



Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV2 with Avaya Aura® Communication Manager 5.2.1 using QSIG Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager 5.2.1 using QSIG trunks.

IPC UnigyV2 is a trading communication solution. In the compliance testing, IPC UnigyV2 used E1 QSIG trunks to Avaya Aura® Communication Manager, for turret users on IPC to reach users on Avaya Aura® Communication Manager 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 UnigyV2 to interoperate with Avaya Aura® Communication Manager 5.2.1 using QSIG trunks.

The Unigy Platform is a unified trading communications system designed specifically to make the entire trading ecosystem more productive, intelligent and efficient. Based on an SIP-enabled, open and distributed architecture, Unigy utilizes the latest, standards-based technology to create a groundbreaking, innovative Unified Trading Communications (UTC) solution.

Unigy offers a portfolio of devices and applications that serve the entire trading workflow, across the front, middle and back offices.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turrent users with Avaya SIP, Avaya H.323, 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 IPC UnigyV2.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

The serviceability testing focused on verifying the ability of IPC UnigyV2 to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC UnigyV2.

2.2. Test Results

All test cases were executed. The following were the observations on IPC UnigyV2 from the compliance testing.

- Interpretation of DTMF from Avaya is not a supported feature in the current release.

2.3. Support

Technical support on IPC UnigyV2 can be obtained through the following:

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

3. Reference Configuration

As shown in the test configuration below, IPC UnigyV2 at the Remote Site 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 DS1 circuit pack on Avaya Aura® Communication Manager with the IPC Media Gateway. E1 QSIG trunks are used from IPC UnigyV2 to Avaya Aura® Communication Manager, to reach users on Avaya Aura® Communication Manager and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Avaya and IPC sites. Unique extension ranges were associated with Avaya Aura® Communication Manager users at the Avaya site (H.323 – 2200x, SIP – 2800x), and IPC turret users at the IPC site (7205x). The Avaya Aura® SIP Enablement Services was used in the configuration to support Avaya SIP endpoints.

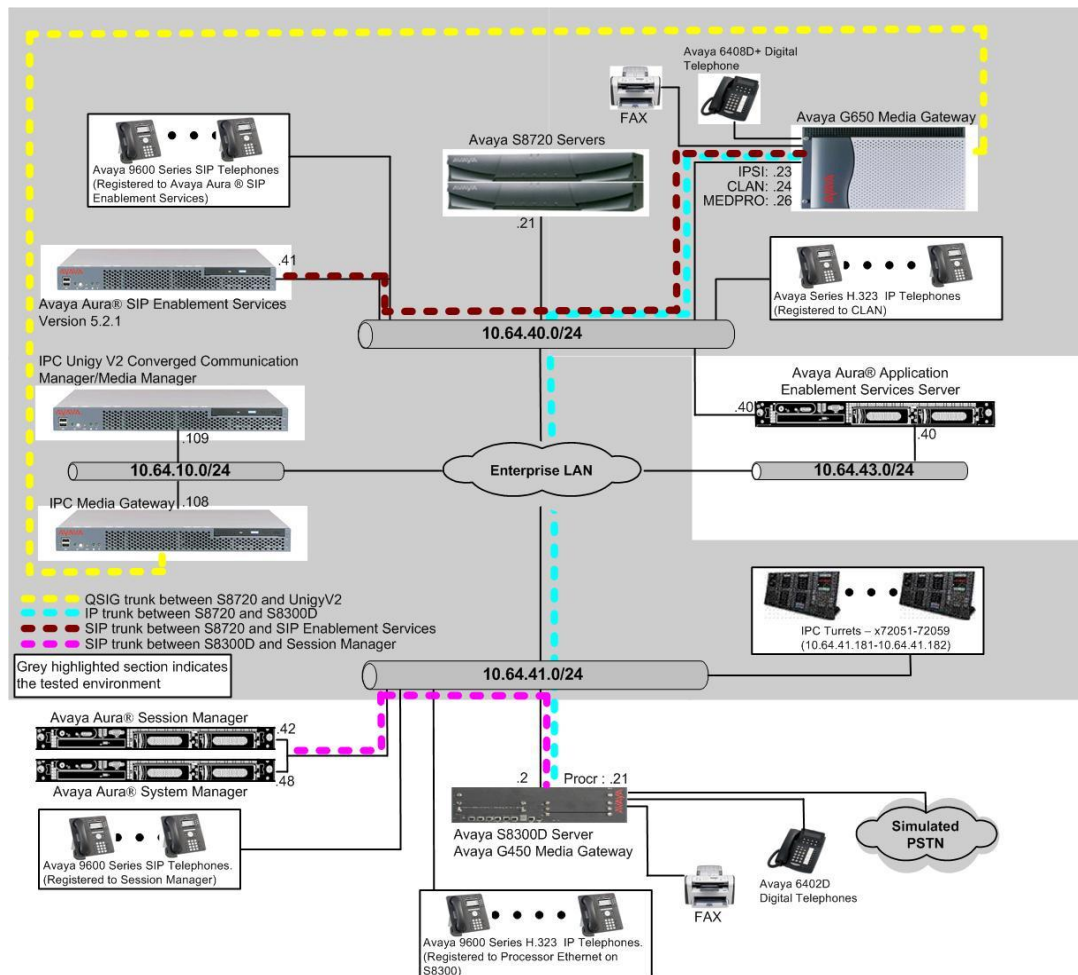


Figure 1: Test Configuration of IPC UnigyV2

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8720 Servers	R015x.02.1.016.4-19880
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack• TN2302AP IP Media Processor• TN464HP	HW01 FW028 HW20 FW118 HW13 FW022
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 9630 IP Telephone (SIP)	2.6.8
IPC UnigyV2 <ul style="list-style-type: none">• Media Manager• Converged Communication Manage• Media Gateway• Turrets	02.00.00.00.1495 02.00.00.00.1495 6.40A.042.004 02.00.00.00.14956

