



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy with Avaya Communication Server 1000 7.5 using QSIG 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 QSIG trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used E1 QSIG trunks to Avaya Communication Server 1000, 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 QSIG trunks.

IPC Unigy (hereafter referred to as Unigy) is a trading communication solution. In the compliance testing, IPC Unigy used E1 QSIG trunks to Avaya Communication Server 1000 7.5 (hereafter referred to as Communication Server 1000), for turret users on IPC Unigy 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 Unigy turret users with Communication Server 1000 SIP, IP, 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 E1 connection to Unigy.

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, and attended conference.

The serviceability testing focused on verifying the ability of Unigy to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to Unigy.

2.2. Test Results

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

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, Unigy configuration consists of the Media Manager, Converged Communication Manager, Media Gateway, 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.

There is a physical connection between the 2Mb PRI circuit pack on Avaya Communication Server 1000 with the Unigy Media Gateway. E1 QSIG trunks are used from Unigy to Communication Server 1000, to reach users on Communication Server 1000 and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Unigy and Communication Server 1000. During compliance testing, extension ranges 58xxx were associated with Communication Server 1000 users and 36xxx were associated with the Unigy turret users. Avaya Call Pilot Directory Number (DN) is 58888 and the PSTN number is 96139655570.

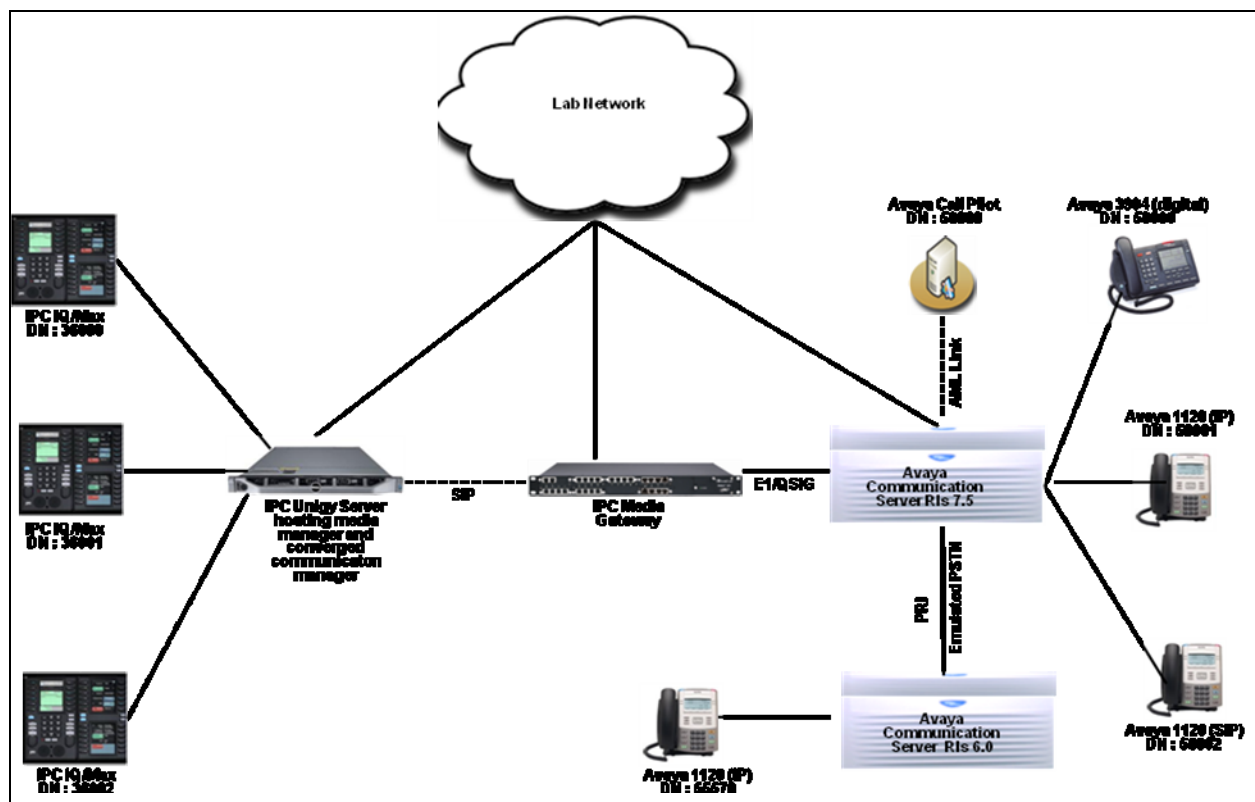


Figure 1: Compliance Test Setup in the lab

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 Digital user (3904)	NA
Avaya IP user (1120)	0624C8A
Avaya SIP user (1120)	04.01.13.00
IPC Unigy <ul style="list-style-type: none">Media ManagerConverged Communication ManagerMedia GatewayTurret (IQ/Max)	01.00.00.04.0003 01.00.00.04.0003 6.00AL.025.0002 01.00.00.04.0003

5. Configure Avaya Communication Server 1000

This section provides the procedures for configuring Communication Server 1000 system. The procedures include the following areas:

- Logging into the Element Manager via Unified Communications Manager.
- Configuring the D-Channel Loop.
- 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 users are already created and also the PRI Trunk between the Communication Servers 7.5 and 6.0 is configured for emulated PSTN setup during compliance testing. For detail configuration details refer to **Section 10[1]**.

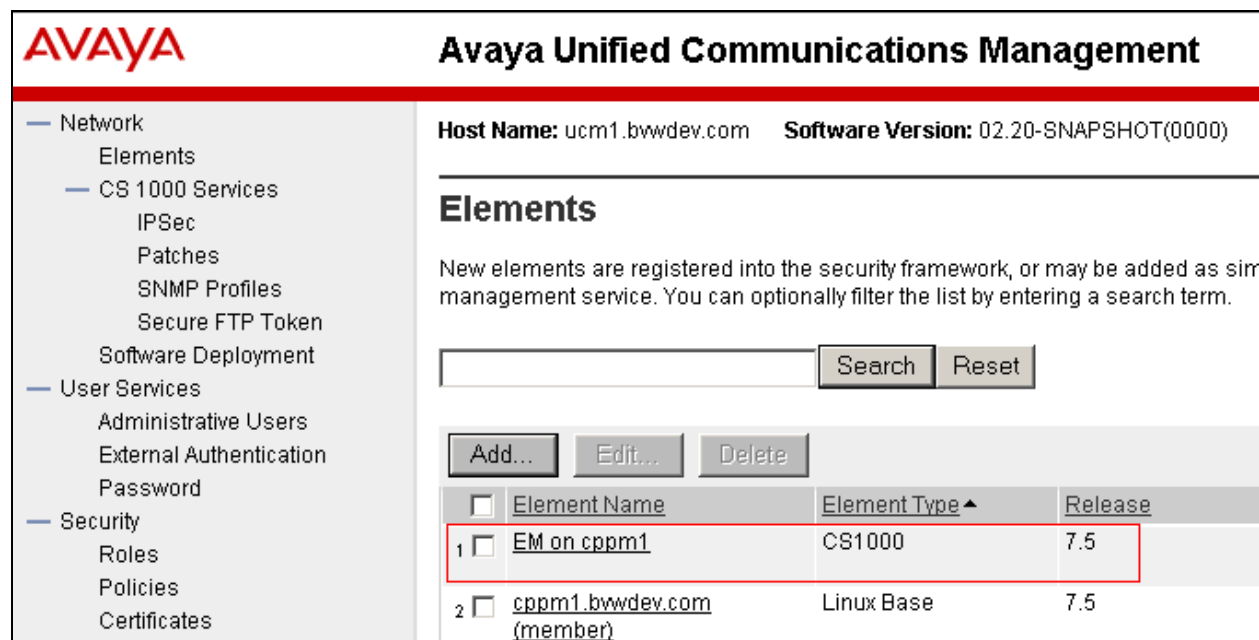
5.1. Logging to Element Manager via Unified Communication Manager

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.

The image shows the login screen of the Unified Communications Manager (UCM). It features a red header with the AVAYA logo in the bottom right corner. Below the header, there is a white area containing a login form. The form has two input fields: 'User ID:' and 'Password:'. Below these fields is a 'Log In' button. To the left of the form, there is a disclaimer text: 'This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.' At the bottom left of the white area, there is a copyright notice: 'Copyright © 2002-2010 Avaya Inc. All rights reserved.'

Figure 2: UCM Login Screen

From the 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 Call Server.



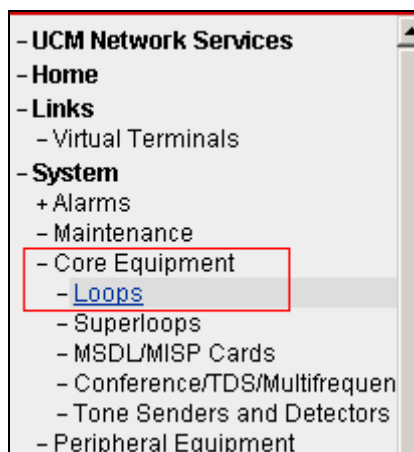
The screenshot shows the Avaya Unified Communications Management interface. The left sidebar contains a navigation tree with categories: Network, User Services, and Security. The main content area displays the 'Elements' section, showing a list of registered elements. The first element, 'EM on cppm1', is highlighted with a red box. Below the list are buttons for 'Add...', 'Edit...', and 'Delete'.

