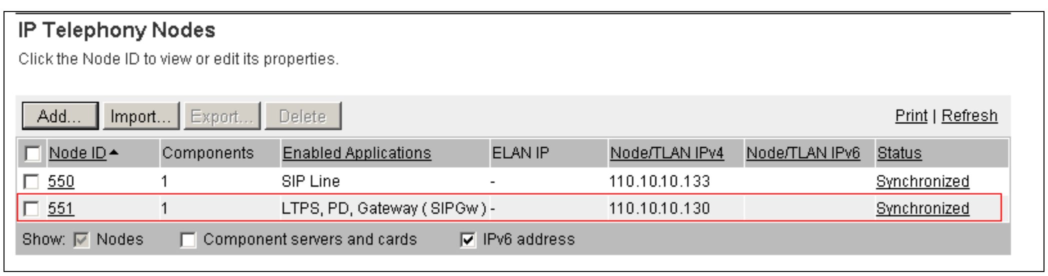

Figure 5: Accessing the Node

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

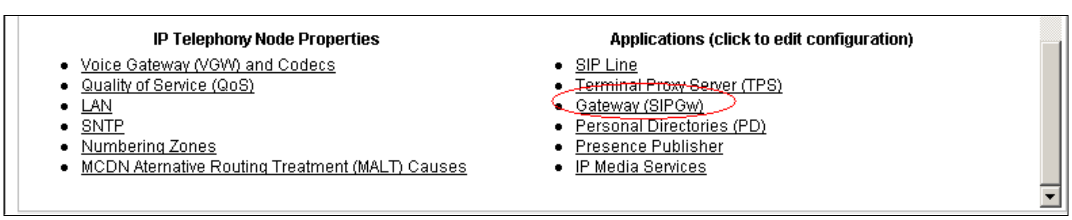

Figure 6: Accessing the SIP Signaling Gateway

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 **Gateway endpoint name**.

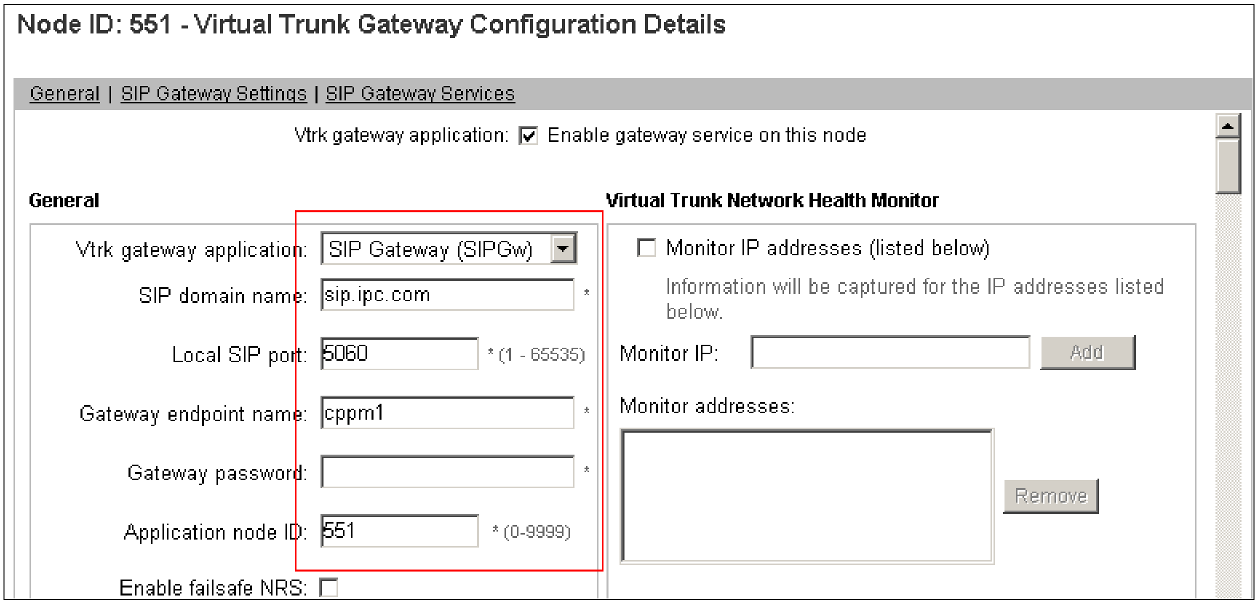

Figure 7: SIPGw General tab Configuration

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 default. During compliance testing **110.10.10.198** was the IP address of the Avaya Aura® Session Manager.

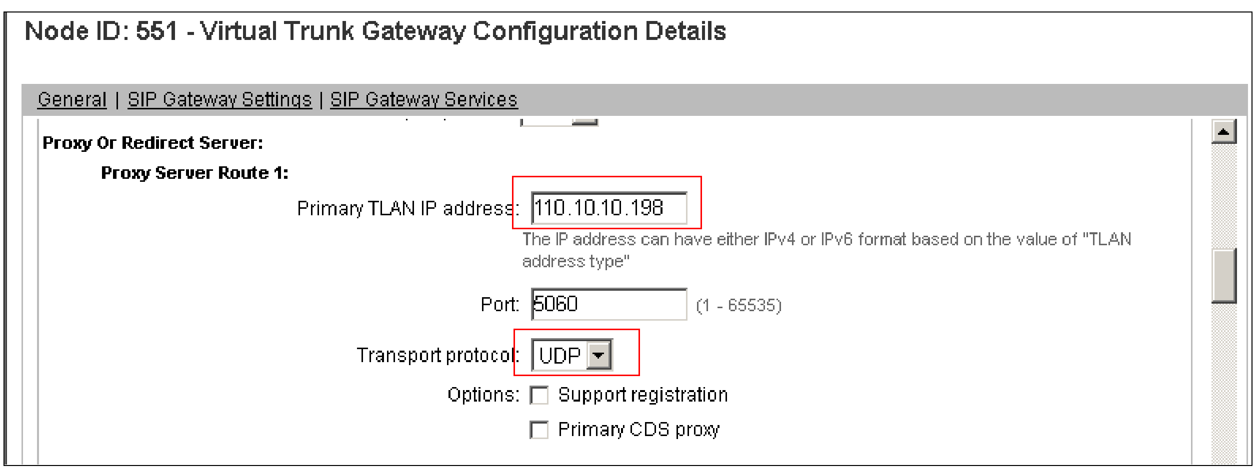

Figure 8: Proxy or Redirect Server Configuration

In the **SIP URI Map** section enter the values as shown in **Figure 9** below. These values need to be matched if integration has to be successful between Alliance and Communication Server 1000 since Alliance is only able to understand the below values in its SIP messaging properties.

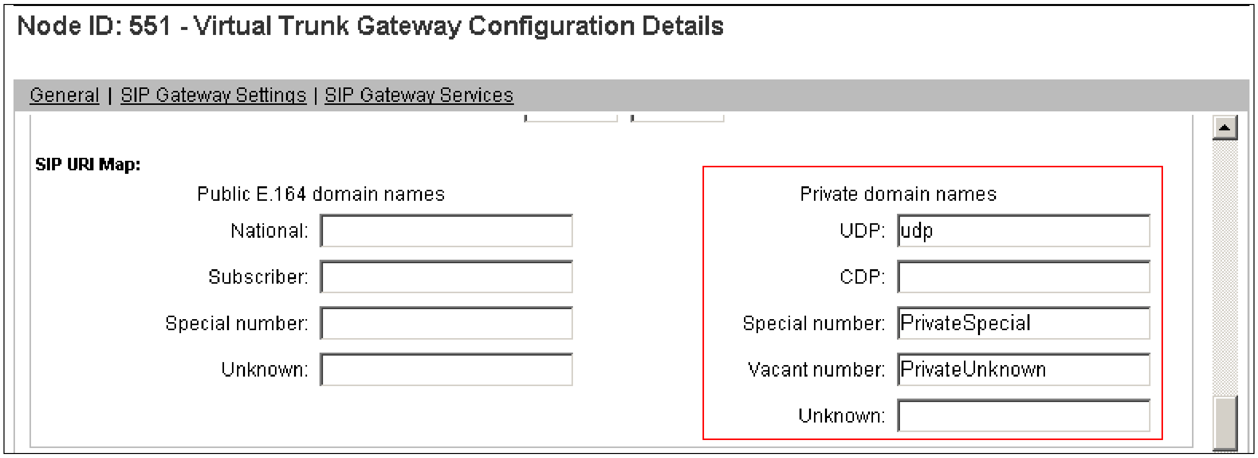

Figure 9: SIP URI Map Configuration

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

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.

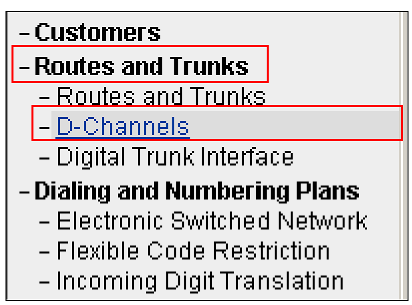

Figure 10: EM Screen showing navigation tree to D-Channels

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.