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager license
- Administer system parameters special applications
- Administer system parameters features
- Administer system parameters coverage forwarding
- Administer DS1 circuit pack
- Administer ISDN trunk group
- Administer ISDN signaling group
- Administer trunk group members
- Administer route pattern
- Administer public unknown numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer PSTN trunk group
- Administer tandem calling party number

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 4**, and verify that **ISDN-PRI** is enabled, as shown below.

```
display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? n                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                           ISDN Feature Plus? y
    Enhanced EC500? y         ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                     ISDN-BRI Trunks? n
  Enterprise Wide Licensing? n                                     ISDN-PRI? y
    ESS Administration? y         Local Survivable Processor? n
  Extended Cvg/Fwd Admin? y         Malicious Call Trace? n
  External Device Alarm Admin? n     Media Encryption Over IP? y
Five Port Networks Max Per MCC? n   Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
Forced Entry of Account Codes? y         Multifrequency Signaling? y
  Global Call Classification? n     Multimedia Call Handling (Basic)? y
    Hospitality (Basic)? y         Multimedia Call Handling (Enhanced)? n
  Hospitality (G3V3 Enhancements)? y   Multimedia IP SIP Trunking? n
    IP Trunks? y
IP Attendant Consoles? n
```

Navigate to **Page 8**, and verify the highlighted QSIG features are enabled, as shown below. As a default they are enabled.

```
display system-parameters customer-options           Page 8 of 11
                QSIG OPTIONAL FEATURES

                Basic Call Setup? y
                Basic Supplementary Services? y
                Centralized Attendant? y
                Interworking with DCS? y
                Supplementary Services with Rerouting? y
                Transfer into QSIG Voice Mail? y
                Value-Added (VALU)? y
```

5.2. Administer System Parameters Special Applications

Use the “change system-parameters special-applications” command, and navigate to **Page 3** to enable **(SA8440) – Unmodified QSIG Reroute Number**.

Under the QSIG call forwarding feature, when a call comes into Communication Manager over the ISDN trunk administered for supplementary service option B and terminates to a station with call forwarding activated to an off-net number, Communication Manager sends an ISDN facility message back to the originating switch. This message contains the complete forward-to number that can include dial plan prefixes and route pattern digit manipulation, etc.

The **Unmodified QSIG ReRoute Number** special application allows the option of bypassing the number manipulation for the forwarded-to party.

```
change system-parameters special-applications       Page 3 of 9
                SPECIAL APPLICATIONS

                (SA8141) - LDN Attendant Queue Priority? n
                (SA8143) - Omit Designated Extensions From Displays? n
                (SA8146) - Display Update for Redirected Calls? n
                (SA8156) - Attendant Priority Queuing by COR? n
                (SA8157) - Toll Free Vectoring until Answer? n
                (SA8201) - Start Time and 4-Digit Year CDR Custom Fields? y
                (SA8202) - Intra-switch CDR by COS? n
                (SA8211) - Prime Appearance Preference? n
                (SA8240) - Station User Admin of FBI? n
                (SA8312) - Meet-Me Paging? n
                (SA8323) - Idle Call Preference Display? n
                (SA8339) - PHS X-Station Mobility? n
                (SA8348) - Map NCID to Universal Call ID? n
                (SA8428) - Station User Button Ring Control? n
                (SA8434) - Delay PSTN Connect on Agent Answer? n
                (SA8439) - Forward Held-Call CPN? y
                (SA8440) - Unmodified QSIG Reroute Number? y
                (SA8475) - SOSM? n
```

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

This feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing trunk to IPC (outgoing trunk to outgoing trunk). For ease of compliance testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
      Music/Tone on Hold: none
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of AttD-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n
```

Navigate to **Page 15. Enable Chained Call Forwarding**, to allow changes to the maximum number of call forwarding hops parameter in **Section 5.4**.

```
change system-parameters features                               Page 15 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

SPECIAL TONE
      Special Dial Tone? n
      Special Dial Tone for Digital/IP Stations: none

REDIRECTION NOTIFICATION
      Display Notification for Do Not Disturb? n
      Display Notification for Send All Calls? n
      Display Notification for Call Forward? n
      Display Notification for Enhanced Call Forward? n
      Display Notification for a locked Station? n
      Display Notification for Limit Number of Concurrent Calls? n
      Display Notification for Posted Messages? n
      Scroll Status messages Timer(sec.):

Chained Call Forwarding? y
```


5.4. Administer System Parameters Coverage Forwarding

Use the “change system-parameters coverage-forwarding” command. Set **Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls** to the desired value. In the compliance testing, the threshold was disabled so that there will be no blocking on the number of calls being redirected off-net within the Call Forward timer.