	Element Name	Element Type	Release
1	EM on cppm1	CS1000	7.5
2	cppm1.bwwdev.com (member)	Linux Base	7.5

Figure 3: UCM Main Screen

5.2. Configuring D-Channel Loop

This section explains the configuration required to add a D-Channel loop which will be used to configure the D-Channel on. In the EM left navigator screen, navigate to **System > Core Equipment > Loops** as shown in **Figure 4** below.

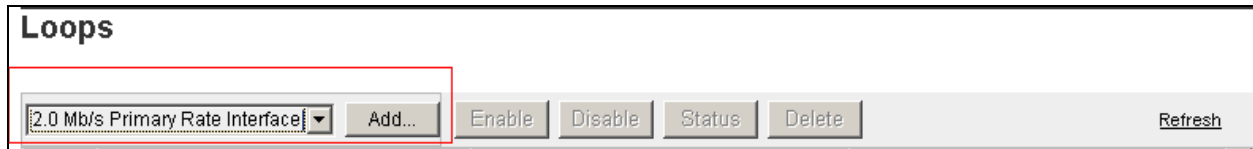


The screenshot shows the left navigation tree of the Element Manager. The tree is expanded to show the 'System' category, which includes 'Core Equipment' and 'Loops'. The 'Loops' item is highlighted with a red box.

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - Core Equipment
 - Loops
 - Superloops
 - MSDL/MISP Cards
 - Conference/TDS/Multifrequen
 - Tone Senders and Detectors
 - Peripheral Equipment

Figure 4: EM Screen showing navigation tree to Loops

Add a Loop by selecting **2.0 Mb/s Primary Rate Interface** from the drop down menu and click on **Add** to continue as shown in **Figure 5** below.

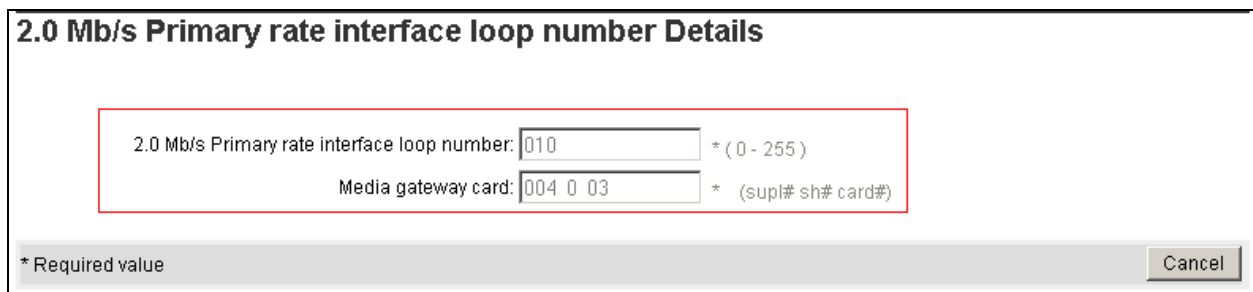


Loops

2.0 Mb/s Primary Rate Interface Add... Enable Disable Status Delete Refresh

Figure 5: Adding a Loop on the 2Mb PRI circuit pack

During compliance testing a loop number of **10** was selected and the physical location of the circuit pack was in **004 0 03**. Enter these values as shown in **Figure 6** below to complete adding the loop.



2.0 Mb/s Primary rate interface loop number Details

2.0 Mb/s Primary rate interface loop number: 010 * (0 - 255)

Media gateway card: 004 0 03 * (supl# sh# card#)

* Required value Cancel

Figure 6: Loop Configuration

5.3. Configuring D-Channel

This section explains the configuration of a D-Channel on the 2Mb PRI circuit pack. From the EM navigation screen, navigate to **Routes and Trunks > D-Channels** as shown in **Figure 7** below.

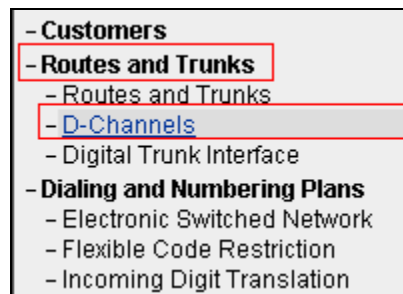


Figure 7: EM Screen showing navigation tree to D-Channels

Choose a D-Channel number to add as shown in **Figure 8** below. During compliance testing D-Channel number **5** was selected. Click on **to Add** to continue.

D-Channels

Maintenance

- [D-Channel Diagnostics \(LD 96\)](#)
- [Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)
- [MSDL Diagnostics \(LD 96\)](#)
- [TMDI Diagnostics \(LD 96\)](#)
- [D-Channel Expansion Diagnostics \(LD 48\)](#)

Configuration

Choose a D-Channel Number: and type:

Figure 8: Adding D-Channel

Configure the **Basic Configuration** values for the D-Channel as shown in **Figure 9** below. Note here that the D-Channel PRI loop number is the same one that was configured in **Section 5.2** above.

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	MSDL
Media Gateway Card:	004 0 03 (supl# sh# card#) *
Group number:	
Device number:	
Port number:	1
Designator:	QSIG_IPC
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Primary Rate Interface (PRI) *
Interface type for D-channel:	ISIG interface with GF platform (ISGF)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	10
Primary Rate Interface:	<input type="button" value="more PRI"/>
Secondary PRI2 loops:	
Release ID of the switch at the far end:	5
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	200 Range: 1 - 4000

Figure 9: D-Channel Basic Configuration

To edit the **Remote Capabilities** of the D-Channel, click on **Edit** button as shown in **Figure 10** below.

Integrated Services Signaling Link Maximum: 200 Range: 1 - 4000

- Basic options (BSCOPT)

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

- PINX customer number: 0

- Progress signal:

- Calling Line Identification: Prefix = 0 for North American dialing plan. (OPT0)

- Output request Buffers: 32

- D-channel transmission Rate: 64 kb/s clear (64KC)

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

- Remote Capabilities: **Edit**

+ - Change protocol timer value (TIMR)

- B channel Service messaging.: ☐

Figure 10: Editing Remote Capabilities Screen

Select the boxes values for the Remote Capabilities as shown in **Figures 11a** and **11 b** below. Click on **Return - Remote Capabilities** button to return back to the main screen to complete the D-Channel configuration.

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input checked="" type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call completion on busy for QSIG and EuroISDN BRI (CCBS)	<input type="checkbox"/>
Call completion on no response using integer value (CCNI)	<input checked="" type="checkbox"/>
Call completion on no response using object identifier (CCNO)	<input type="checkbox"/>
Call completion to no reply for QSIG and EuroISDN BRI (CCNR)	<input type="checkbox"/>
Network call park (CPK)	<input type="checkbox"/>
Connected line identification presentation (COLP)	<input checked="" type="checkbox"/>
Call transfer integer (CTI)	<input checked="" type="checkbox"/>
Call transfer object (CTO)	<input type="checkbox"/>
Diversion info. is sent using integer value (DV1I)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2I)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3I)	<input checked="" type="checkbox"/>
EuroISDN - div. info sent. rerouting req. processed (DV3O)	<input type="checkbox"/>

Figure 11a: Remote Capabilities Values

Network name display method 2 (ND2) ☐

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☒

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☒

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

~~N1-2 name display option. (NDS)~~ ☐

Message waiting indication using integer values (QMWI) ☒

Message waiting indication using object identifier (QMWO) ☐

User to user signalling (UUI) ☐

Return - Remote Capabilities Cancel

Figure 11b: Remote Capabilities Values (cont'd)

5.4. Configuring Route and Trunks

This section explains the configuration of the QSIG route and trunks which will be used by Communication Server 1000 and Unigy. To add a new route, navigate to **Routes and Trunks > Routes and Trunks** from the EM left hand navigator window as shown in **Figure 12** below.

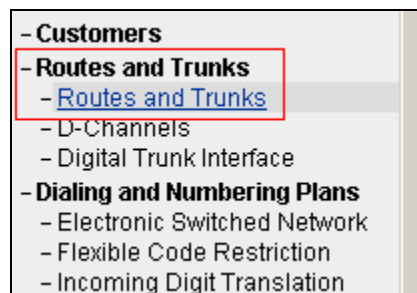


Figure 12: EM Screen showing navigation tree to Routes and Trunks

From the Routes and Trunks screen click on **Add route** button to start configuring a new route as shown in **Figure 13** below.

The screenshot shows the 'Routes and Trunks' header. Below it, a red rectangle highlights a row containing: a plus sign icon, a 'Customer: 0' label, 'Total routes: 6', 'Total trunks: 123', and an 'Add route' button.

Figure 13: Adding a new Route

During compliance testing **Route number 50** was added. Select the values from the drop down menu and configure the values as shown in **Figures 14a** and **14b** below.

The screenshot shows the 'Route Basic Configuration' form. A red oval highlights the title '- Basic Configuration'. The form contains the following fields and options:

- Route data block (RDB) (TYPE): RDB
- Customer number (CUST): 00
- Route number (ROUT): 50
- Designator field for trunk (DES): QSIG_IPC
- Trunk type (TKTP): TIE
- Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO) [dropdown]
- Access code for the trunk route (ACOD): 8050 *
- Trunk type M911P (M911P): ☐
- The route is for a virtual trunk route (VTRK): ☐
- Digital trunk route (DTRK): ☒
- ISDN BRI packet handler route (BRIP): ☐
- Digital trunk type (DGTP): PRI2
- Integrated services digital network option (ISDN): ☒
- Mode of operation (MODE): ISDN/PRA route, DTRK must be YES (PRA) [dropdown]
- Interface type for route (IFC): ISIG interface with GF platform. (ISGF) [dropdown]
- Send billing number (SBN): ☐
- Private network identifier (PNI): 00003 (0 - 32700)
- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN) [dropdown]
- Insert ESN access code (INAC): ☒
- Display of access prefix on CLID (DAPC): ☐

Figure 14a: Route Basic Configuration values

Process notification networked calls (PNNC) : ☐

- 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) : ☐

Figure 14b: Route Network Options values

Configure the trunk values as shown in **Figure 15** below. Note that the **Terminal number** starts with **010 01** since the D-Channel loop was built on Loop 10. Click on **Edit** button to configure the required **Class of Service** for the trunks.