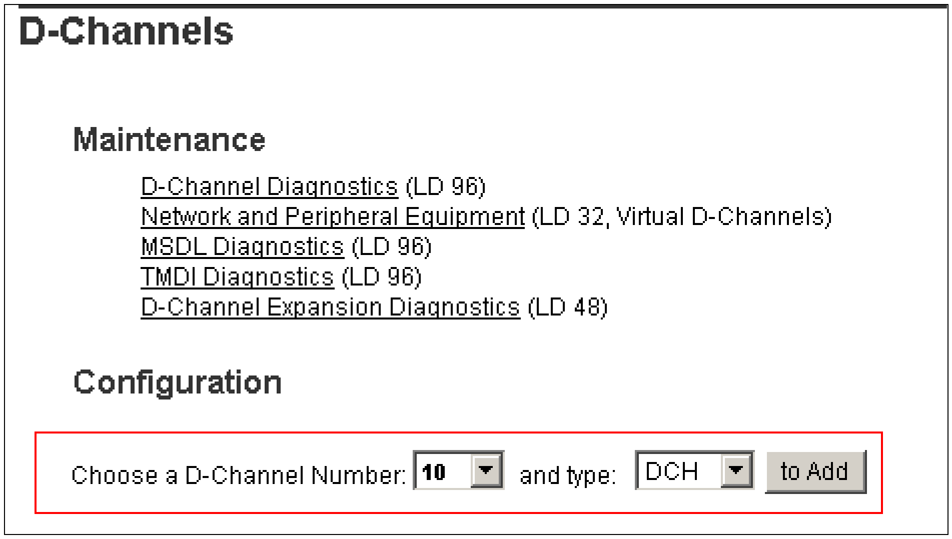

Figure 11: Adding D-Channel

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

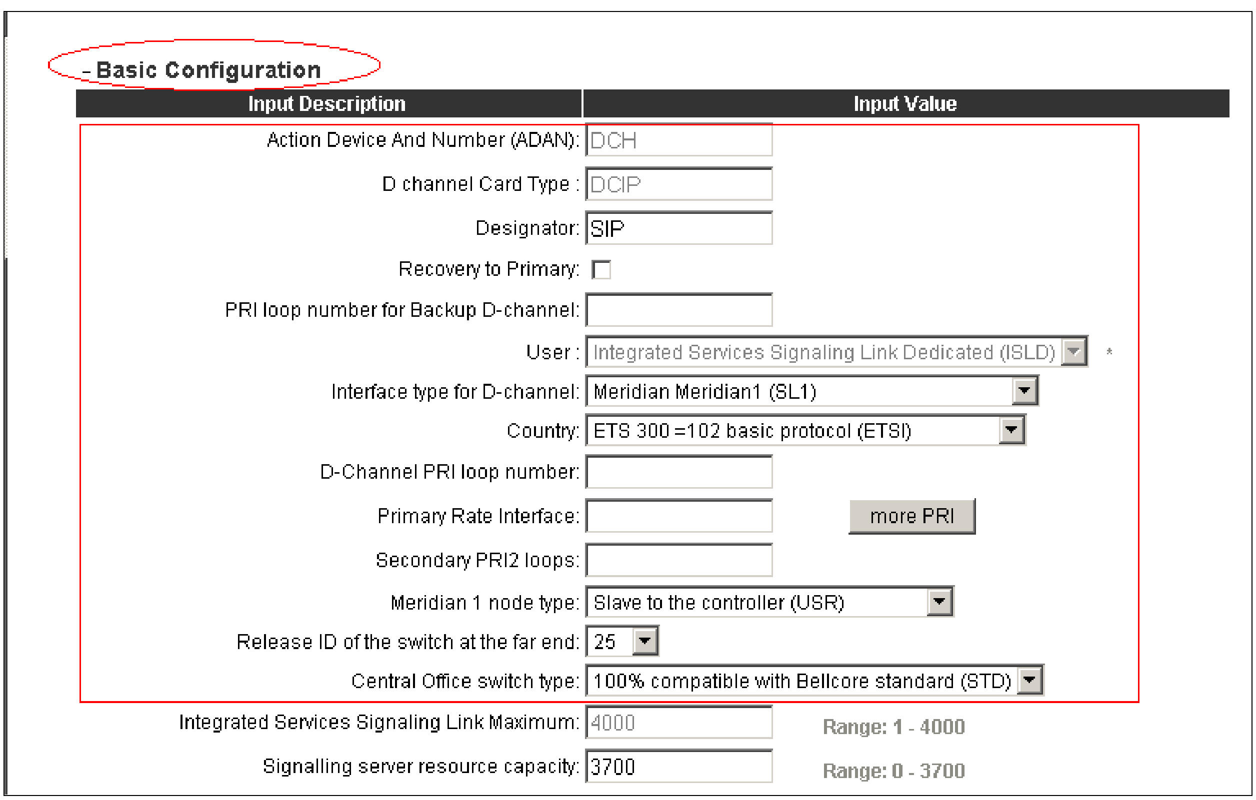

Figure 12: D-Channel Basic Configuration

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

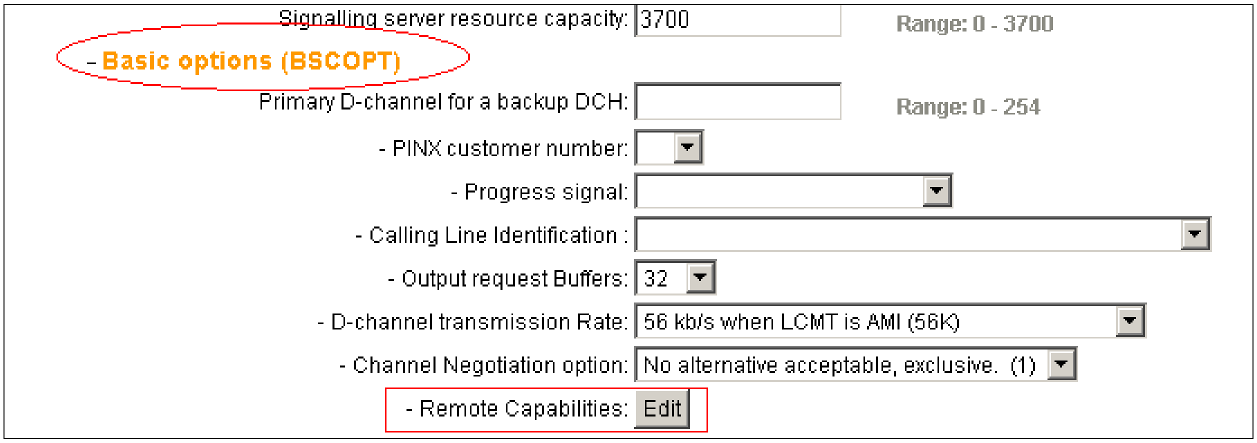

Figure 13: Editing Remote Capabilities Screen

Select the boxes values for the 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.

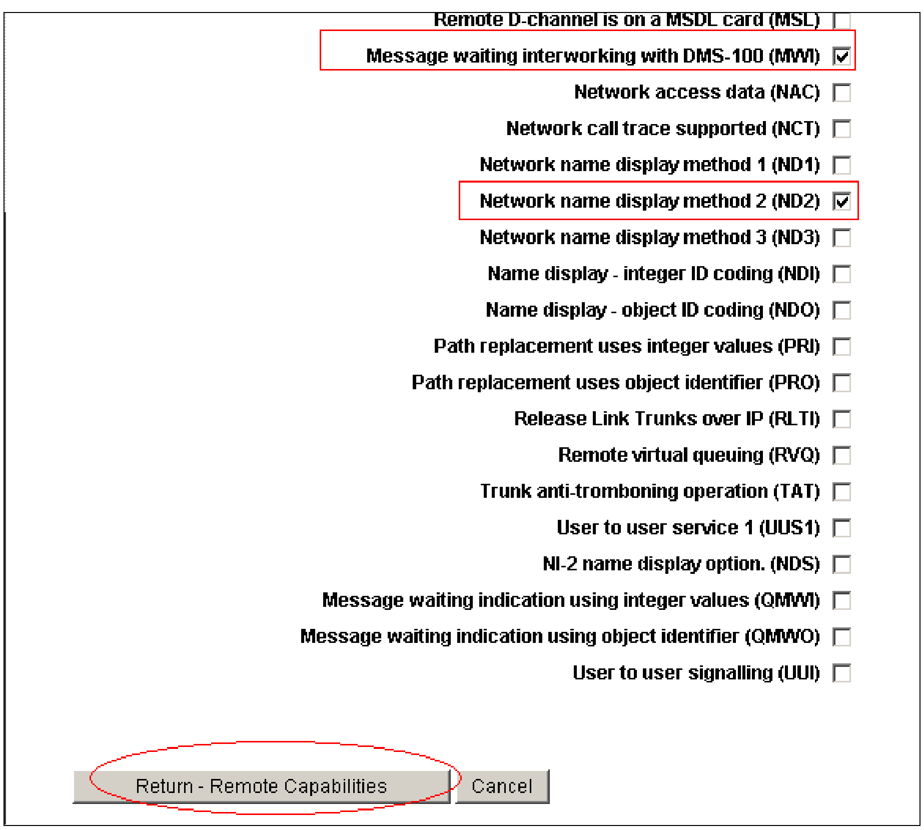

Figure 14: Remote Capabilities Values

5.4. Configuring Route and Trunks

This section explains the configuration of the SIP route and trunks which will be used by Communication Server 1000 and Alliance 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.

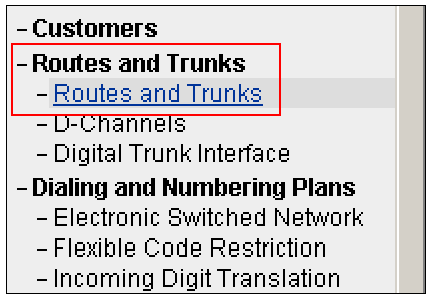

Figure 15: EM Screen showing navigation tree to Routes and Trunks

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

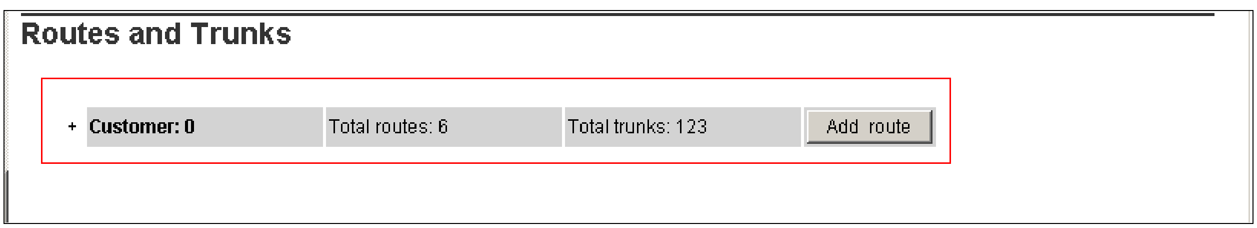

Figure 16: Adding a new Route

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.