```
change system-parameters coverage-forwarding                               Page 1 of 2
                                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

CALL COVERAGE/FORWARDING PARAMETERS
    Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
    Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
    Coverage - Caller Response Interval (seconds): 4
    Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: n
    Location for Covered and Forwarded Calls: called
    PGN/TN/COR for Covered and Forwarded Calls: caller
    COR/FRL check for Covered and Forwarded Calls? n
    QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path? n
COVERAGE
    Keep Held SBA at Coverage Point? y
    External Coverage Treatment for Transferred Incoming Trunk Calls? n
    Immediate Redirection on Receipt of PROGRESS Inband Information? n
    Maintain SBA At Principal? n
    QSIG VALU Coverage Overrides QSIG Diversion with Rerouting? n
    Station Hunt Before Coverage? n
FORWARDING
    Call Forward Override? n
    Coverage After Forwarding? y
```

On Page2, verify the **Maximum Number Of Call Forwarding Hops** is set. The following screen shows the default settings.

```
change system-parameters coverage-forwarding                               Page 2 of 2
                                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)

    Coverage Of Calls Redirected Off-Net Enabled? n

CHAINED CALL FORWARDING
    Maximum Number Of Call Forwarding Hops: 6
    Station Coverage Path For Coverage After Forwarding: init@S8720T
```

5.5. Administer DS1 Circuit Pack

Use the “add ds1 x” command, where “x” is the slot number of the DS1 circuit pack with physical connectivity to IPC. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name
- **Line Coding:** “hdb3”
- **Signaling Mode:** “isdn-pri”
- **Connect:** “pbx”
- **Interface:** “peer-master”
- **Peer Protocol:** “Q-SIG”
- **Side:** “a”
- **Interface Companding:** “mulaw”
- **CRC:** “y”
- **Channel Numbering:** “timeslot”

```
add ds1 1a09                                     Page 1 of 1
DS1 CIRCUIT PACK
Location: 01A09                                Name: QSIG-E1-IPC
Bit Rate: 2.048                                Line Coding: hdb3
Signaling Mode: isdn-pri
Connect: pbx                                    Interface: peer-master
TN-C7 Long Timers? n                            Peer Protocol: Q-SIG
interworking Message: PROgress                  Side: a
Interface Companding: mulaw                     CRC? y
Idle Code: 11111111                            Channel Numbering: timeslot
DCP/Analog Bearer Capability: 3.1kHz
T303 Timer(sec): 4
Disable Restarts? n
Slip Detection? n                               Near-end CSU Type: other
```

5.6. Administer ISDN Trunk Group

Administer an ISDN trunk group to interface with IPC. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “isdn”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”
- **Carrier Medium:** “PRI/BRI”
- **Service Type:** “tie”

```
add trunk-group 80                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 80                                     Group Type: isdn                                     CDR Reports: y
Group Name: ElQSIG-IPC                               COR: 1                                     TN: 1                                     TAC: 1080
Direction: two-way                                   Outgoing Display? n                       Carrier Medium: PRI/BRI
Dial Access? n                                       Busy Threshold: 255   Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n                               TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```

Navigate to **Page 2**. For **Supplementary Service Protocol**, enter “b” for QSIG. For **Digit Handling (in/out)**, enter “enbloc/enbloc”. Retain the default values for the remaining fields.

```
add trunk-group 80                                     Page 2 of 21
  Group Type: isdn

TRUNK PARAMETERS
  Codeset to Send Display: 6                         Codeset to Send National IEs: 6
  Max Message Size to Send: 260                     Charge Advice: none
Supplementary Service Protocol: b                     Digit Handling (in/out): enbloc/enbloc

Trunk Hunt: cyclical

Incoming Calling Number - Delete:                    Insert:                    Digital Loss Group: 13
  Bit Rate: 1200                                     Synchronization: async   Format:
Disconnect Supervision - In? y   Out? y             Duplex: full
Answer Supervision Timeout: 0
Administer Timers? n                     CONNECT Reliable When Call Leaves ISDN? n
```

Navigate to **Page 3**. Enable **Send Name**, **Send Calling Number**, and **Send Connected Number**. For **Format**, enter “private”.

add trunk-group 80		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Wideband Support? n
	Internal Alert? n	Maintenance Tests? y
	Data Restriction? n	NCA-TSC Trunk Member: 30
	Send Name: y	Send Calling Number: y
Used for DCS? n	Hop Dgt? n	Send EMU Visitor CPN? n
Suppress # Outpulsing? n	Format: private	
Outgoing Channel ID Encoding: preferred	UII IE Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Send Called/Busy/Connected Number: y	
	Hold/Unhold Notifications? y	
Send UII IE? y	Modify Tandem Calling Number? n	
Send UCID? n		
Send Codeset 6/7 LAI IE? y	Dsl Echo Cancellation? n	
Apply Local Ringback? n		
Show ANSWERED BY on Display? y		
	Network (Japan) Needs Connect Before Disconnect? n	

5.7. Administer ISDN Signaling Group

Administer an ISDN signaling group for the new trunk group to use for signaling. Use the “add signaling-group n” command, where “n” is an available signaling group number. For **Primary D-Channel**, enter the slot number for the DS1 circuit pack from **Section 5.5** and port “16”. Set desired values for **Max number of NCA TSC** and **Max number of CA TSC**.