Customer 0, Route 50, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block: TIE

Terminal number: 010 01

Designator field for trunk: QSIG_IPC

Extended trunk:

Member number: 1

Level 3 Signaling:

Card density: SD

Start arrangement Incoming :

Start arrangement Outgoing:

Trunk group access restriction: 0

Channel ID for this trunk:

Network music: ☐

Class of Service: **Edit**

+ Advanced Trunk Configurations

Figure 15: Trunk Properties

Figures 16a and 16b 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.

- Class of Service	
Input Description	Input Value
- ACD Priority:	ACD Priority not required (APN)
- Analog Semi-Permanent Connections:	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT:	
- Barring:	Barring Denied (BARD)
- Battery Supervised COT:	
- Busy Tone Supervised COT:	
- Calling Line Identification:	
- Calling party:	Calling party Denied (CND)
- Central Office Ringback:	
- Centrex Switchhook Flash:	Centrex Switchhook Flash Denied (THFD)
- Dial Pulse:	Dial Pulse (DIP)
- DTR PAD value:	
- Echo Canceling:	Echo Canceling Denied (ECD)
- Hong Kong DTI:	
- Loop Break Supervised COT:	
- Make-break ratio for dial pulse:	10 pulses per second (P10)
- Manual Incoming:	

Figure 16a: Trunk Class of Service

- Polarity:	
- Priority:	Low Priority (LPR)
- Restriction level:	Unrestricted (UNR)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- Short or long line:	
- Transmission Class of Service:	Via Net Loss (VNL)
- Warning Tone:	Warning Tone Allowed (WTA)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- ARF Supervised COT:	

Figure 16b: Trunk Class of Service (cont'd)

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 Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 17** below.

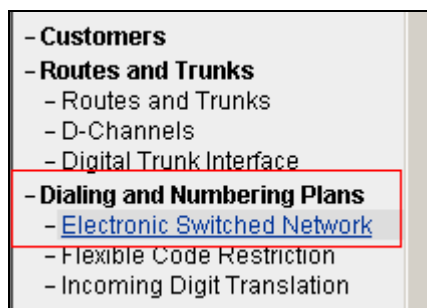


Figure 17: EM Screen showing navigation tree to Electronic Switched Network

Click on **Digit Manipulation Block (DGT)** option as shown in **Figure 18** below.

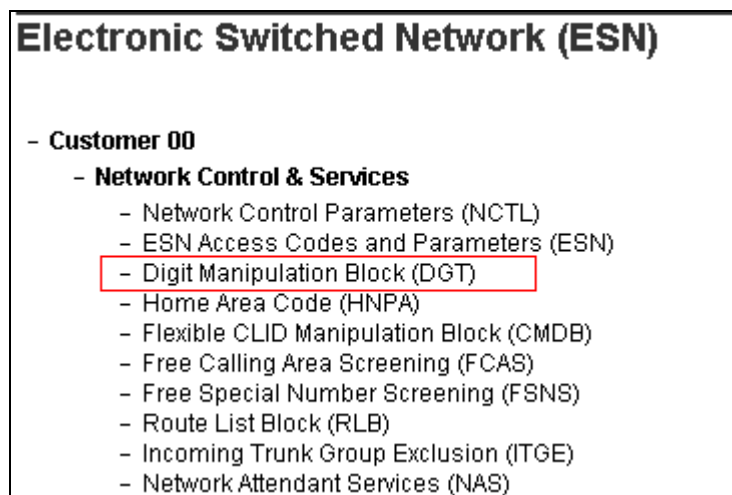


Figure 18: Accessing Digit Manipulation Block

Select a block index to configure and click on **to Add** button as shown in **Figure 19** below. During compliance testing **Digit Manipulation Block Index** of 7 was added.

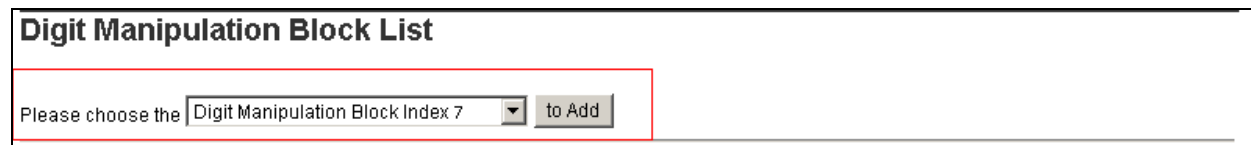
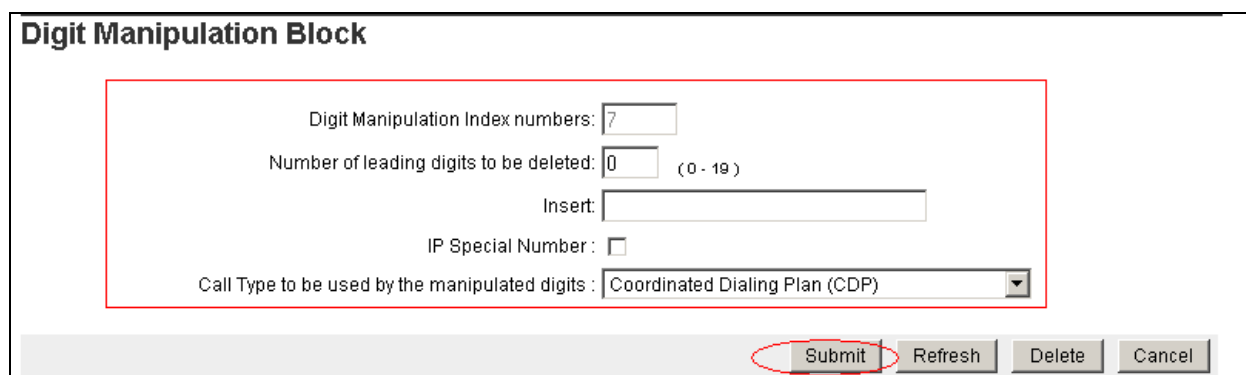


Figure 19: Adding a Digit Manipulation Block Index

Figure 20 below shows the values configured. Click on **Submit** to complete adding the Digit Manipulation Block configuration.

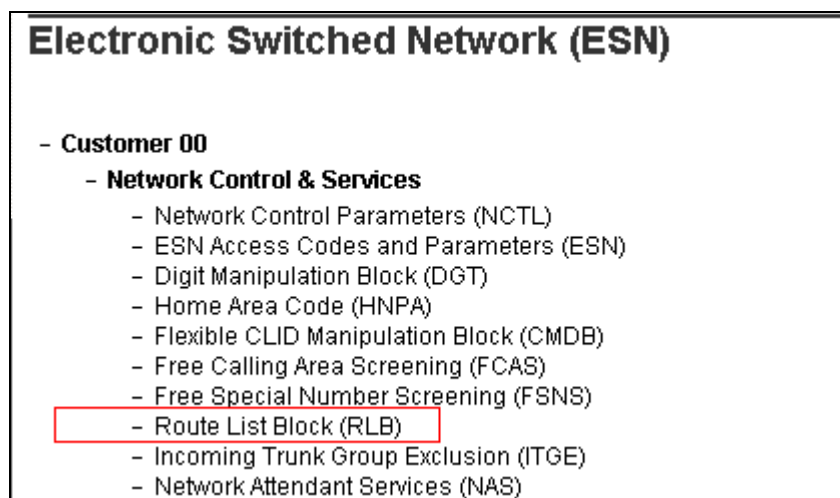


The screenshot shows a web form titled "Digit Manipulation Block". Inside a red rectangular box, there are several input fields: "Digit Manipulation Index numbers:" with the value "7", "Number of leading digits to be deleted:" with the value "0" and a range "(0 - 19)", "Insert:" with an empty text box, "IP Special Number:" with an unchecked checkbox, and "Call Type to be used by the manipulated digits:" with a dropdown menu showing "Coordinated Dialing Plan (CDP)". Below the red box, there are four buttons: "Submit" (circled in red), "Refresh", "Delete", and "Cancel".

Figure 20: Digit Manipulation Block properties

5.6. Configuring Route List Block

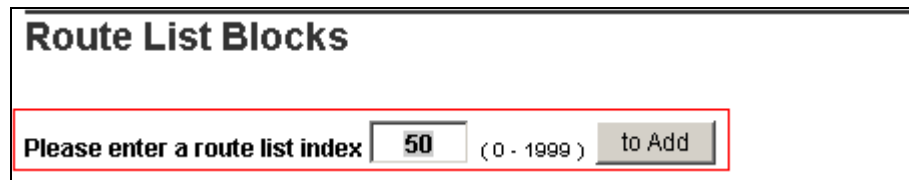
This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 17** above. Click on **Route List Block (RLB)** option as shown in **Figure 21** below.



The screenshot shows a web page titled "Electronic Switched Network (ESN)". Under the heading "- Customer 00", there is a sub-heading "- Network Control & Services". Below this, there is a list of options: "Network Control Parameters (NCTL)", "ESN Access Codes and Parameters (ESN)", "Digit Manipulation Block (DGT)", "Home Area Code (HNPA)", "Flexible CLID Manipulation Block (CMDDB)", "Free Calling Area Screening (FCAS)", "Free Special Number Screening (FSNS)", "Route List Block (RLB)" (highlighted with a red box), "Incoming Trunk Group Exclusion (ITGE)", and "Network Attendant Services (NAS)".