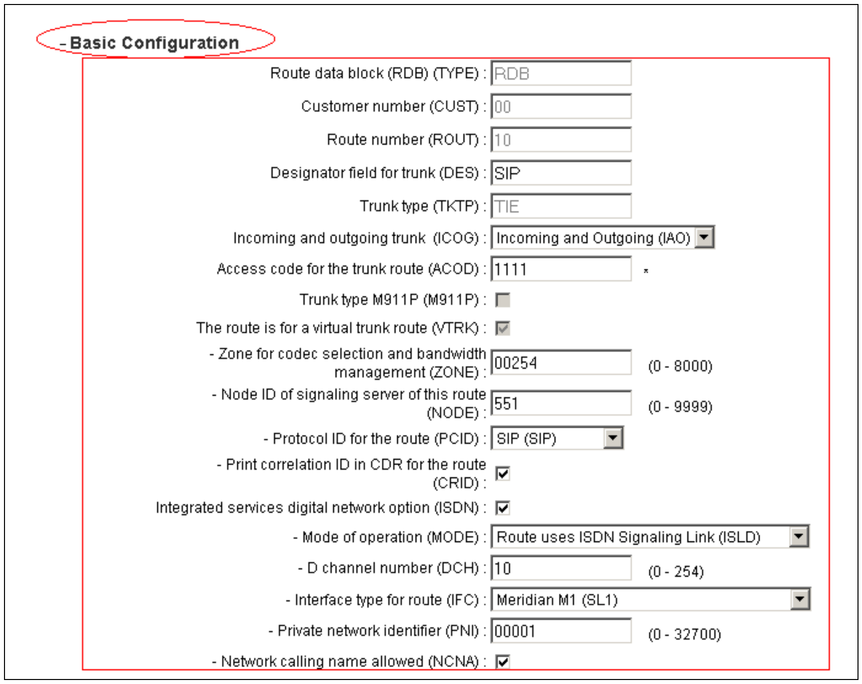

Figure 17a: Route Basic Configuration values

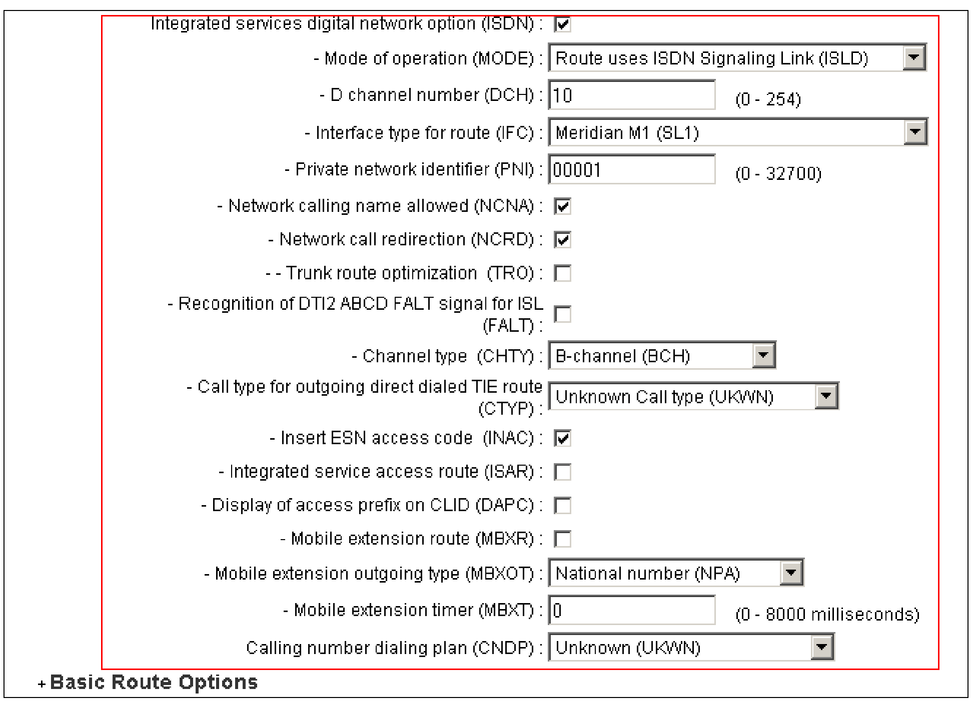

Figure 17b: Route Network Options values

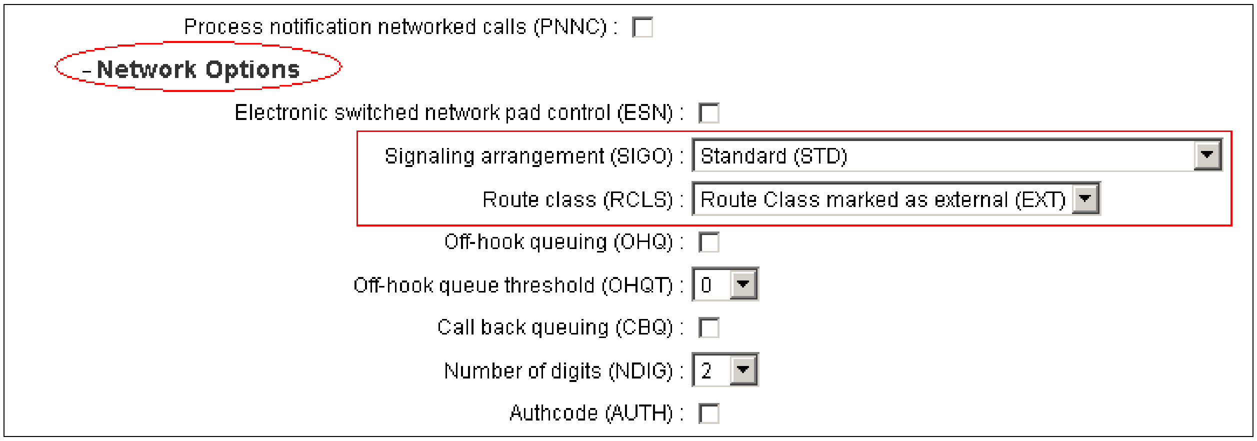

Figure 17c: Route Network Options values

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

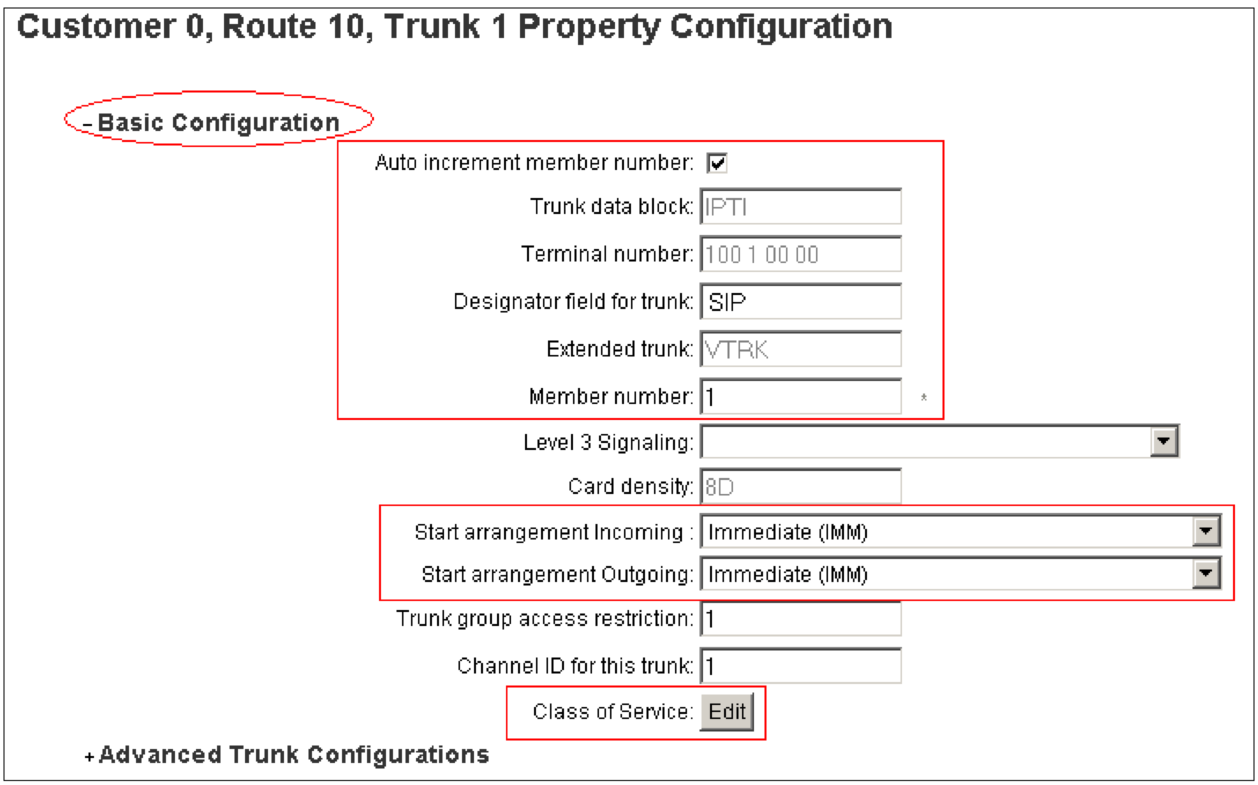

Figure 18: Trunk Properties

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 (not shown) to complete the trunks configuration.

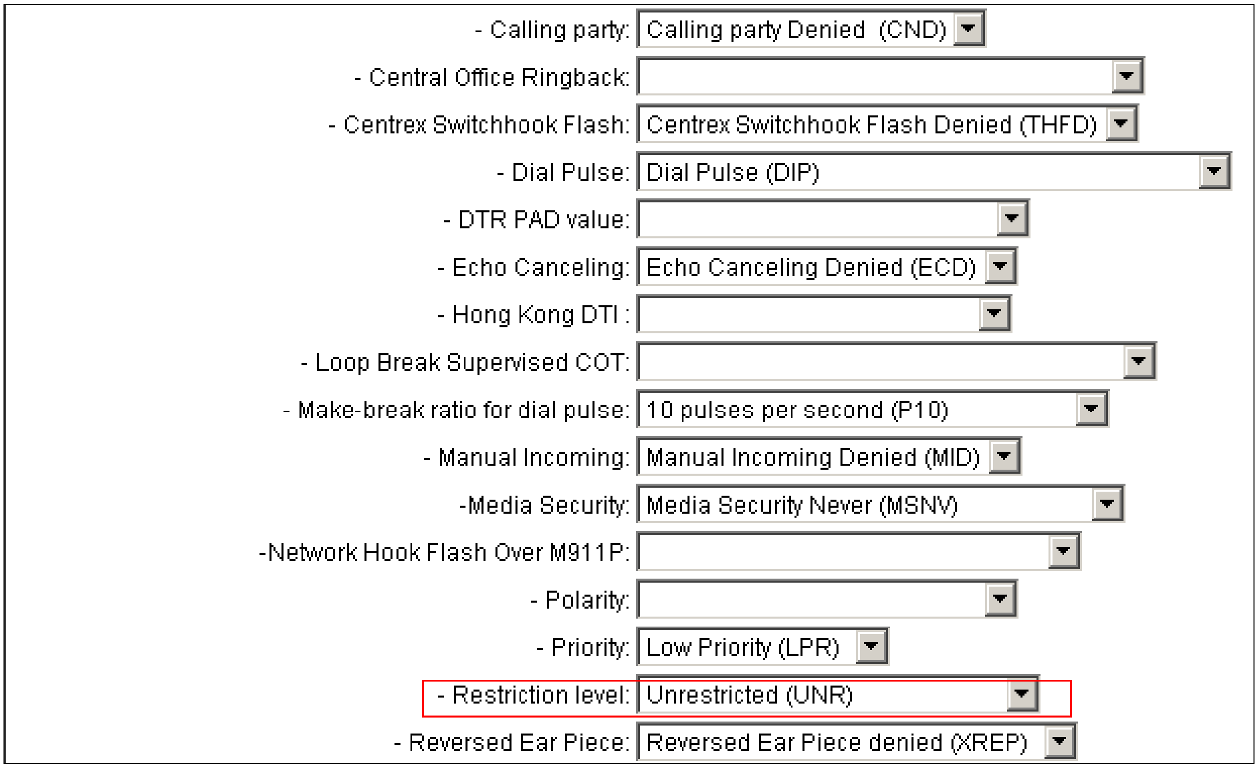

Figure 19: Trunk Class of Service

5.5. Configuring Digit Manipulation Block

This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Alliance system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** below.

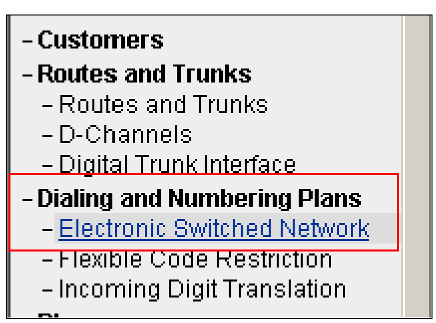

Figure 20: EM Screen showing navigation tree to Electronic Switched Network

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

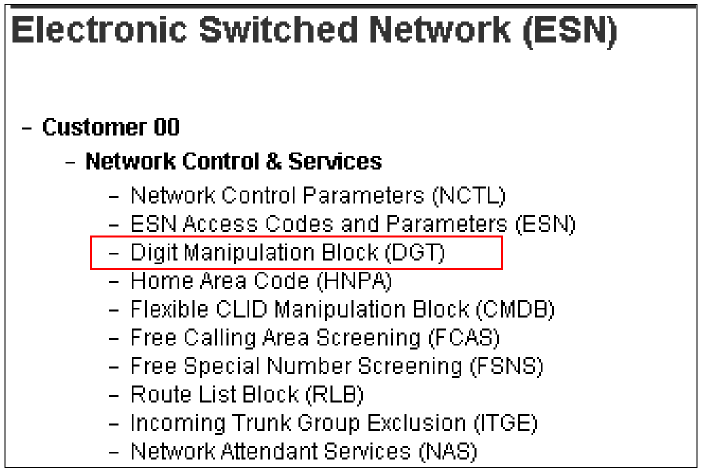

Figure 21: Accessing Digit Manipulation Block

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 Communication Server 1000 system by default.