For **Trunk Group for NCA TSC** and **Trunk Group for Channel Selection**, enter the ISDN trunk group number from **Section 5.6**. For **TSC Supplementary Service Protocol**, enter “b” for QSIG. Retain the default values for the remaining fields.

add signaling-group 80		Page 1 of 1
SIGNALING GROUP		
Group Number: 80	Group Type: isdn-pri	
Associated Signaling? y		Max number of NCA TSC: 30
Primary D-Channel: 01A0916		Max number of CA TSC: 30
	Trunk Group for NCA TSC: 80	
Trunk Group for Channel Selection: 80		
TSC Supplementary Service Protocol: b	Network Call Transfer? n	

5.8. Administer Trunk Group Members

Use the “change trunk-group n” command, where “n” is the ISDN trunk group number added in **Section 5.6**. Navigate to **Page 3**. For **NCA-TSA Trunk Member**, enter the highest trunk group member number to use for routing of tandem QSIG call independent signaling connections.

```
change trunk-group 80                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n          Measured: none          Wideband Support? n
                             Internal Alert? n        Maintenance Tests? y
                             Data Restriction? n      NCA-TSC Trunk Member: 30
                             Send Name? y            Send Calling Number? y
                             Hop Dgt? n              Send EMU Visitor CPN? n
  Used for DCS? n
  Suppress # Outpulsing? n  Format: private
  Outgoing Channel ID Encoding: preferred  UII IE Treatment: service-provider

                             Replace Restricted Numbers? n
                             Replace Unavailable Numbers? n
                             Send Called/Busy/Connected Number? y
                             Hold/Unhold Notifications? y
                             Modify Tandem Calling Number? n
  Send UII IE? y
  Send UCID? n
  Send Codeset 6/7 LAI IE? y          Dsl Echo Cancellation? n

  Apply Local Ringback? n
  Show ANSWERED BY on Display? y
                                   Network (Japan) Needs Connect Before Disconnect? n
```

Navigate to **Page 5** and **6**. Enter all 30 ports of the DS1 circuit pack into the **Port** fields, and the corresponding **Code** and **Sfx** fields will be populated automatically. Enter the ISDN signaling group number from **Section 5.7** into the **Sig Grp** fields as shown below.

```
change trunk-group 80                                     Page 5 of 21
TRUNK GROUP
  Administered Members (min/max): 1/30
GROUP MEMBER ASSIGNMENTS  Total Administered Members: 30

  Port   Code Sfx Name      Night      Sig Grp
1: 01A0901 TN464 G          Night      80
2: 01A0902 TN464 G          Night      80
3: 01A0903 TN464 G          Night      80
4: 01A0904 TN464 G          Night      80
5: 01A0905 TN464 G          Night      80
6: 01A0906 TN464 G          Night      80
7: 01A0907 TN464 G          Night      80
8: 01A0908 TN464 G          Night      80
9: 01A0909 TN464 G          Night      80
10: 01A0910 TN464 G          Night      80
11: 01A0911 TN464 G          Night      80
12: 01A0912 TN464 G          Night      80
13: 01A0913 TN464 G          Night      80
14: 01A0914 TN464 G          Night      80
15: 01A0915 TN464 G          Night      80
```

change trunk-group 80						Page	6 of 21
						TRUNK GROUP	
						Administered Members (min/max):	1/30
GROUP MEMBER ASSIGNMENTS						Total Administered Members:	30
	Port	Code	Sfx	Name	Night	Sig	Grp
16:	01A0917	TN464	G			80	
17:	01A0918	TN464	G			80	
18:	01A0919	TN464	G			80	
19:	01A0920	TN464	G			80	
20:	01A0921	TN464	G			80	
21:	01A0922	TN464	G			80	
22:	01A0923	TN464	G			80	
23:	01A0924	TN464	G			80	
24:	01A0925	TN464	G			80	
25:	01A0926	TN464	G			80	
26:	01A0927	TN464	G			80	
27:	01A0928	TN464	G			80	
28:	01A0929	TN464	G			80	
29:	01A0930	TN464	G			80	
30:	01A0931	TN464	G			80	

5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach IPC, in this case “80”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The ISDN trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 80										Page	1 of 3
Pattern Number: 80 Pattern Name: To PSTN via G3r											
SCCAN? n Secure SIP? n											
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC			
No			Mrk	Lmt	List	Del	Digits	QSIG			
								Intw			
1: 80 0										n	user
2:										n	user
3:										n	user
4:										n	user
5:										n	user
6:										n	user
BCC VALUE		TSC	CA-TSC	ITC BCIE		Service/Feature		PARM	No.	Numbering	LAR
0 1 2 M 4 W			Request						Dgts	Format	
										Subaddress	
1:	y	y	y	y	y	n	n	rest		none	
2:	y	y	y	y	y	n	n	rest		none	
3:	y	y	y	y	y	n	n	rest		none	

5.10. Administer Public Unknown Numbering

Use the “change public-unknown-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 5-digit extension beginning with 2 and routed to trunk group 80 will result in a 5-digit calling number.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	2	80		5	Total Administered: 11
					Maximum Entries: 9999

5.11. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 720xx to IPC. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 720xx, as shown below.

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching			Insert		Node
Pattern	Len	Del	Digits	Net Conv	Num
720	5	0		aar	n

5.12. Administer AAR Analysis

Use the “change aar analysis 7” command, and add an entry to specify how to route calls to 7205x. In the example shown below, calls with digits 7205x will be routed as an AAR call using route pattern “80”.

change aar analysis 7					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 2
Dialed	Total	Route	Call	Node	ANI
String	Min Max	Pattern	Type	Num	Reqd
7205	5 5	80	aar		n

5.13. Administer PSTN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing ISDN trunk group number used to reach the PSTN, in this case “10”.