Figure 21: Accessing Route List Block

Start adding a **route list index** as shown in **Figure 22** below. During compliance testing list index **50** was added. Click on **to Add** to continue.

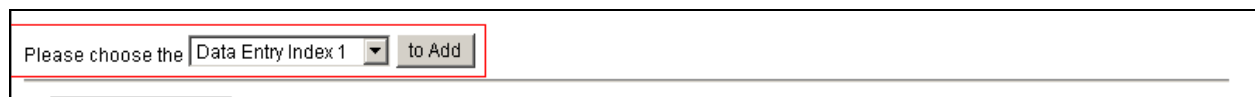


Route List Blocks

Please enter a route list index (0 - 1999)

Figure 22: Adding Route List Index


Add a **Data Entry Index** as shown in **Figure 23** below. During compliance testing entry index **1** was selected and click on **to Add** to continue.



Please choose the

Figure 23: Adding Data Entry Index

Figures 24a and **24b** below show the values configured for the index block used during compliance testing. **Route Number** of **50** and **Digit Manipulation Index** of **7** were selected as per the configuration explained in **Sections 5.4** and **5.5** respectively. Click on **Submit** to complete the configuration.



Indexes

Time of Day Schedule:

Facility Restriction Level: (0 - 7)

Digit Manipulation Index:

ISL D-Channel Down Digit Manipulation Index: (0 - 1999)

Free Calling Area Screening Index:

Free Special Number Screening Index:

Business Network Extension Route: ☐

Incoming CLID Table: (0 - 100)

Figure 24a: Route List Block properties

Options

Local Termination entry: ☐

Route Number:

Skip Conventional Signaling: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion:

- QSIG Alternate Routing Causes:

Preferred Routing:

ISDN Drop Back Busy:

ISDN Off-Hook Queuing Option: ☐

Off-Hook Queuing Allowed: ☐

Call Back Queuing Allowed: ☐

VNS Options

Entry is a VNS Route: ☐

Figure 24b: Route List Block properties (cont'd)

5.7. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the 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 17** above. Click on **Distant Steering Code (DSC)** option as shown in **Figure 25** below.

Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)

Figure 25: Accessing Distant Steering Code

From the drop down menu select **Add** and enter a distant steering code to add as shown in **Figure 26** below. During compliance testing a code of **360** was added since the Unigy extension range started with 36xxx. Click on **to Add** to continue.



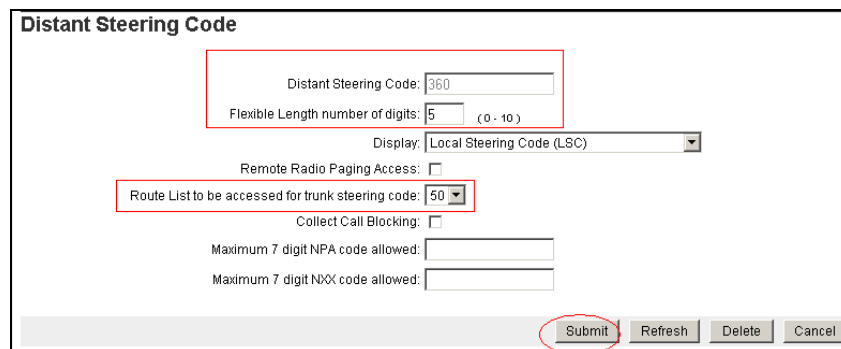
Distant Steering Code List

Add ▼

Please enter a distant steering code to Add

Figure 26: Adding a Distant Steering Code

Enter the values as shown in **Figure 27** below. Note that **Route List to be accessed for trunk steering code** value selected is **50** based on the configuration explained in **Section 5.6** above. Click on **Submit** to complete the configuration.



Distant Steering Code

Distant Steering Code:

Flexible Length number of digits: (0 - 10)

Display: Local Steering Code (LSC) ▼

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code: ▼

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

Submit Refresh Delete Cancel

Figure 27: Distant Steering Code properties

6. 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 media gateway
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

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 detail administration and configuration of Unigy system refer to **Section 10 [2]**.

6.1. 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 28** 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**.

The image shows a web-based login interface for the IPC Unigy Management System. On the left is the IPC logo. To its right are labels for 'User Name:' and 'Password:' followed by input fields. A red rectangle highlights both input fields. Below the password field is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. To the right of the checkbox is a 'Login' button, which is also circled in red. At the bottom of the form, the text reads: 'IPC Unigy™ Management System', 'Unigy™ Version 01.00.00.04.0003', and '© Copyright 2011 IPC Systems, Inc.'

Figure 28: Unigy Management System Login Screen

6.2. Administer Media Gateway

The screen as shown in **Figure 29** below is displayed next. Select **Configuration > Site Configuration** from the top menu.

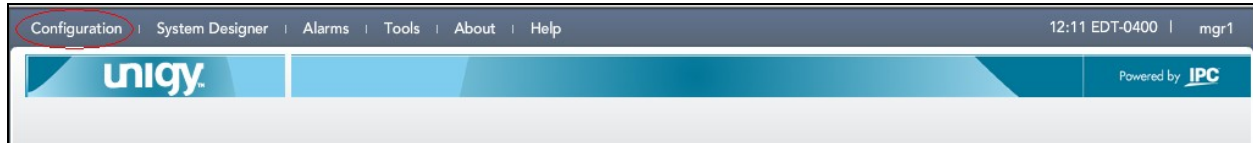


Figure 29: Unigy Management System Login Screen

Figure 30 below shows the **Site Configuration** information displayed in the left pane. Select **Trunks > Media Gateways**, to display a list of media gateway in the lower left pane. Select the applicable media gateway from the listing, in this case **MG-110.10.10.225**, where the 110.10.10.225 is the IP address of the Media Gateway.

The **Media Gateway** information is displayed in the upper right pane. Select the applicable physical card, in this case **Slot 1**.

The **Media Gateway Module Details** information is displayed in the lower right pane. Select **2 Port TDM** for **Type**, and click **Save**.

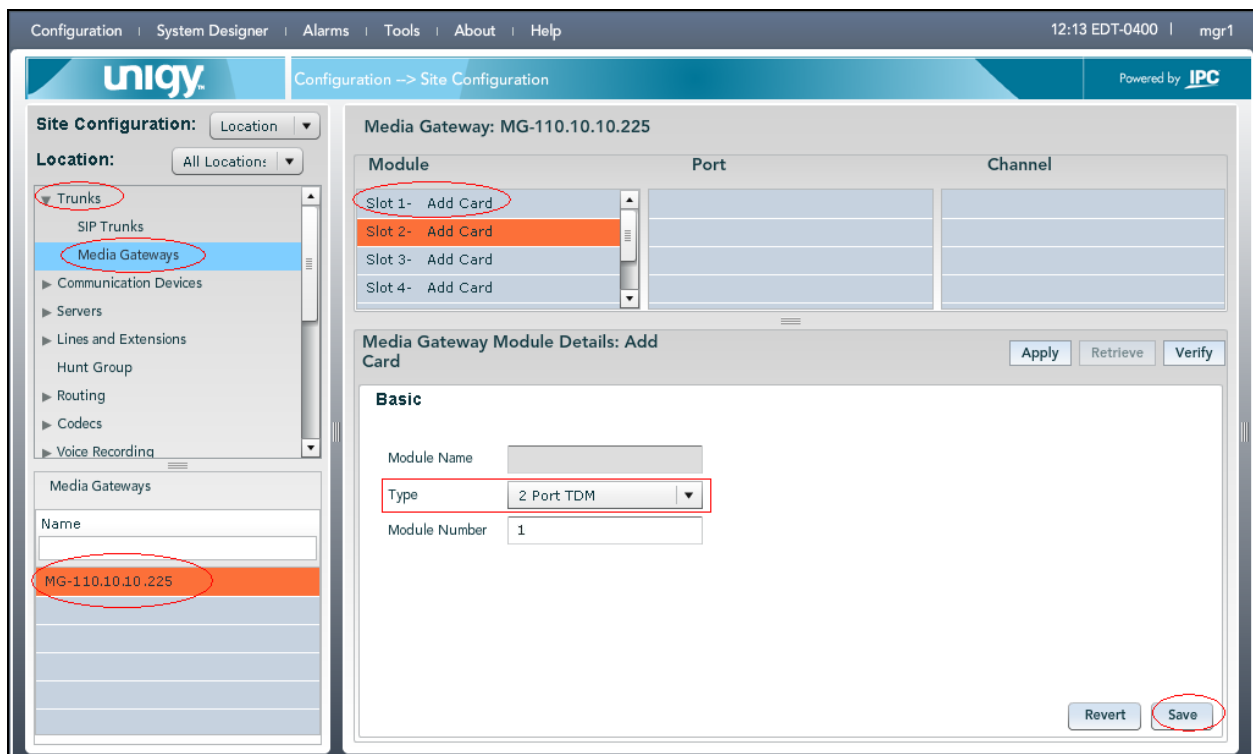


Figure 30: Media Gateway Configuration under Trunks

In the updated screen as shown in **Figure 31**, click on a desired **Port** in the upper right pane, in this case **Port 1**.

The **Media Gateway Port Details** information is displayed in the lower right pane. Select the values shown from the drop down menu of the **Port Properties** tab.