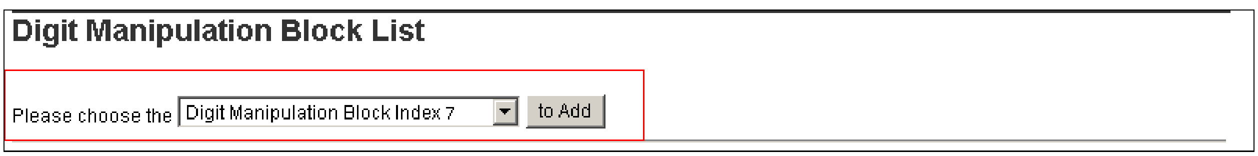

Figure 22: Adding a Digit Manipulation Block Index

5.6. Configuring Route List Block

This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Alliance 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.

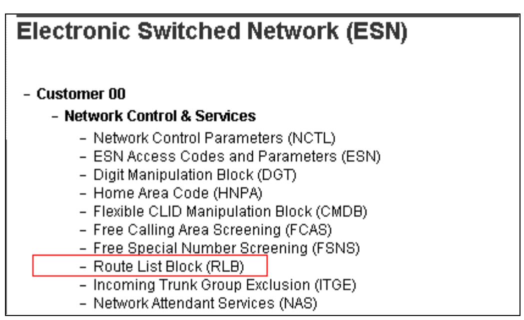

Figure 23: Accessing Route List Block

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.

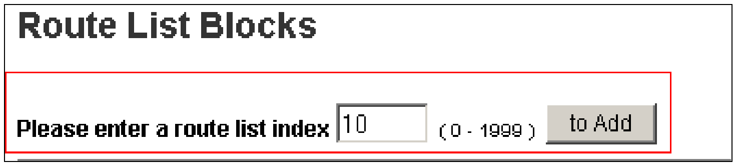

Figure 24: Adding Route List Index

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

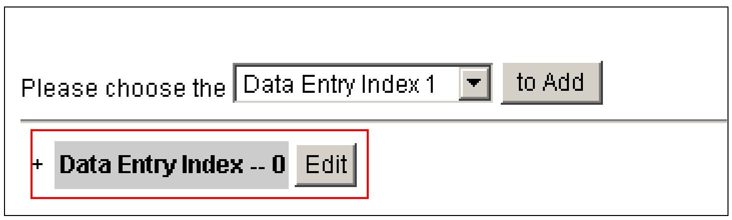

Figure 25: Adding Data Entry Index

Figure 26 below show the values configured for the index block used during compliance testing. **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.

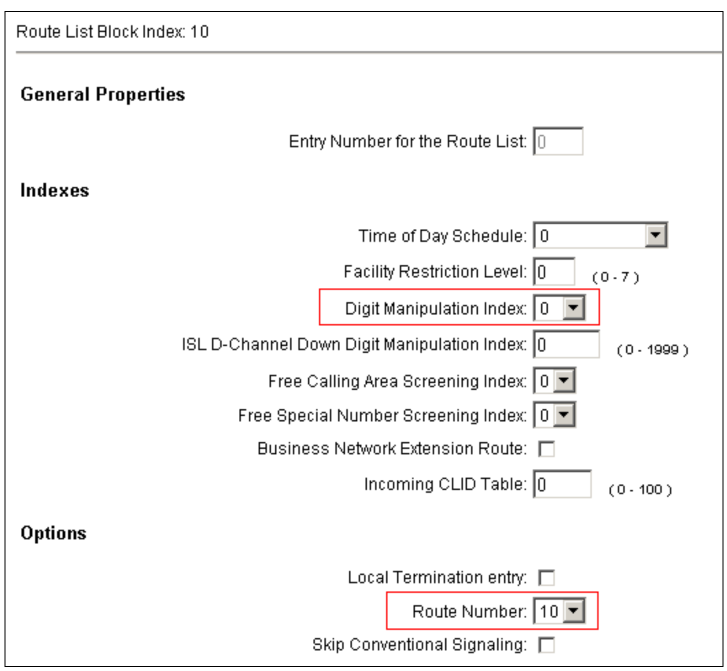

Figure 26: Route List Block properties

5.7. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Alliance system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** above. Click on **Distant Steering Code (DSC)** option as shown in **Figure 27** below.

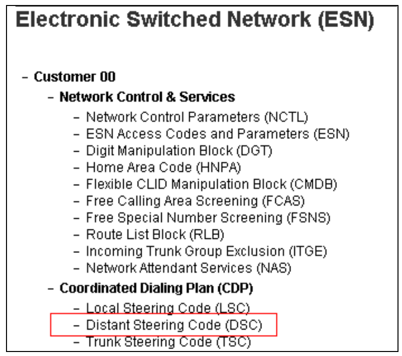

Figure 27: Accessing Distant Steering Code

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 Alliance 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 **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.

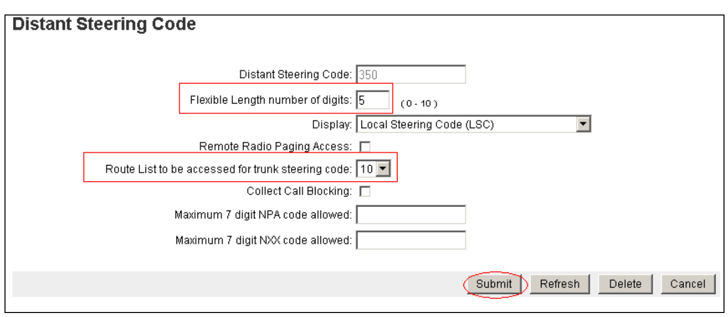

Figure 29: Distant Steering Code properties

6. Configure 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 Domain.
- Adding 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 the System Manager and accessing the Network Routing Policy.

To launch the System Manager Login screen, start an IE browser and type the IP address of the 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 on **Log On** to continue.

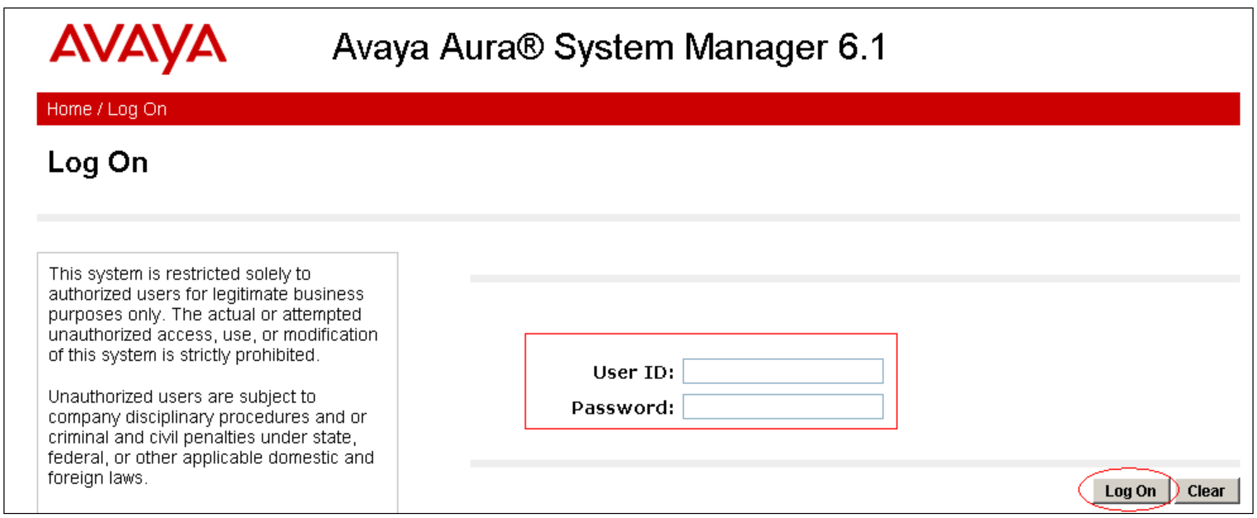

Figure 30: Avaya Aura® System Manager Login Screen

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

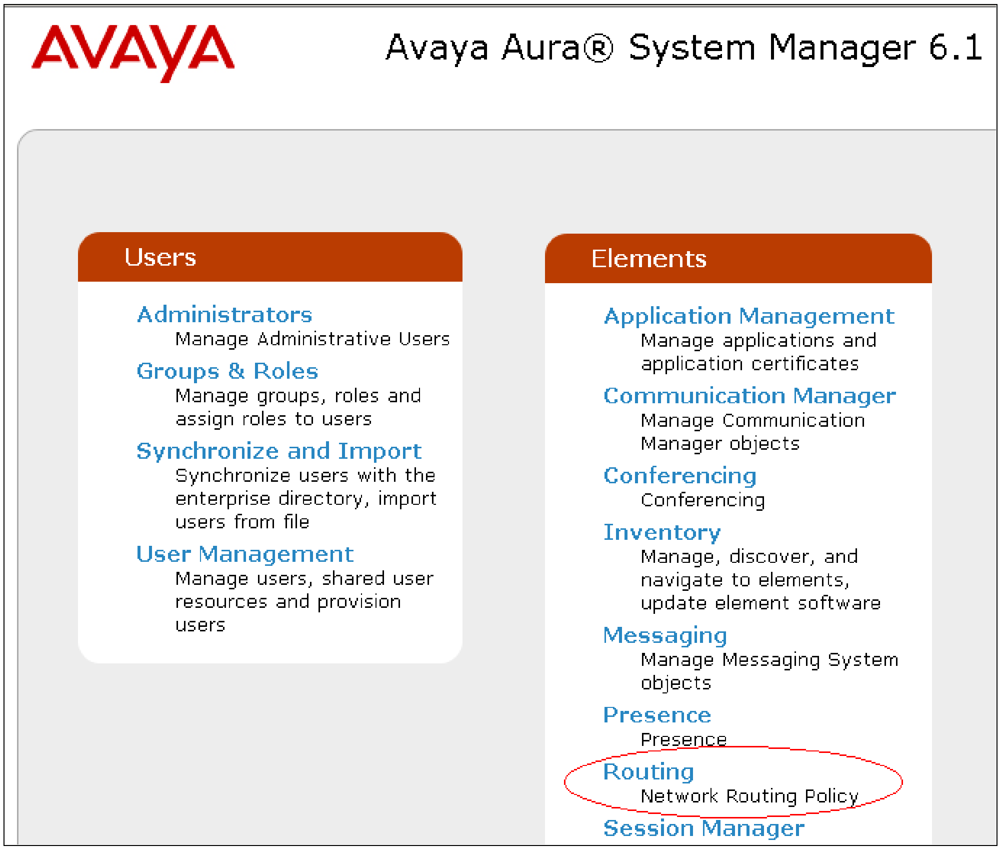

Figure 31: Avaya Aura® System Manager Main Screen

6.2. Adding Domain

To add a domain, select **Domains** from the left hand window of the Routing screen and click on **New** (not shown). Configure the **Name** 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.

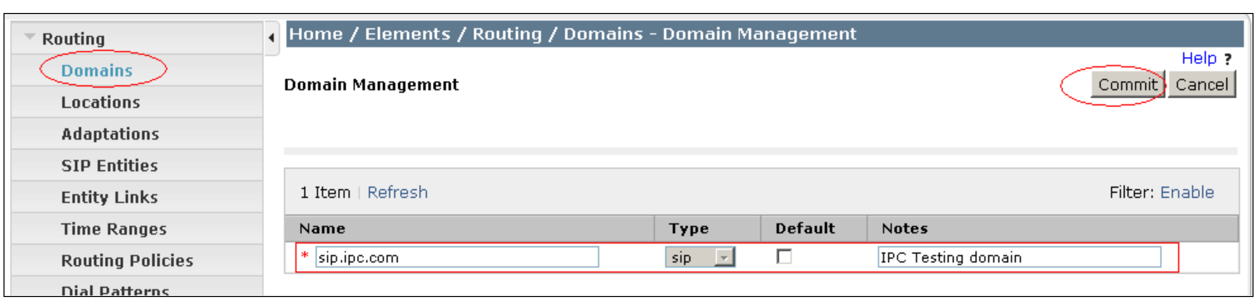

Figure 32: Domain Management

6.3. Adding Location

To add a location, select **Locations** from the left hand window of the Routing screen and click on **New** (not shown). Configure the **Name** as shown in **Figure 33** below and click on **Commit** to add a Domain. 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 for the Session Manager, Alliance System and the Communication Server 1000 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 **IPC** and **sip.ipc.com** since Alliance 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.