For **Modify Tandem Calling Number**, enter “y” to allow for the calling party number from IPC to be modified.

```
change trunk-group 10                                     Page 3 of 22
TRUNK FEATURES
    ACA Assignment? n                                     Measured: none
    Internal Alert? n                                     Maintenance Tests? y
    Data Restriction? n                                   NCA-TSC Trunk Member:
    Send Name: y                                          Send Calling Number: y
    Used for DCS? n                                       Send EMU Visitor CPN? n
    Suppress # Outpulsing? n                               Format: private
    UI IE Treatment: shared
    Maximum Size of UI IE Contents: 128
    Replace Restricted Numbers? n
    Replace Unavailable Numbers? n
    Send Connected Number: n
    Hold/Unhold Notifications? n
    Modify Tandem Calling Number? y
    BSR Reply-best DISC Cause Value: 31
Network Call Redirection: none
    Send UI IE? y
    Send UCID? y
    Send Codeset 6/7 LAI IE? y
```

5.14. Administer Tandem Calling Party Number

Use the “change tandem-calling-party-num” command, to define the calling party number to send to the PSTN for tandem calls from IPC turret users.

In the example shown below, all calls originating from a 5-digit extension beginning with 7205 and routed to trunk group 10, will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

```
change tandem-calling-party-num                           Page 1 of 8
CALLING PARTY NUMBER CONVERSION
FOR TANDEM CALLS
    Incoming      Outgoing
    Number      Number
    Trk
    CPN
    Len Prefix   Format Grp(s) Delete Insert Format
    5  7205      10      3035383547 pub-unk
```

After all configuration changes, perform **save translation** to save changes.

6. Configure IPC Converged Communications Server

This section provides the procedures for configuring IPC Media Manager and Media Gateway. 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
- 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.

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 below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

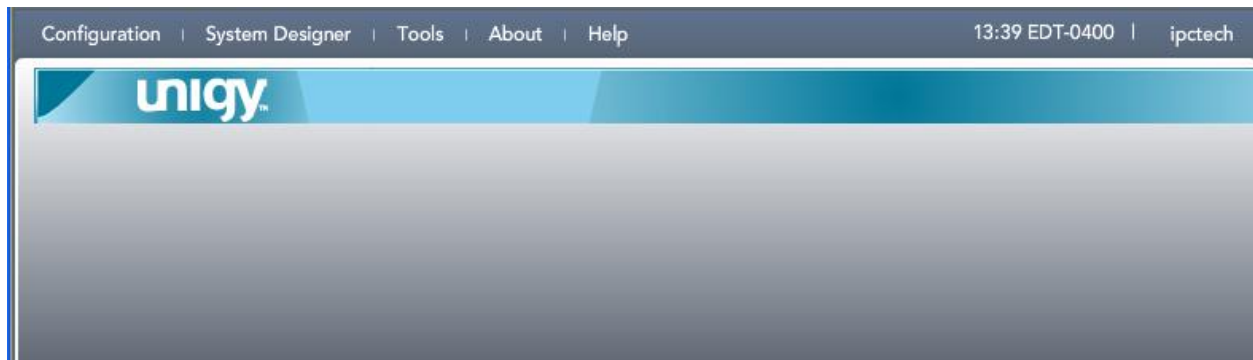
In the subsequent screen (not shown), click **Continue**.



The screenshot shows the login interface for the IPC Unigy Management System. It features the IPC logo on the left. To the right of the logo are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a link to 'Terms of Use'. A 'Login' button is positioned to the right of the checkbox. At the bottom of the form, the following text is displayed: 'IPC Unigy™ Management System', 'Unigy™ Version 02.00.00.00.1495', and '© Copyright 2012 IPC Systems, Inc.'

6.2. Administer Media Gateway

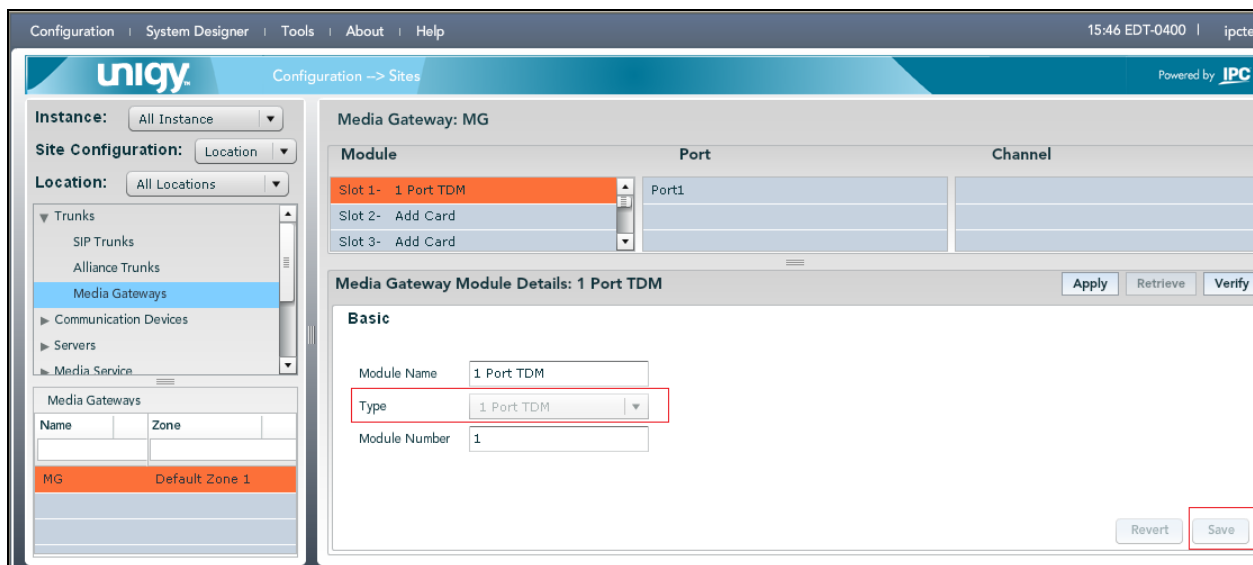
The screen below is displayed next. Select **Configuration** → **Sites** from the top menu.