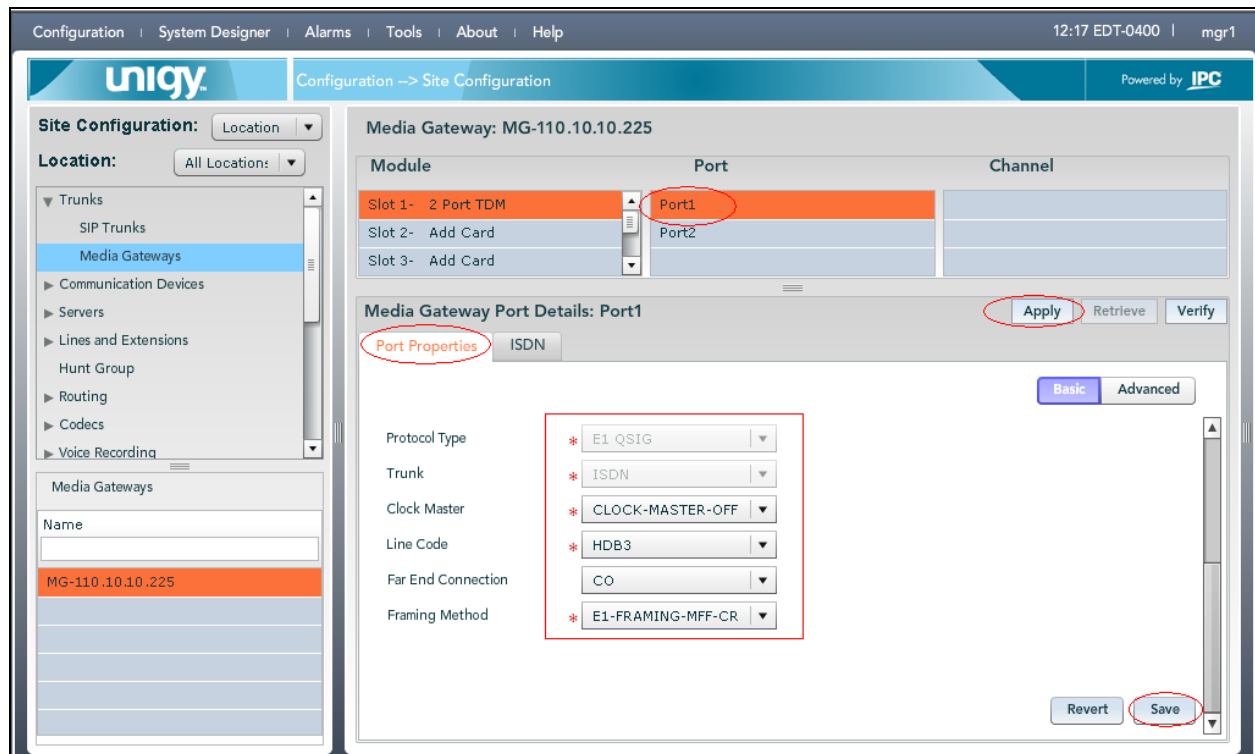


Figure 31: Port Properties

Figures 32a and 32b show the **ISDN** properties. During compliance testing the values shown below were used. Note that 110.10.10.225 is the IP address of the Media Gateway. Leave the remaining values at default.

The screenshot shows the 'Media Gateway Port Details: Port1' configuration window. The 'ISDN' tab is selected and highlighted with a red circle. The 'Basic' section is active, showing the following fields: Trunk Name (QSIG/ISDN Trunk 1), Destination Address (110.10.10.225), Destination Port (5060), Inbound Significant Digits (* 0), External Called Party Prefix, and Internal Called Party Prefix. A red box highlights the Trunk Name, Destination Address, Destination Port, and Inbound Significant Digits fields. The 'Apply', 'Retrieve', and 'Verify' buttons are at the top right.

Figure 32a: ISDN Properties

The screenshot shows the 'Media Gateway Port Details: Port1' configuration window, ISDN tab. The 'Advanced' section is active, showing the following fields: Internal Called Party Prefix, Connected Party Update (* UPDATE), SubscribeMWI (0), MWI Subscription Time (0), Trunk Group ID (0), Connection Type (* Dial Tone), ISDN Termination Side (USER-TERMINATION-), and Q931 Layer Response Behavior (0x40080000). A red box highlights the Connected Party Update, SubscribeMWI, MWI Subscription Time, Trunk Group ID, Connection Type, and ISDN Termination Side fields. The 'Save' and 'Revert' buttons are at the bottom right.

Figure 32b: ISDN Properties (cont'd)

Click **Save** followed by **Apply** to complete the configuration.

6.3. Administer Trunk Groups

Select **Routing > Trunk Groups** in the left pane, and click the **Add** icon in the lower left pane to add a new trunk group as shown in **Figure 33** 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).

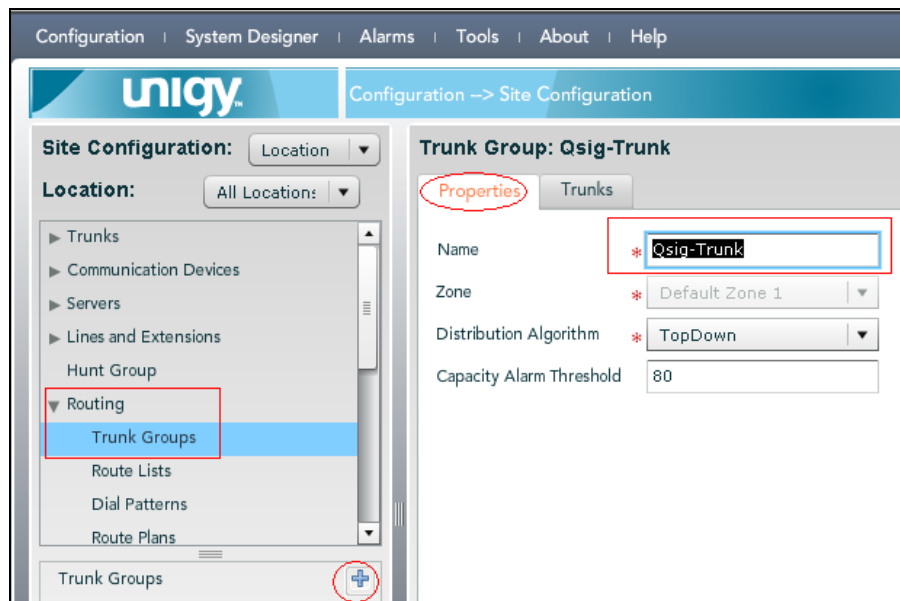


Figure 33: Adding Trunk Group

Select the **Trunks** tab in the right pane as shown in **Figure 34** below. The screen is updated with three panes. In the right pane, select the **MG Trunks** tab. In the **Media Gateway** listing, select and expand the applicable media gateway slot and port (not shown) from **Section 6.2**, and drag the selection to the **Name** column in the middle pane as shown below. Click on **Save** (not shown) to complete the configuration.

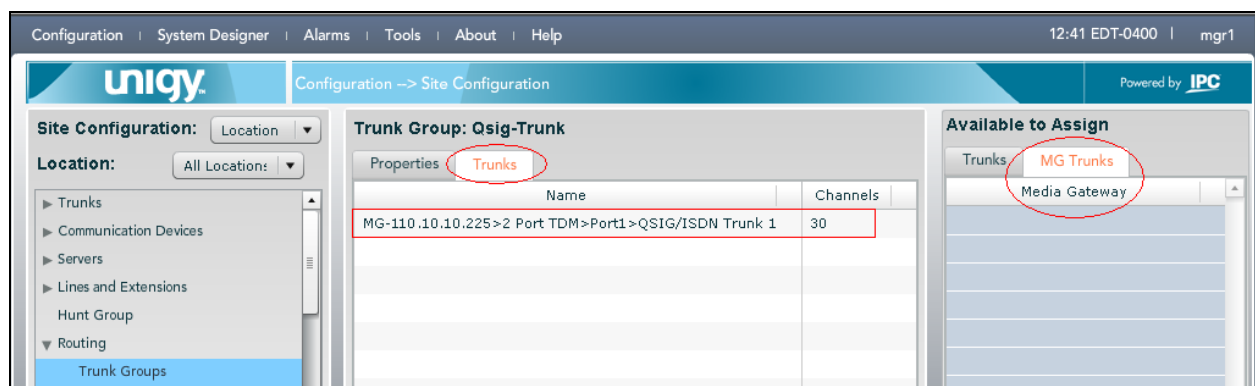


Figure 34: Adding Trunk Group

6.4. Administer Route Lists

Select **Routing > Route Lists** in the left pane, and click the **Add** icon in the lower left pane to add a new route list as shown in **Figure 35** 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 6.3** 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.