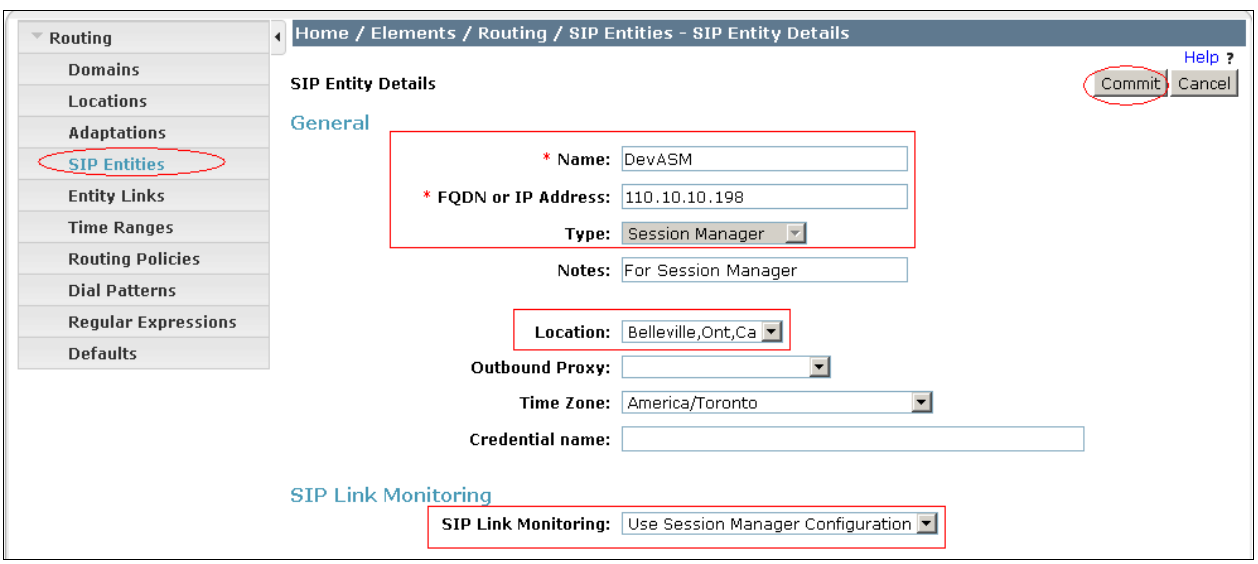

Figure 34a: SIP Entity Details for Session Manager

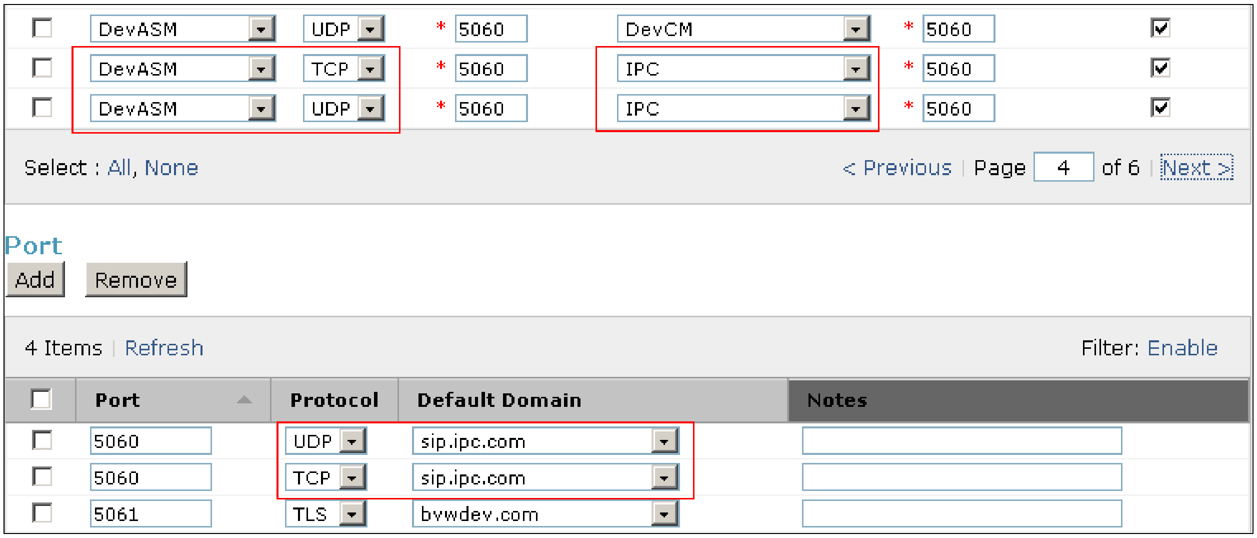

Figure 34b: SIP Entity Details for Session Manager (cont'd)

Figures 35a and **35b** show the SIP Entity Details for the Alliance System routing. The **FQDN or IP Address** of **110.10.10.226** is the IP address of the Alliance System. Also note that both **TCP** and **UDP** protocols need to be selected for **IPC** since Alliance 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.

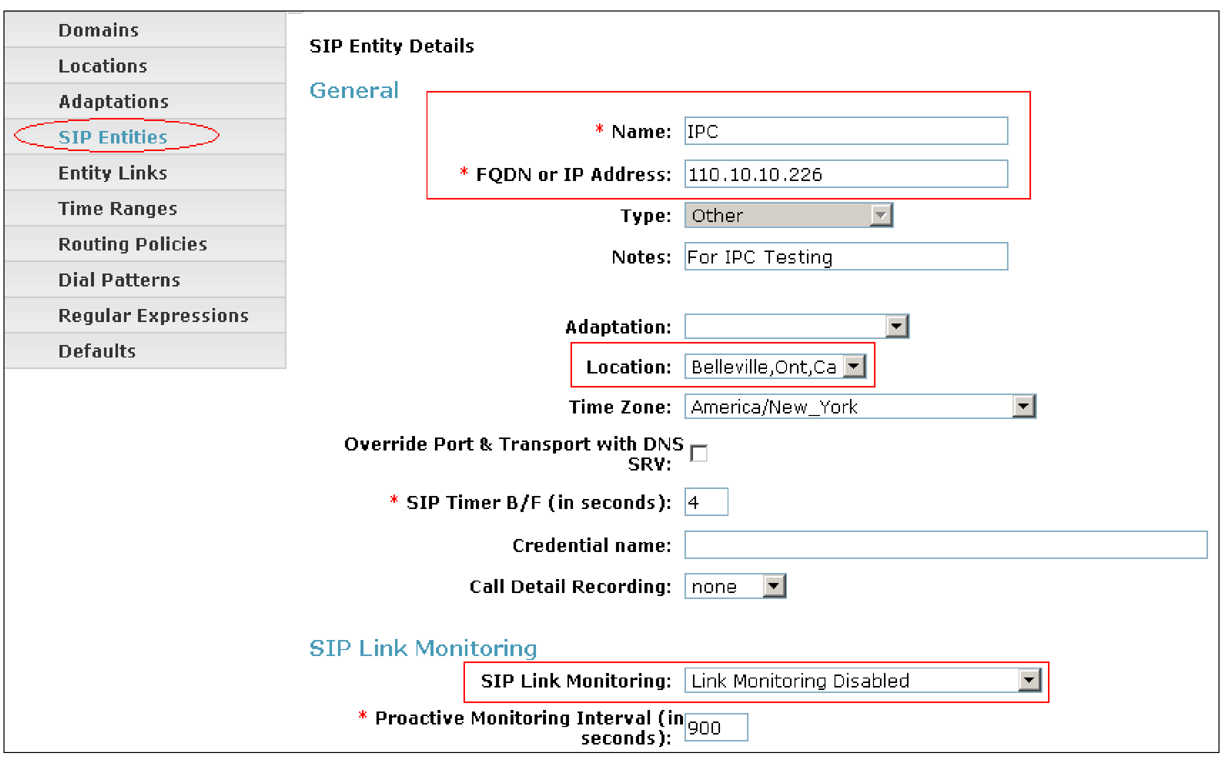

Figure 35a: SIP Entity Details for Alliance System

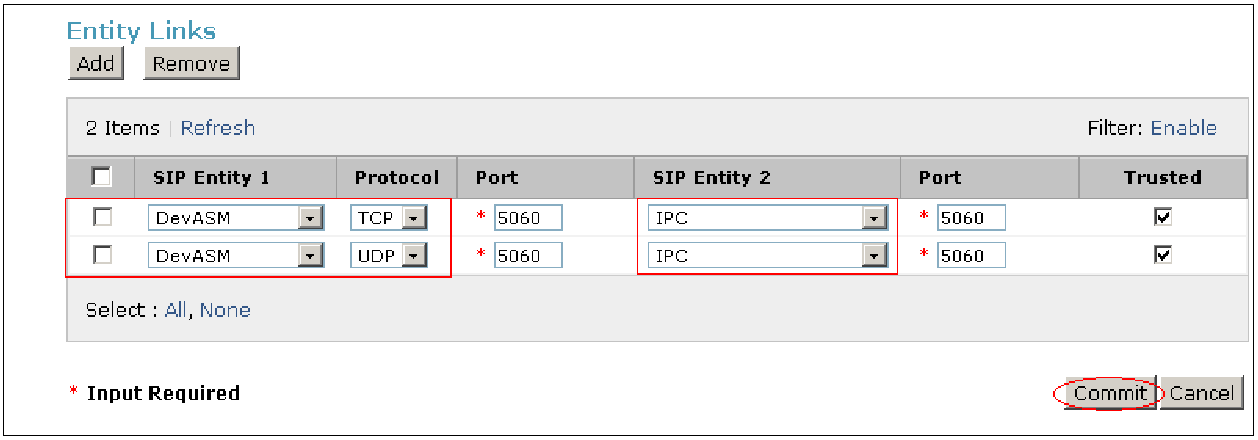

Figure 35b: SIP Entity Details for Alliance System (cont'd)

Figures 36a and **36b** show the SIP Entity Details for the Communication Server 1000 System routing. The **FQDN or IP Address** of **110.10.10.130** is the Node IP address of the SIP Signaling Gateway of the Communication Server 1000 System. Click on **Commit** to complete adding the SIP Entity.