The **Sites** information is 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”.

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 “1 Port TDM” for **Type**, and click **Save**.



In the updated screen, 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. For **Protocol Type**, select “E1 QSIG”. Retain the default values for the remaining fields.

Click **Save** (not shown), followed by **Apply**.


The screenshot displays the UniGy Configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The main header shows 'unigy Configuration --> Sites' and 'Powered by IPC'. The left sidebar contains a tree view with categories like 'Trunks', 'Media Gateways', 'Communication Devices', 'Servers', 'Media Service', 'Prototype Devices', 'SNMP Forwarding', and 'Routing'. The 'Media Gateways' section is expanded, showing a table with columns 'Name' and 'Zone'. The table lists 'MG' under 'Default Zone 1'. The main content area is titled 'Media Gateway: MG' and features a table with columns 'Module', 'Port', and 'Channel'. The 'Port' column is highlighted, showing 'Port1'. Below this, the 'Media Gateway Port Details: Port1' section is visible, with tabs for 'Port Properties' and 'ISDN'. The 'Port Properties' tab is active, showing a 'Basic' configuration. The 'Protocol Type' field is highlighted with a red box and set to 'E1 QSIG'. Other fields include 'Distant End Name', 'PBX Trunk Group Reference', 'Trunk Info', 'Alliance ICM Trunk', 'Trunk' (set to 'ISDN'), 'Alliance Site', 'Alliance Site IP Address', 'Clock Master' (set to 'CLOCK-MASTER-OFF'), 'Line Code' (set to 'HDB3'), 'Far End Connection' (set to 'PBX'), and 'Framing Method' (set to 'E1-FRAMING-MFF-CR').

Module	Port	Channel
Slot 1- 1 Port TDM	Port1	
Slot 2- Add Card		
Slot 3- Add Card		
Slot 4- Add Card		
Slot 5- Add Card		
Slot 6- Add Card		

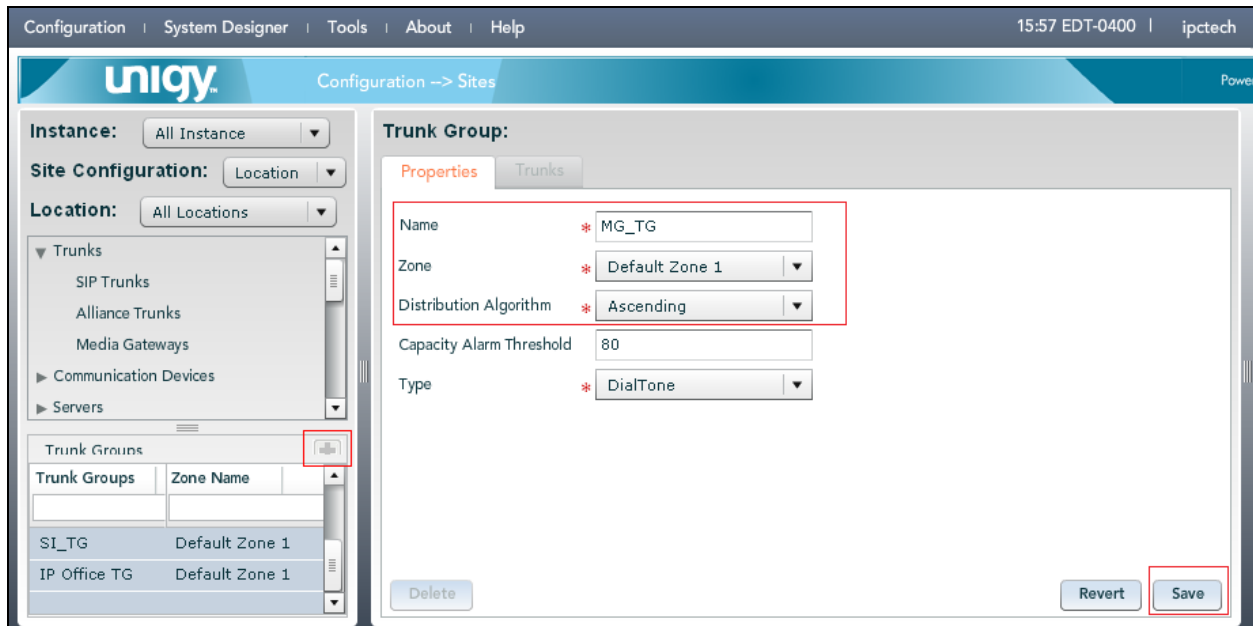
Name	Zone
MG	Default Zone 1

Media Gateway Port Details: Port1	
Port Properties	
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
Protocol Type	E1 QSIG
Alliance ICM Trunk	<input type="checkbox"/>
Trunk	ISDN
Alliance Site	
Alliance Site IP Address	
Clock Master	CLOCK-MASTER-OFF
Line Code	HDB3
Far End Connection	PBX
Framing Method	E1-FRAMING-MFF-CR