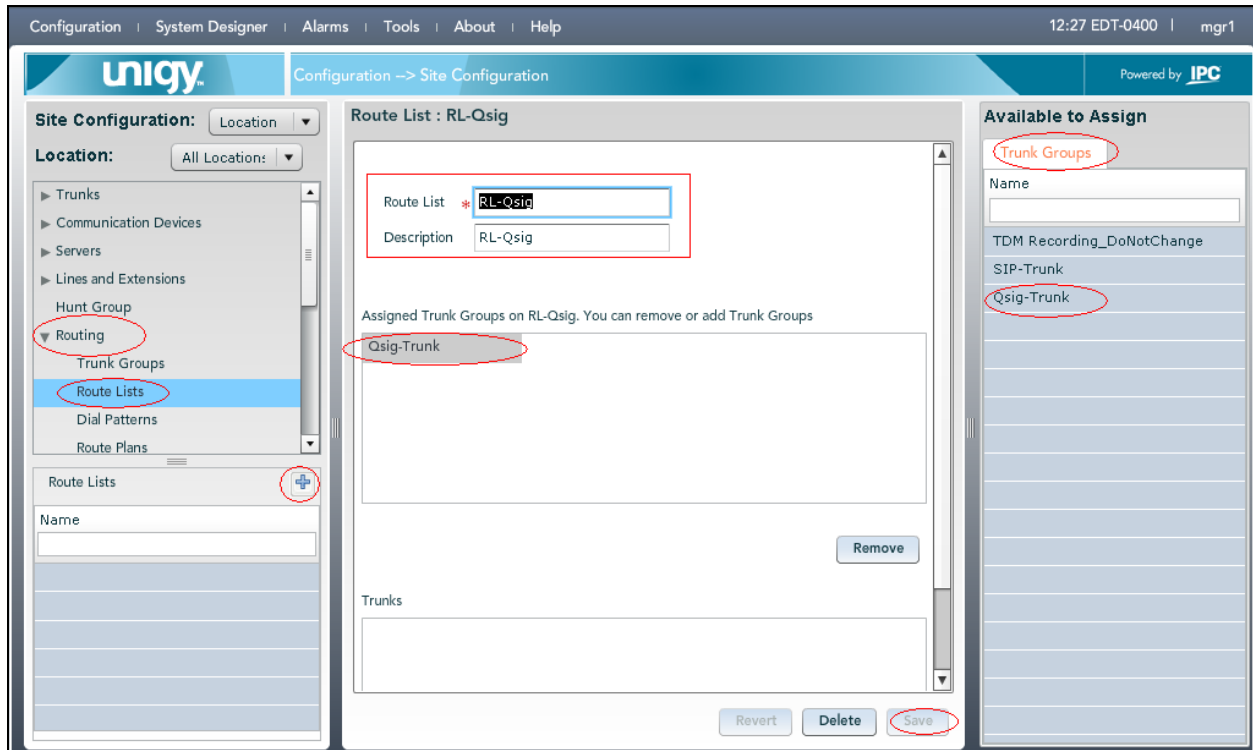


Figure 35: Adding Route List

6.5. 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 36** 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 the Avaya extensions, in this case **58\$\$\$** with “\$” matching to any digit. For **Call Classification**, select **External**. Click on **Save** to complete adding a dial pattern.

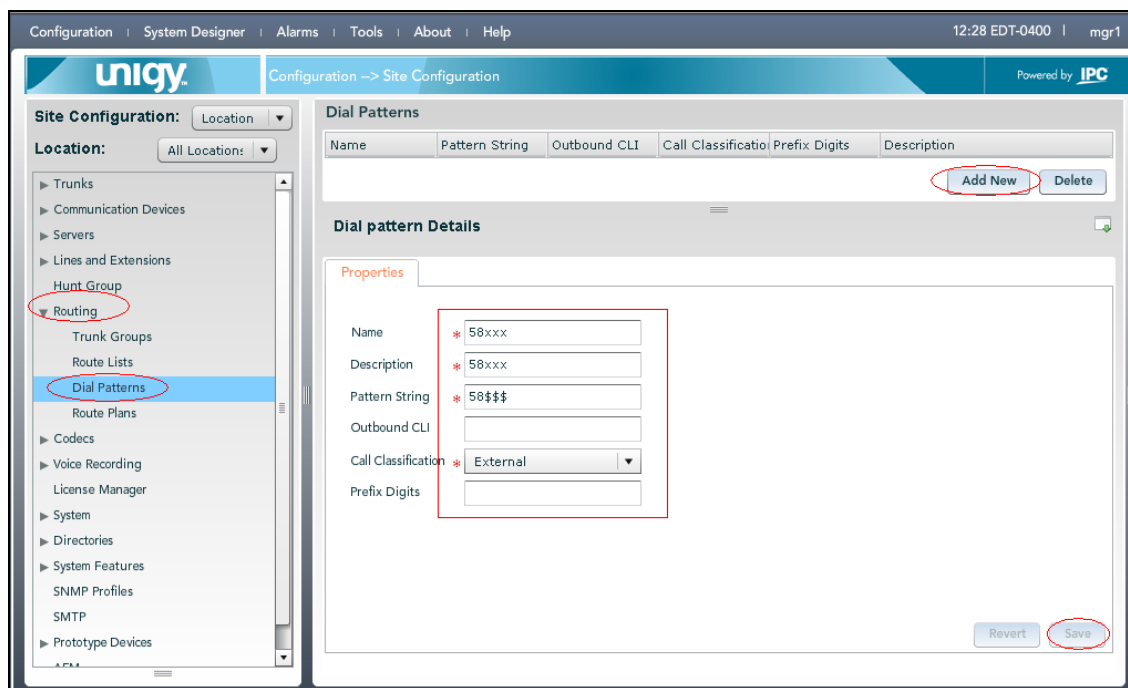


Figure 36: Adding a Dial Pattern

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix. In the compliance testing, two dial patterns were created as shown in **Figure 37** below.

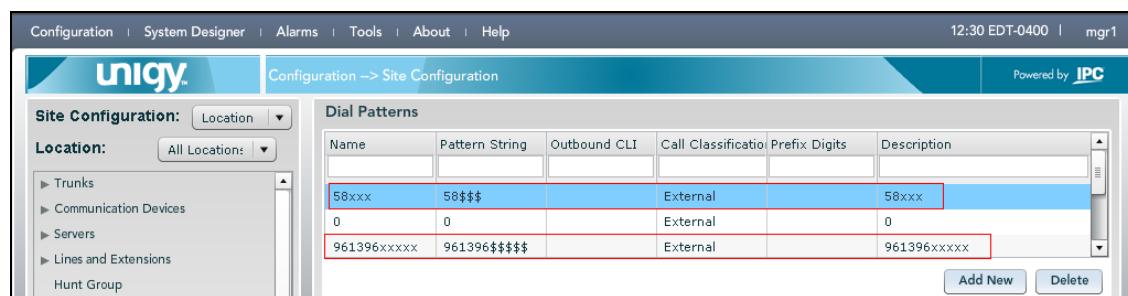


Figure 37: Extension and PSTN Dial Patterns

6.6. 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 38** below.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter * to denote any calling party from Unigy. For **Called Party**, select the dial pattern for the Avaya users from **Section 6.5**. Select **Forward** for **Action**, and click on **Save**.

The screenshot shows the Unigy configuration interface. The left pane shows the 'Site Configuration' tree with 'Routing' and 'Route Plans' highlighted. The middle pane is titled 'Route Plan' and contains a 'Create New Route Plan' form. The form fields are: UI Name (58xxx), Description (empty), Calling Party (*), Called Party (58xxx), and Action (Forward). The 'Save' button is circled in red. The right pane is titled 'Available to Assign' and shows a list of route plans.

Figure 38: Creating a new Route plan

The screen is updated with the newly created route plan as shown in **Figure 39** below. Select the route plan, and click **Edit** toward the bottom of the screen (not shown).

The screenshot shows the Unigy configuration interface. The left pane shows the 'Site Configuration' tree. The middle pane is titled 'Route Plan' and contains a 'List of Route Plans' table. The table has columns: UI Name, Calling Party, Called Party, and Action. The row with UI Name 58xxx, Calling Party *, Called Party 58xxx, and Action FORWARD is highlighted with a red box.

UI Name	Calling Party	Called Party	Action
58xxx	*	58xxx	FORWARD

Figure 39: New Route Plan

The screen is updated with three panes again, as shown in **Figure 40** below. In the right pane, select the route list from **Section 6.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration.

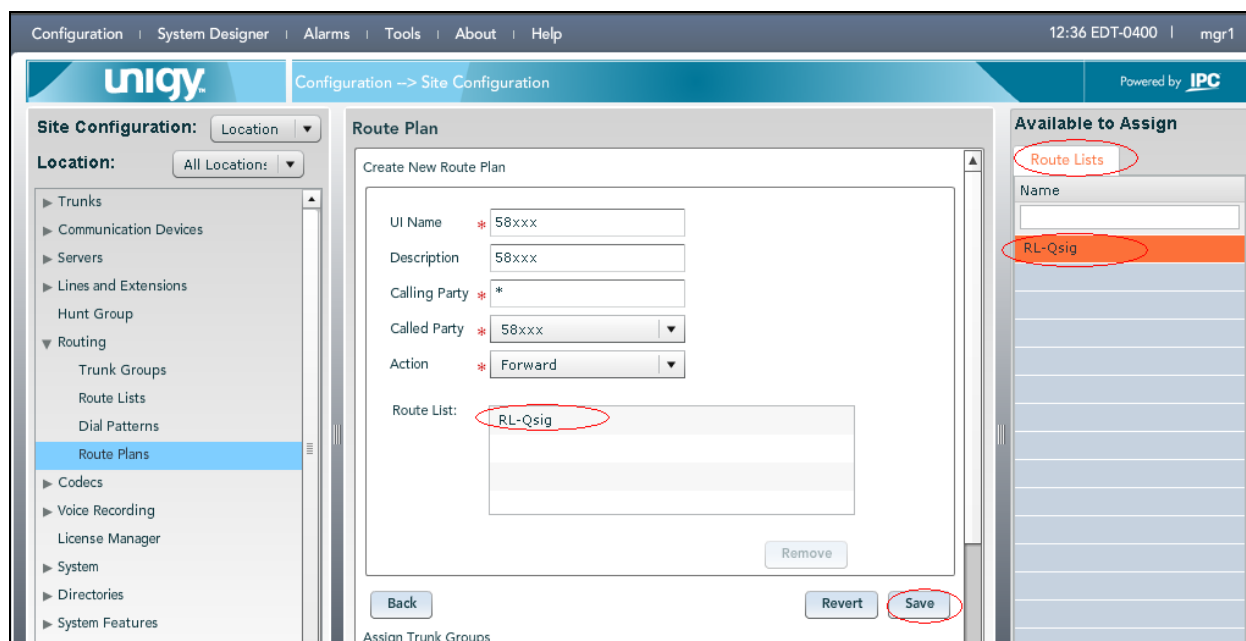


Figure 40: Adding Route List to Route Plan

Repeat this section to add another route plan for the PSTN. During compliance testing, two route plans were created as shown in **Figure 41** below.