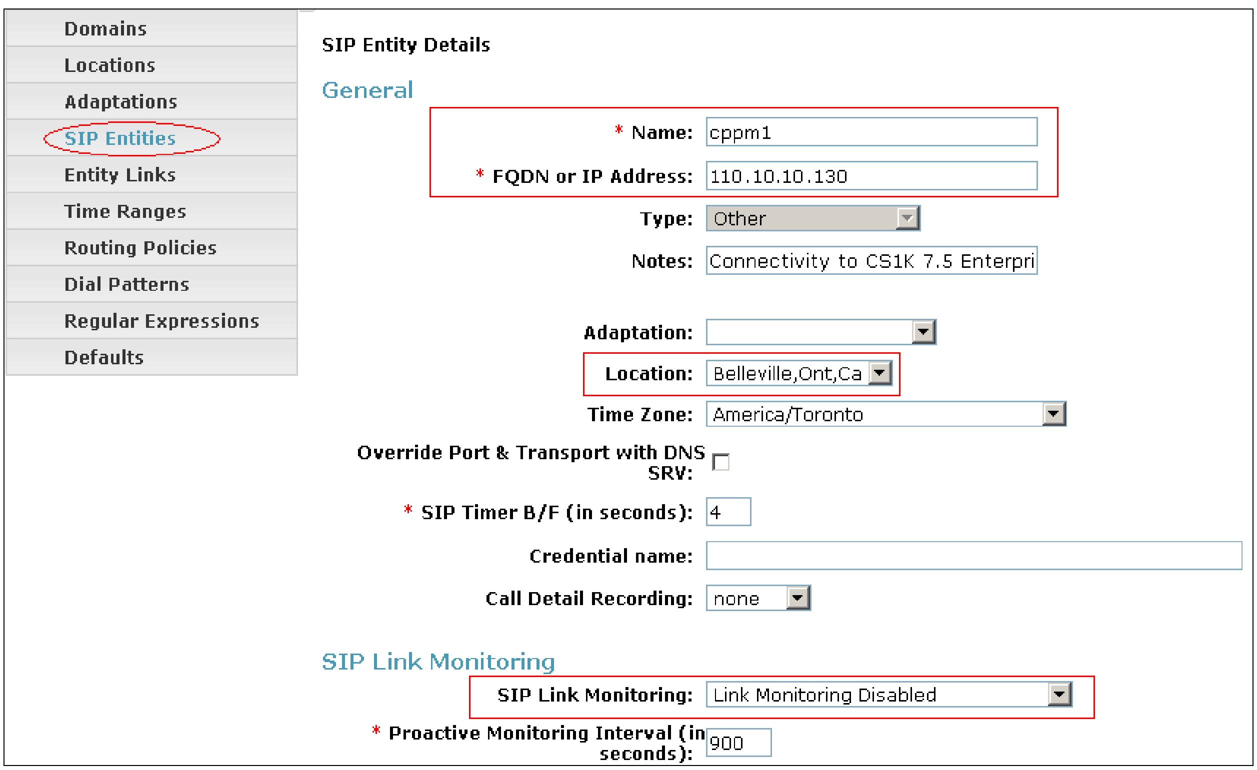

Figure 36a: SIP Entity Details for Communication Server 1000 System

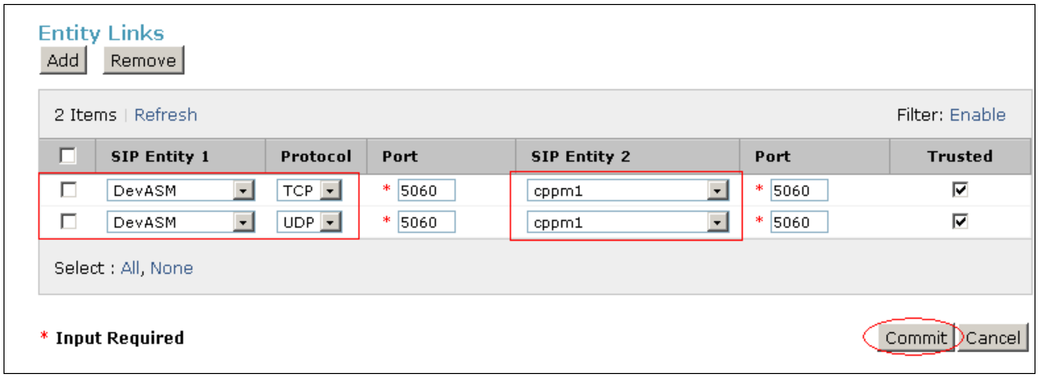

Figure 36b: SIP Entity Details for Communication Server 1000 System (cont'd)

6.5. Adding Routing Policies

This section explains the Routing Policy configuration for Alliance and Communication Server 1000 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 Alliance System. Select the Alliance System as the SIP Entity Destination and add the dial pattern associated with the Alliance 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.

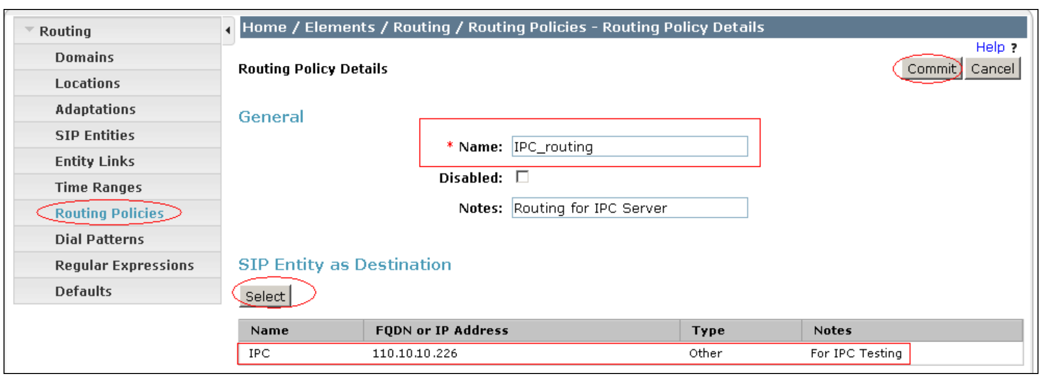

Figure 37a: Routing Policy Details for Alliance System

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

Figures 38a and **38b** show the Routing Policy Details for the Communication Server 1000 System. Select the Communication Server 1000 System as the SIP Entity Destination and add the dial pattern associated with the Communication Server 1000 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.

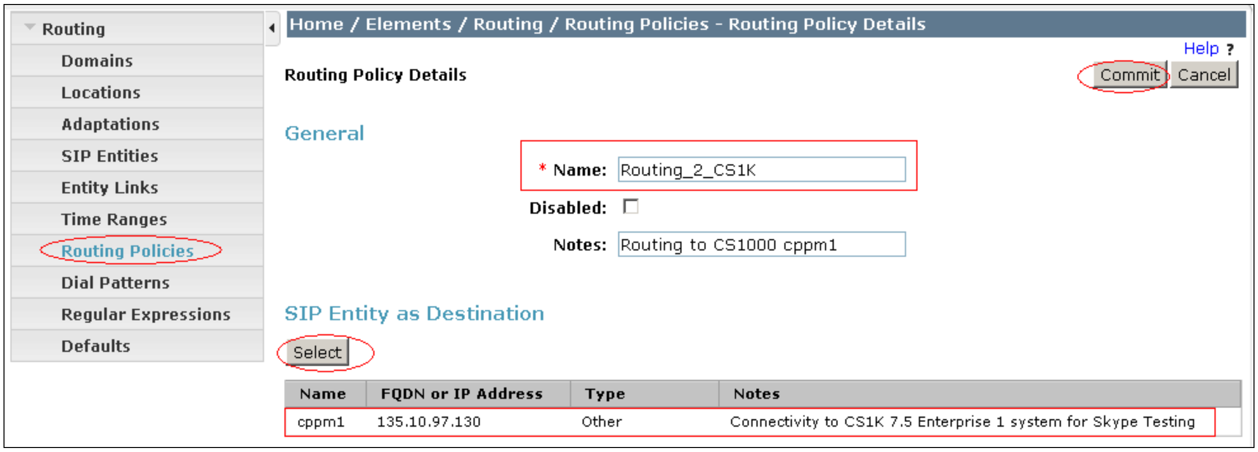

Figure 38a: Routing Policy Details for Communication Server 1000

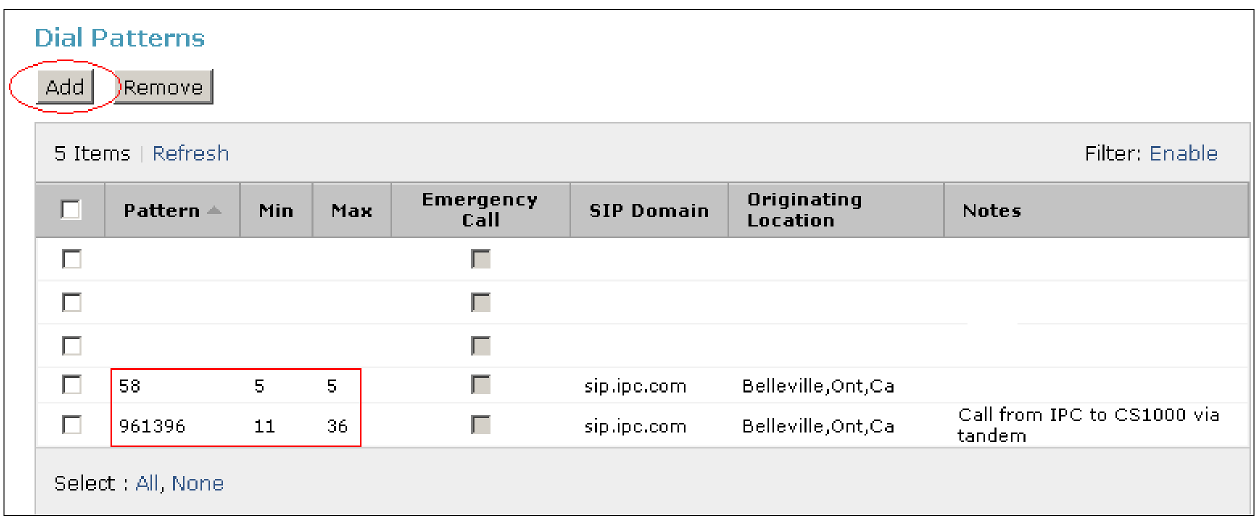

Figure 38b: Routing Policy Details for Communication Server 1000 (cont'd)

6.6. Adding Dial Patterns

This section explains the steps to add a dial pattern for the Alliance and Communication Server 1000 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 Alliance System. During compliance testing extensions range on Alliance system started with 350xx and therefore **350** are 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.