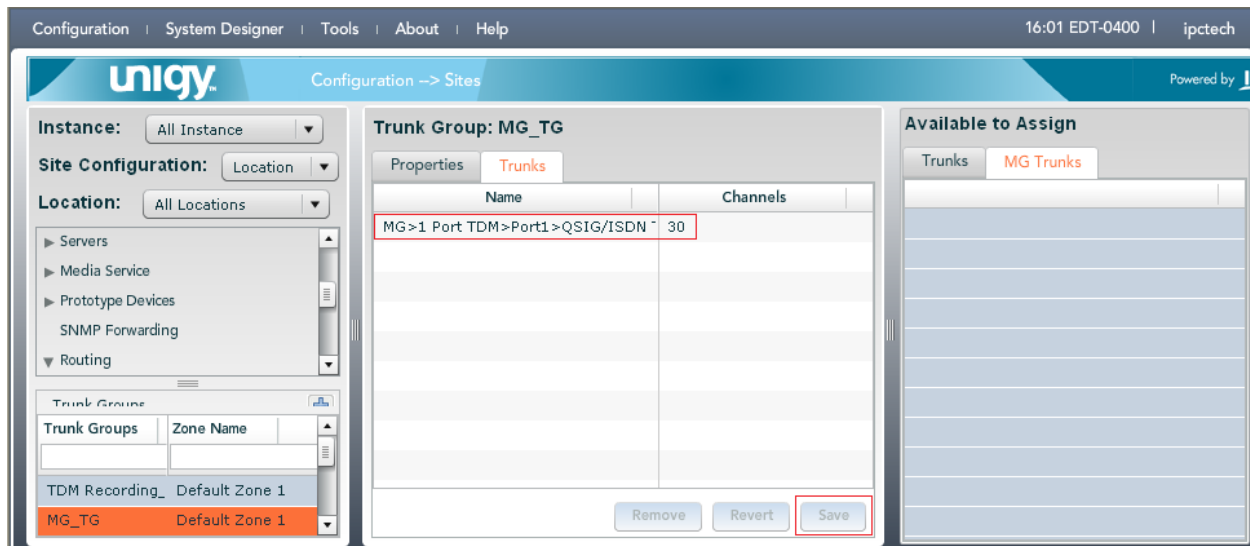
6.3. Administer Trunk Groups

Select **Routing** → **Trunk Groups** (not shown) in the left pane, and click the **Add** icon () in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, select “Default Zone 1” for the **Zone** Field, select a Distribution Algorithm, and click **Save**. Select the **Trunks** tab in the right pane.



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 from **Section 6.2** and drag the selection to the **Name** column in the middle pane as shown below. Click **Save**.



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.

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

The screenshot shows the UniV2 configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Tools', 'About', and 'Help'. The main header displays 'unigy Configuration -> Sites' and 'Powered by IPC'. The left sidebar shows a tree view with 'Route Lists' selected. The central pane is titled 'Route List : Route List' and contains the following fields:

- Route List: * RL_MG
- Description:
- Instance: * Default Instance
- Type: * DialTone
- Alliance Site Id:

Below these fields is a section titled 'Assigned Trunk Groups on Route List. You can remove or add Trunk Groups' containing a list with 'MG_TG'. At the bottom of the central pane are 'Revert', 'Delete', and 'Save' buttons.

The right sidebar is titled 'Available to Assign' and shows a list of trunk groups: 'MG_TG' (highlighted), 'SI_TG', and 'IP Office TG'. Above this list is a 'Trunk Groups' section with a table containing 'TDM Recording_DoNotChange'.

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.

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 endpoints, in this case “*”, meaning any digit. For **Zone**, select “Default Zone 1”. Click **Save**.

Configuration | System Designer | Tools | About | Help 16:18 EDT-0400 | ipctech

Configuration --> Sites

Instance: All Instance

Site Configuration: Location

Location: All Locations

Trunks

Communication Devices

Servers

Media Service

Prototype Devices

SNMP Forwarding

Routing

Trunk Groups

Route Lists

Dial Patterns

Route Plans

Trunk Dial Plans

Trunk Dial Plan Rules

Name	Pattern String	Description	Zone Name
all	*	all	Default Zone 1

Add New Delete

Dial pattern Details

Properties

Name * all

Zone * Default Zone 1

Description * all

Pattern String * *

Revert Save

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.

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 UnigyV2. For **Destination**, enter “*” to denote any called party from UnigyV2. Select “Forward” for **Action**. Select “Default Instance” for **Instance**, and click **Save**.

The screenshot shows the 'Create New Route Plan' form in the Unigy Configuration -> Sites interface. The form fields are:

- UI Name: all
- Description: (empty)
- Calling Party: *
- Destination: *
- Action: Forward
- Instance: Default Instance

The 'Save' button is highlighted in red.