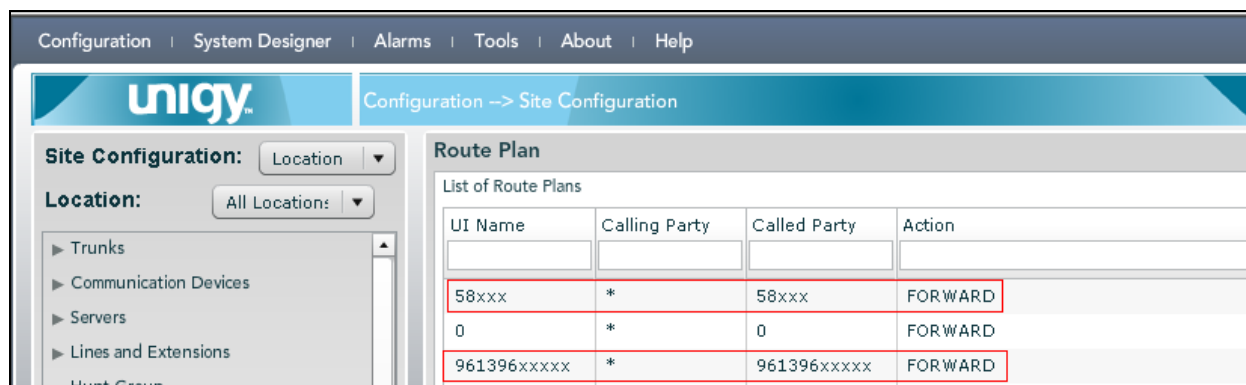


Figure 41: Extension and PSTN Route Plan

7. Configure IPC Media Gateway

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

- Launch gateway web interface.
- Administer trunk settings.
- Administer connected number.
- Configuring Media Gateway Clock Settings.

The configuration of the Media Gateway is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes. Note that IPC resells the AudioCodes Mediant 1000 MSBG as part of their solution.

7.1. Launch Gateway Web Interface

Access the Media Gateway web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Gateway. Log in (not shown) using the appropriate credentials.

7.2. Administer Trunk Settings

The screen as shown in **Figure 42** below is displayed. Select the radio button for **Full** in the left pane, and select **VoIP > PSTN Settings > Trunk Settings**, to display the **Trunk Settings** screen. Click **Stop Trunk**, followed by the arrow next to **Q931 Layer Response Behavior**.

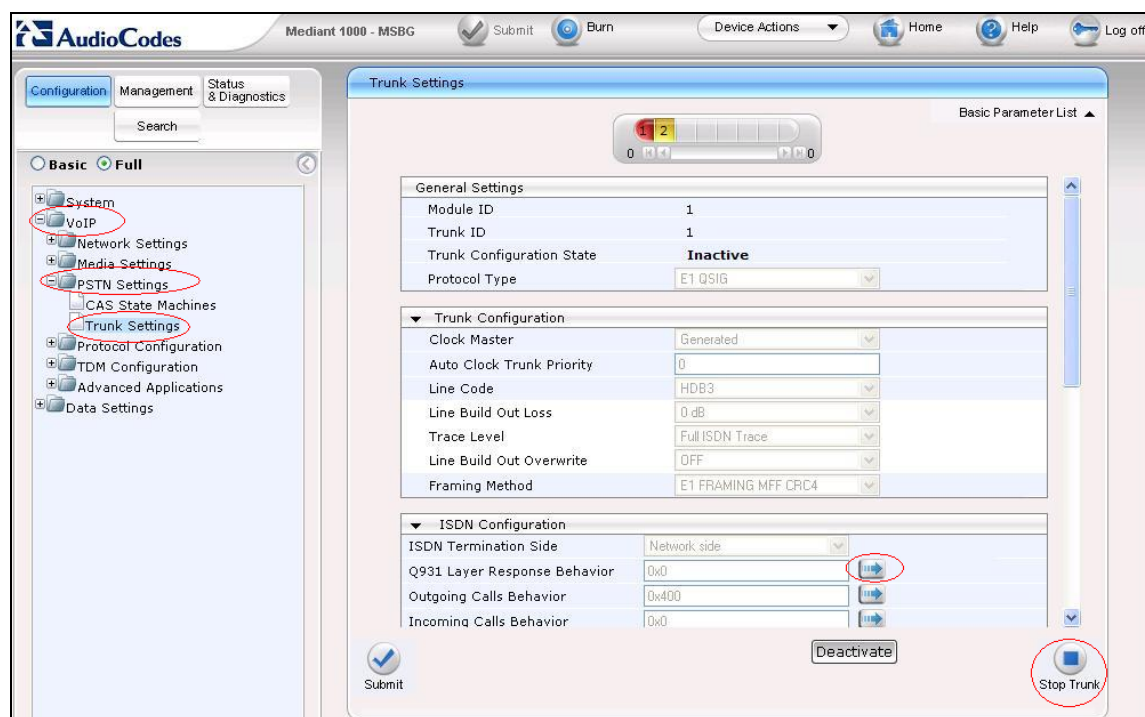


Figure 42: Trunk Settings screen of Media Gateway

Q931 Layer Response Behavior screen as shown in **Figure 43** below is displayed. Enable the corresponding bits for the following values and click on **Submit**.

- **NO STATUS ON UNKNOWN IE**
- **NO STATUS ON INV OP IE**
- **ACCEPT UNKNOWN FAC IE**
- **ACCEPT A LAW**
- **QSI ENCODE INTEGER**

Bit Hex Value	Bit Name	Bit Value
0x000001	NO STATUS ON UNKNOWN IE	1
0x000002	NO STATUS ON INV OP IE	1
0x000004	ACCEPT UNKNOWN FAC IE	1
0x000080	SEND USER CONNECT ACK	0
0x000200	EXPLICIT INTERFACE ID	0
0x000800	ALWAYS EXPLICIT	0
0x008000	ACCEPT MU LAW	0
0x010000	EXPLICIT PRES SCREENING	0
0x020000	STATUS INCOMPATIBLE STATE	0
0x040000	STATUS ERROR CAUSE	0
0x080000	ACCEPT A LAW	1
0x200000	RESTART INDICATION	0
0x400000	FORCED RESTART	0
0x40000000	QSI ENCODE INTEGER	1
0x80000000	SESS National Mode For Bch Maintenance	Custom Mode

Figure 43: Q931 Layer Response Behavior Bit Values

Return to the **Trunk Settings** screen as shown in **Figure 42** above; click **Apply Trunk Settings**, followed by **Burn** to commit the changes (not shown).

7.3. Administer Connected Number

Access the Media Gateway administration page web interface by using the URL “http://ip-address/AdminPage” in an Internet browser window, where “ip-address” is the IP address of the Media Gateway.

The screen as shown in **Figure 44** below is displayed. Select **ini Parameters** and enter the appropriate credentials in the pop-up box (not shown).



Figure 44: Accessing ini Parameters

The screen as shown in **Figure 45** below is displayed. Enter the values shown below to set destination using the connected number. Click **Apply New Value**.

A screenshot of the 'ini Parameters' page in the Media Gateway administration web interface. On the left sidebar, 'ini Parameters' is selected. The main area has a light blue background. At the top, there is a form with two input fields: 'Parameter Name:' containing 'UseDestinationasconnectednumber' and 'Enter Value:' containing '1'. To the right of these fields is a button labeled 'Apply New Value'. Below the form is a large white rectangular area labeled 'Output Window'.

Figure 45: UseDestinationasconnectednumber Value

7.4. Configuring Media Gateway Clock settings

Access the Media Gateway administration page web interface as explained in **Section 7.3** above.

Select **ini Parameters** as shown in **Figure 44** above and enter the appropriate credentials in the pop-up box (not shown).

The screen as shown in **Figure 46** below is displayed. Type a **Parameter Name** and check the existing value as shown in the **Output Window**. If a value needs to be changed, type the new value in the **Enter Value** box and click on **Apply New Value**.