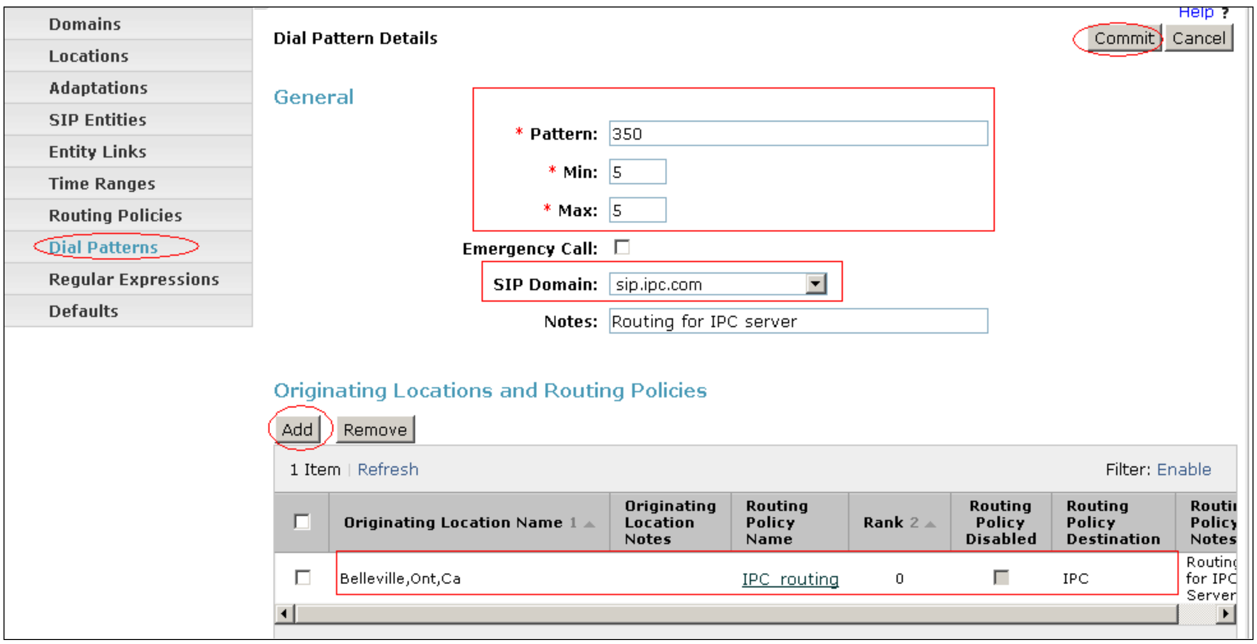

Figure 39: Dial Pattern Details

7. Configure IPC System Interconnect

This section provides the procedures for configuring IPC System Interconnect. The procedures include the following areas:

- Launch One Management System
- Administer SIP configuration
- Administer routing plan
- Administer wire groups
- Administer trusted host

The configuration of System Interconnect is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch One Management System

Access the One Management System web interface by using the URL "http://ip-address/oneview" in an Internet browser window, where "ip-address" is the IP address of IPC System Center. Log in using the appropriate credentials. The Login screen is displayed as shown in **Figure 40** below. Enter the appropriate credentials. Check **I agree to the terms and conditions**, and click **Login**. The **License Login** screen is displayed next (not shown). Enter the appropriate password and click **Login**. In the subsequent **Login Information** screen (not shown), click **Continue**.

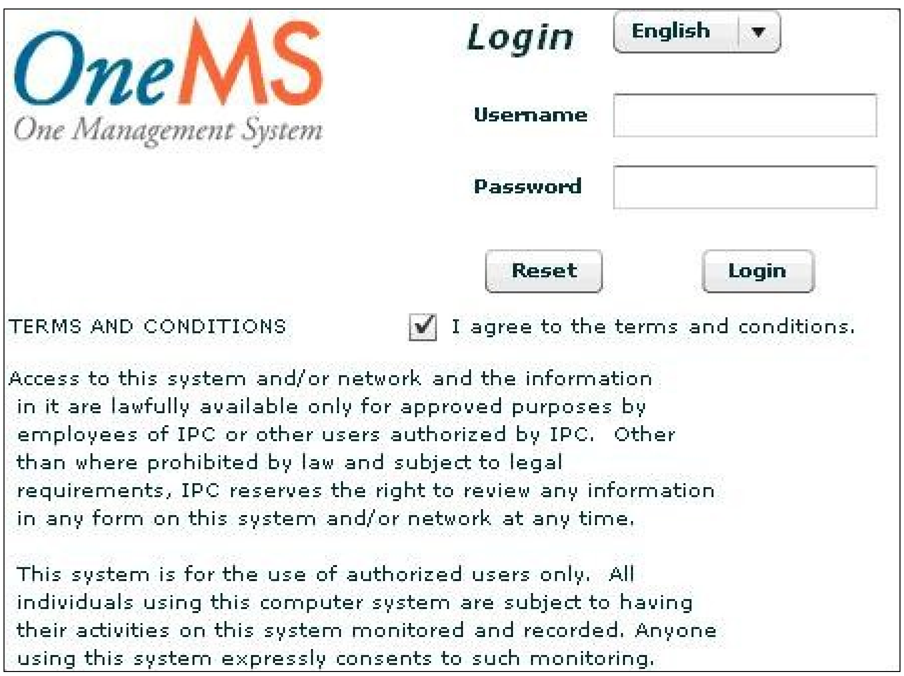

Figure 40: One Management System Login Screen

7.2. Administer SIP Configuration

The screen below in **Figure 41** is displayed next, with the Main Menu screen in the forefront. Select **NEXUS > SIP Trunk Parameters > Edit SIP Config**, as shown below.

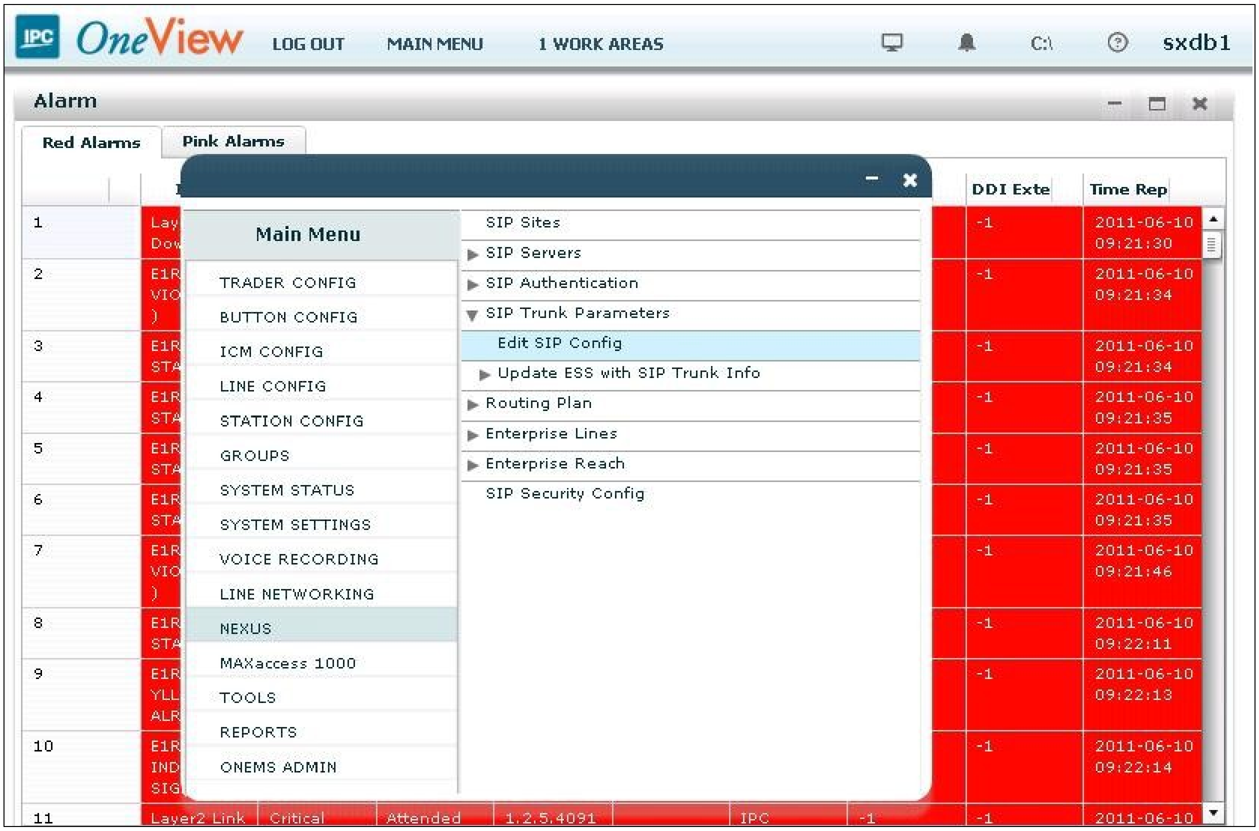

Figure 41: Main Screen

The Edit SIP Config screen is displayed as shown in **Figure 42** below. For **DDI Group ID/ DDI Group Name**, select the relevant SIP trunk card number from the drop-down list, in this case "5". Click **Submit**.

Figure 42: Edit SIP Config Screen

Figure 43 below shows the SIP Config parameters.

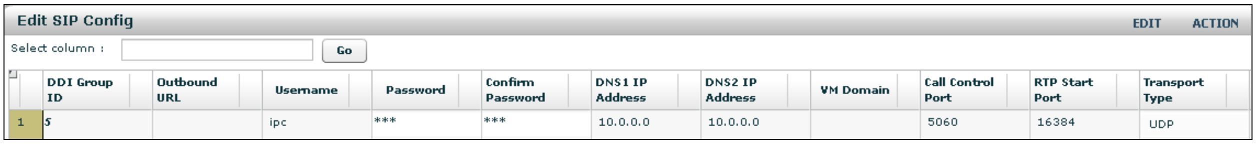

Figure 43: SIP Config Screen

7.3. Administer Routing Plan

Select **MAIN MENU** from the top menu to display the Main Menu screen. Select **NEXUS > Routing Plan > View/Edit/Delete Routing Plan**, as shown in **Figure 44** below. Click **Submit** in the subsequent screen (not shown) to search for all routing plans.

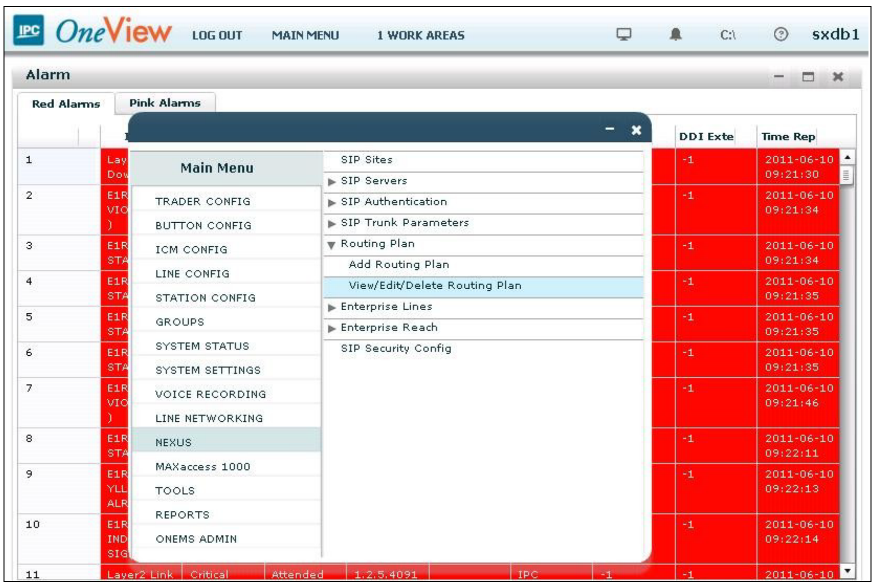

Figure 44: Routing Plan

The View/Edit/Delete Routing Plan screen as seen in **Figure 45** below is displayed. The entry with **Sequence Number 3** was used for routing of inbound calls to IPC. Note that the **Destination** URL contains the internal default value for the SIP trunk card, in this case "group5.com". The entry with **Sequence Number 4** was used for routing of outbound calls to Session Manager. Note the **Destination** URL includes the IP address of the signaling interface for Session Manager, and the transport protocol from **Section 5.2**. IPC Alliance uses UDP by default. If the protocol is other than UDP, then this needs to be added after the URL.