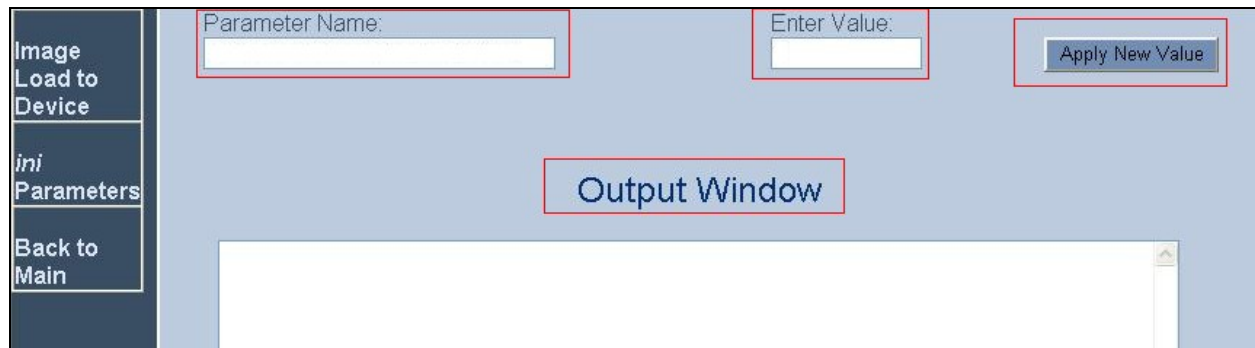


Figure 46: Screen showing Output Window of ini Parameters

During compliance testing the following **ini Parameters** values were checked and changed for the integration to be successful. These parameters of Media Gateway settings are related to clocking, which ensure that the clock slippages are not present on the E1QSIG link between Unigy Media Gateway and Communication Server1000.

- Parameter Name: CLOCKMASTER
Parameter Current Value: 0
Value selected was 0 to recover the clock from the Communication Server.
- Parameter Name: TDMBUSCLOCKSOURCE
Parameter Current Value: 4
Value selected was 4 in order to use recovered clock from PSTN line of the Communication Server
- Parameter Name: TDMBUSLOCALREFERENCE
Parameter Current Value: 0
Value selected was 0 to select clock of the first E1 in the chassis of Media Gateway.
- Parameter Name: TDMBUSENABLEFALLBACK
Parameter Current Value: 2
Value was 2 so that we enable automatic fallback of the clock to occur.

- Parameter Name: TDMBUSFALLBACKCLOCK
Parameter Current Value: 4
Value was set to 4 so that Media Gateway with synchronize with network in case clock failure occurred.
- Parameter Name: TDMBUSNETREFSPEED
Parameter Current Value: 0
Reference clock was set to 8 kHz (default) for both generation and synchronization
- Parameter Name: TDMBUSPSTNAUTOCLOCKENABLE
Parameter Current Value: 1
Value was set to 1 so that Media Gateway recovers the clock from any connected synchronized slave E1/T1 line
- Parameter Name: TDMBUSPSTNAUTOCLOCKREVERTINGENABLE
Parameter Current Value: 0
Value was set to 1 so as to enable the PSTN trunk Auto-Fallback Reverting feature.
- Parameter Name: AUTOCLOCKTRUNKPRIORITY
Parameter Current Value: 0
Value was set to 0 so as to get highest priority for auto-clock fallback

Figure 47 below shows the **Output Window** with a few examples of the **ini Parameters** and their values.

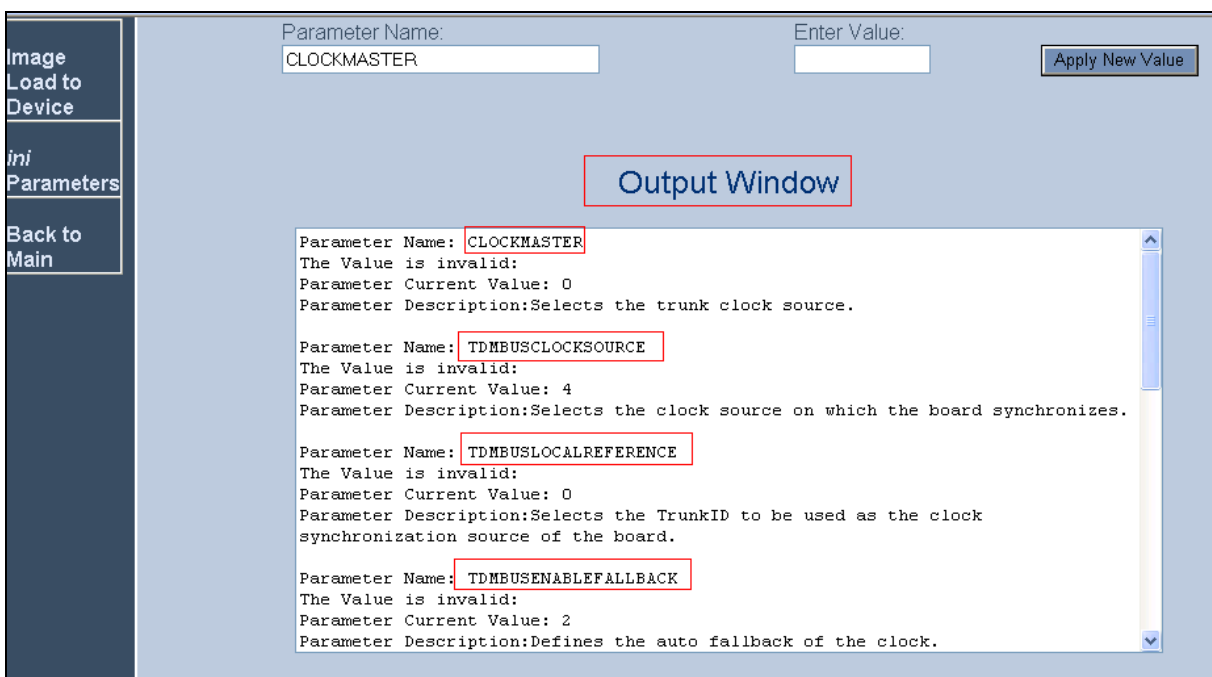


Figure 47: Screen showing Output Window of ini Parameters with example Parameters

8. Verification Steps

The following tests were conducted to verify the solution:

- Basic call features operate successfully between users on both systems.
- E1 connection in the Media Gateway is successfully established when the physical cable is disconnected and connected back.
- Login to the Communication Server 1000 using command line interface (not shown) and verify the status of the D-Channel and D-Channel loop in **LD 96** and **60** respectively.

Figure 48 below shows the D-Channel active and established and the loop enabled with the channels idle.

```
>ld 96
DCH000
.stat dch 5
DCH 005 : OPER      EST  ACTV  AUTO
DES : QSIG_IPC
****
OVL000
>ld 60
DTI000
.stat 10

PRI2 LOOP 10 - ENBL
REF CLK: DSEL
SERVICE RESTORE: YES
ALARM STATUS: ACCEPTABLE
CH 01 - IDLE TIE  VOD *      CH 02 - IDLE TIE  VOD *
CH 03 - IDLE TIE  VOD *      CH 04 - IDLE TIE  VOD *
CH 05 - IDLE TIE  VOD *      CH 06 - IDLE TIE  VOD *
CH 07 - IDLE TIE  VOD *      CH 08 - IDLE TIE  VOD *
CH 09 - IDLE TIE  VOD *      CH 10 - IDLE TIE  VOD *
CH 11 - IDLE TIE  VOD *      CH 12 - IDLE TIE  VOD *
CH 13 - IDLE TIE  VOD *      CH 14 - IDLE TIE  VOD *
CH 15 - IDLE TIE  VOD *      CH 16 - IDLE TIE  VOD *
CH 17 - IDLE TIE  VOD *      CH 18 - IDLE TIE  VOD *
CH 19 - IDLE TIE  VOD *      CH 20 - IDLE TIE  VOD *
CH 21 - IDLE TIE  VOD *      CH 22 - IDLE TIE  VOD *
CH 23 - IDLE TIE  VOD *      CH 24 - IDLE TIE  VOD *
CH 25 - IDLE TIE  VOD *      CH 26 - IDLE TIE  VOD *
CH 27 - IDLE TIE  VOD *      CH 28 - IDLE TIE  VOD *
CH 29 - IDLE TIE  VOD *      CH 30 - IDLE TIE  VOD *
CH 31 - DCH 5
```

Figure 48: CS1000 DCH and Loop Status

- From the Media Gateway web interface, select **VoIP > PSTN Settings > Trunk Settings** to display the **Trunk Settings** screen as shown in **Figure 49** below. Toward the top of the screen, click the applicable trunk port from **Section 6.1**, in this case **1**. Verify that the **Trunk Configuration State** is **Active**.

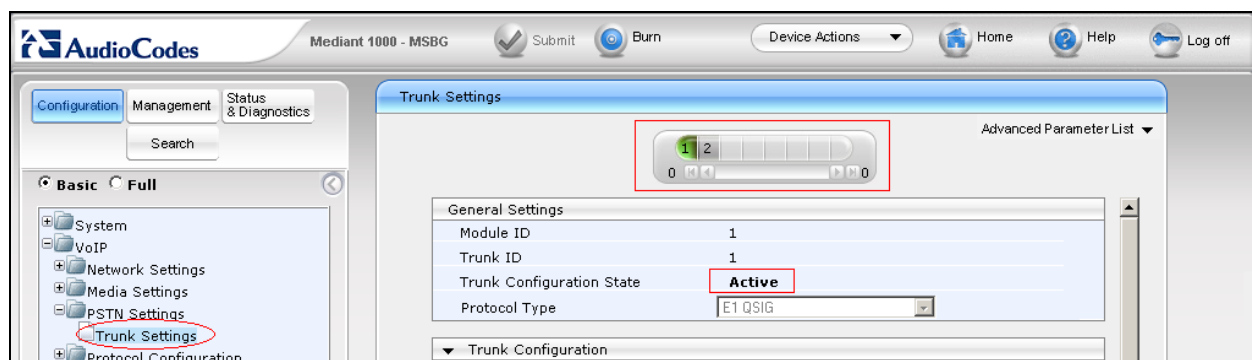


Figure 49: Media Gateway showing Trunk Status Active

9. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy to successfully interoperate with Avaya Communication Server 1000 7.5 using QSIG trunks. All of the executed test cases passed and met the objectives outlined in **Section 2**.

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.

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.