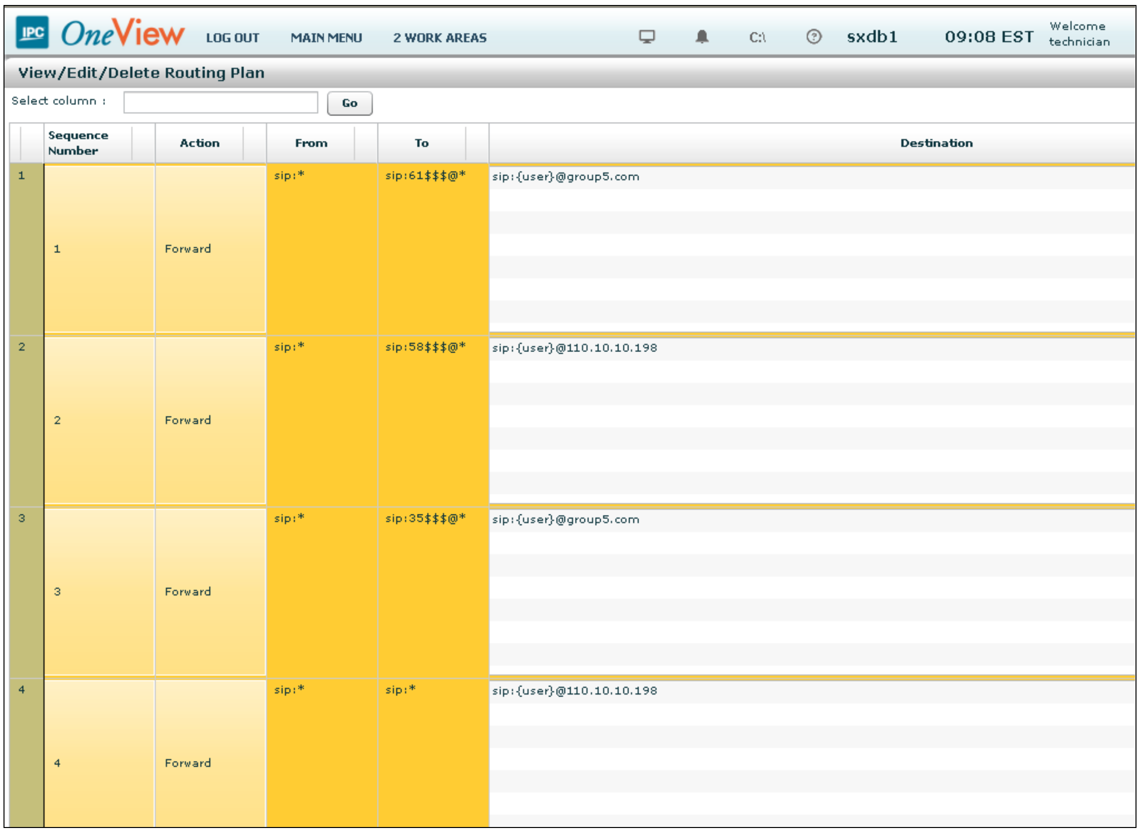

Figure 45: View/Edit/Delete Routing Plan

7.4. Administer Wire Groups

Select **MAIN MENU** from the top menu to display the Main Menu screen. Select **GROUPS > Engineering Groups > Wire Groups**, as shown in **Figure 46** below.

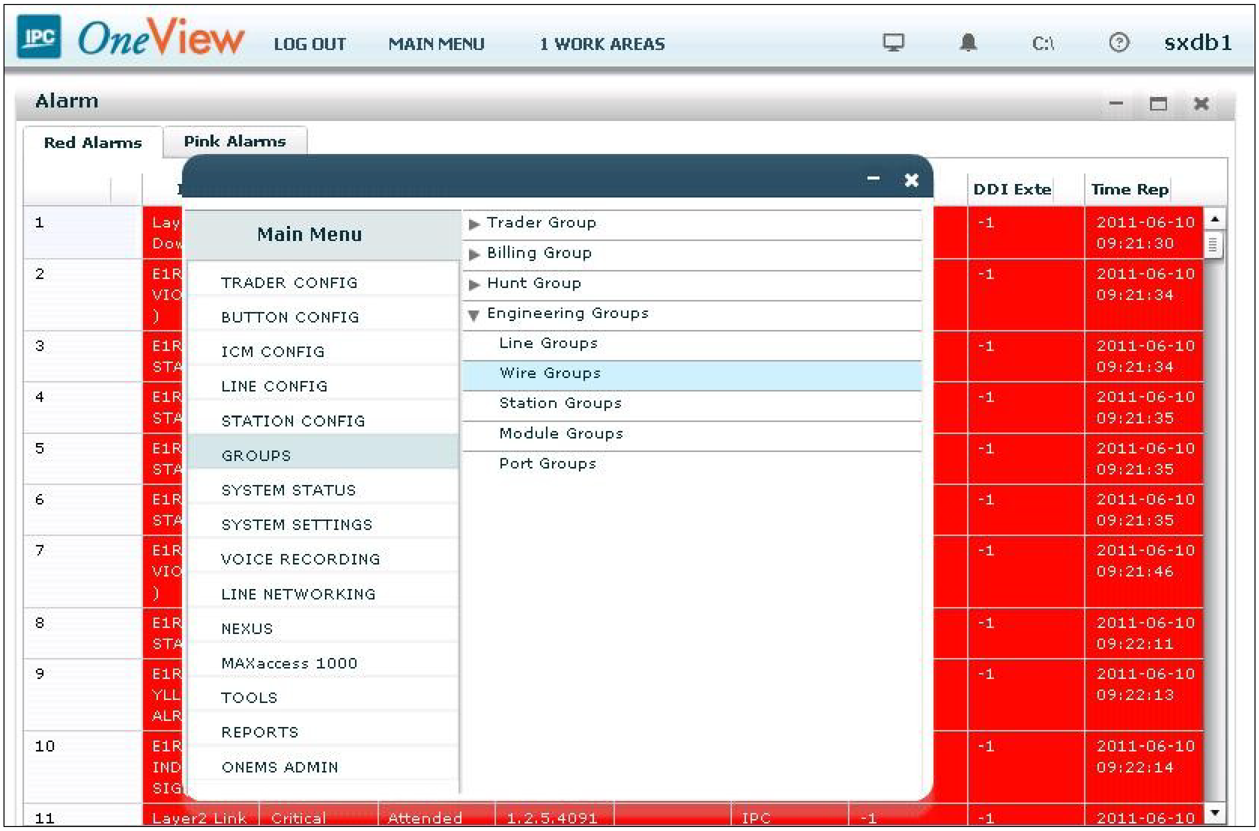

Figure 46: Wire Groups

The Wire Groups screen is displayed as shown in **Figure 47** next. Select "SIP" from the **Select Wire Group** drop-down list, and "Edit" from the **Select Operation** drop-down list, as shown below.

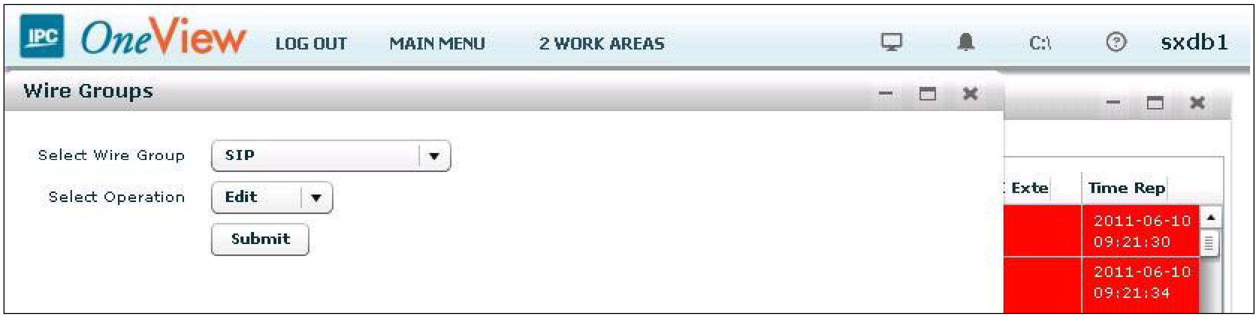

Figure 47: Wire Groups Configuration

The Edit Wire Groups screen is displayed as shown in **Figure 48** below.

- Scroll down the screen as necessary to locate the entry with **Param ID** of “365”. Double click on the corresponding **Param Value** field, and enter “3” to denote Nortel (note that IPC still uses Nortel to represent CS1000) as the PBX provider.
- Locate the entry with **Param ID** of “370”. Double click on the corresponding **Param Value** field, and enter “3”.

69	SIP	SIP	SIP Line Card	47	0	32767	DSP_VTHRESH...	Volume Thresh...	number	136	27
70	SIP	SIP	SIP Line Card	47	0	32767	DSP_VTHRESH...	Volume Thresh...	number	137	27
71	SIP	SIP	SIP Line Card	16423	1	32767	DSP_VBALANCE	DSP Volume B...	number	138	27
72	SIP	SIP	SIP Line Card	32767	1	32767	DSP_TERM_AT...	DSP TERM thre...	number	141	27
73	SIP	SIP	SIP Line Card	0	-5	5	TERM_SHIFT	gain/loss into ...	number	362	27
74	SIP	SIP	SIP Line Card	0	-5	5	PERIPH_SHIFT	gain/loss into ...	number	363	27
75	SIP	SIP	SIP Line Card	6	0	32	INTERDIGIT_TO	interdigit time...	number	364	27
76	SIP	SIP	SIP Line Card	3	1	7	PBX_PROVIDER	1-7/DEF,AVYA...	enum	365	27
77	SIP	SIP	SIP Line Card	6	1	15	MAX_DIVERTS	Max Number of...	number	369	27
78	SIP	SIP	SIP Line Card	3	0	4	FS_ENABLE	0-4/Off, Imm...	number	370	27
79	SIP	SIP	SIP Line Card	200	200	10000	FS_DELAY	Time(msec) to ...	number	371	27
80	SIP	SIP	SIP Line Card	1	1	5	LN_RECORDS	1-5/NONE,MX...	number	375	27

Figure 48: Edit Wire Groups

- Scroll down the screen as necessary to locate the entry with **Param ID** of “661” (not shown). Double click on the corresponding **Param Value** field, and enter “1” to activate detection for G729.
- Locate the entry with **Param ID** of “666” (not shown). Double click on the corresponding **Param Value** field, and enter “1” to enable SIP Provisional Acknowledgement (PRACK).
- Locate the entry with **Param ID** of “668” (not shown). Double click on the corresponding **Param Value** field, and enter “0” to disable SIP Remote Party ID (RPI). Reboot the SIP trunk card.

7.5. Administer Trusted Host

From the Linux shell of the ESS server, navigate to the **/usr/local/SipProxy**/ directory, and issue the command shown below with the "-add" option to add Session Manager as a trusted host. Note that 110.10.10.198 is the IP address of the signaling interface for Session Manager.

The same command can be used with the "-view" option to make certain Session Manager is displayed as a trusted host.

```
[root@esshost ~]# cd /usr/local/SipProxy/
[root@esshost SipProxy]# ./trusted_hosts.pl -add=110.10.10.198
[root@esshost SipProxy]# ./trusted_hosts.pl –view
 ip_address last_modified 110.10.10.198 2011-06-13 10:13:04
```

8. Verification Steps

The following tests were conducted to verify the solution between the Communication Server 1000 and Alliance system:

- All basic call features operate successfully between Communication Server 1000 and Alliance users.
- Connection between Alliance system and Avaya Aura® Session Manager is successfully established when the Ethernet connection is disconnected and connected back on the Alliance System.

9. Conclusion

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

10. Additional References

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

1. *Communication Server 1000 7.50 Administering and System Programming documents*, available at http://support.avaya.com.

2. *Administering Avaya Aura™ Session Manager*, Document Number 03-603324, Issue 1.1, Release 6.1, November 2010, available at http://support.avaya.com.

3. *Nexus Suite 2.0 SP1 Patch11 or Higher Deployment Guide*, Part Number B02200161, Revision Number 01, 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.