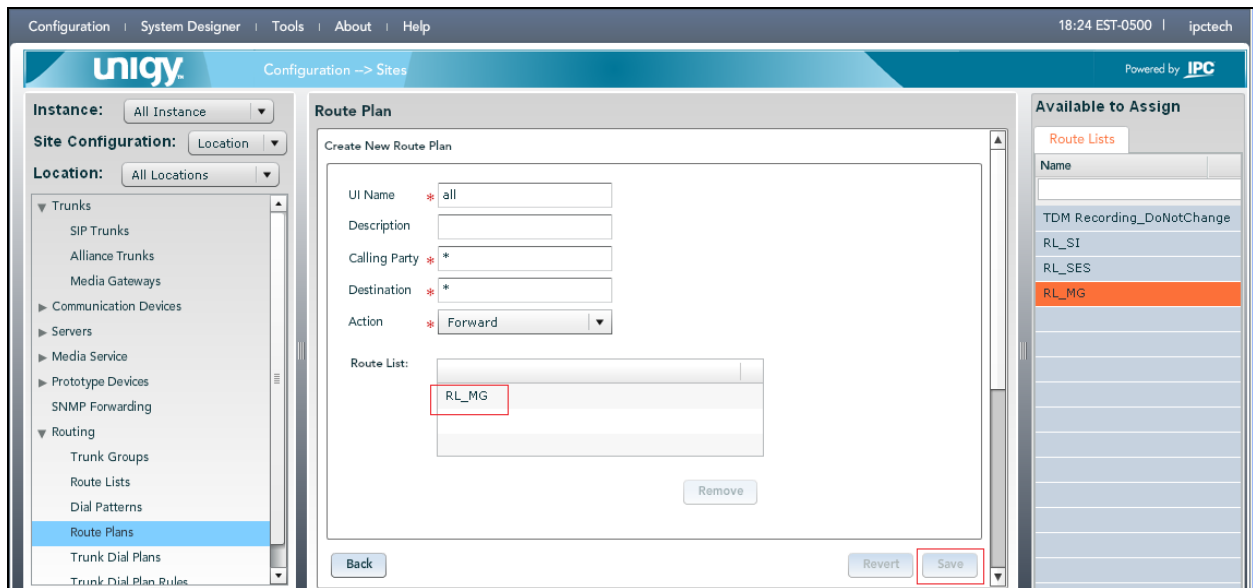
The screen is updated with the newly created route plan. Select the route plan, and click **Edit** under Route Plan Details section toward the bottom of the screen (not shown).

The screenshot shows the 'List of Route Plans' table in the Unigy Configuration -> Sites interface. The table has the following columns: UI Name, Calling Party, Destination, Action, and Instance Name. The first row is highlighted with a red box.

UI Name	Calling Party	Destination	Action	Instance Name
all	*	*	FORWARD	Default Instance

Buttons at the bottom: Delete, Add New, Revert, Save Sequence Change.

The screen is updated with three panes again, as shown below. In the right pane, select the route list and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save**.



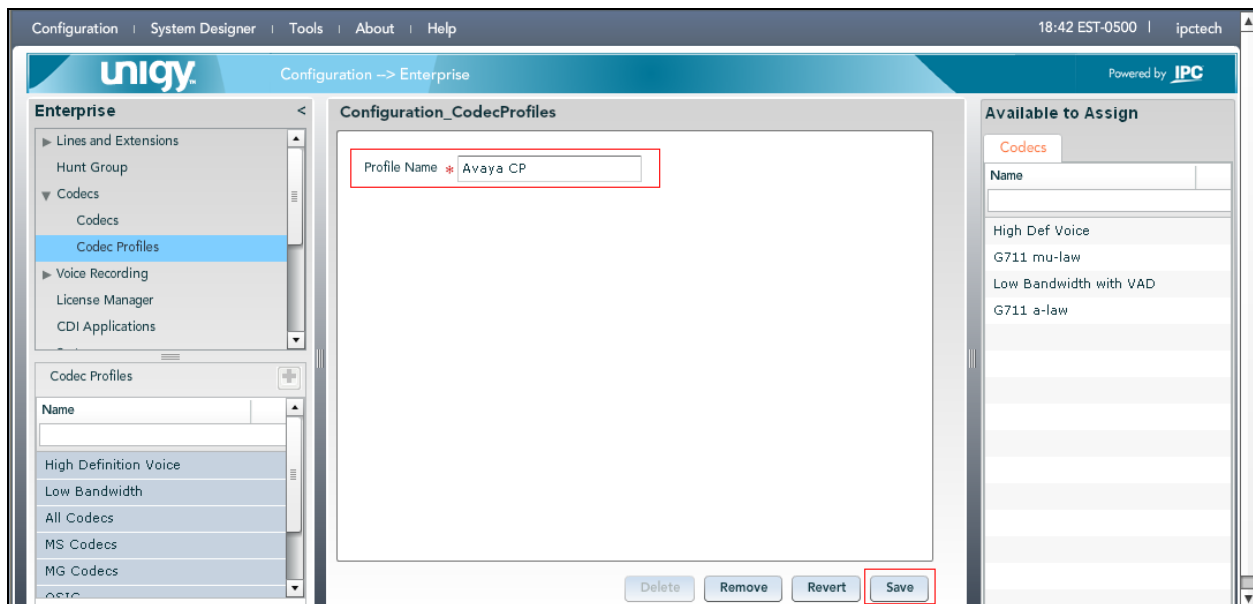
6.7. Administer Codecs

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

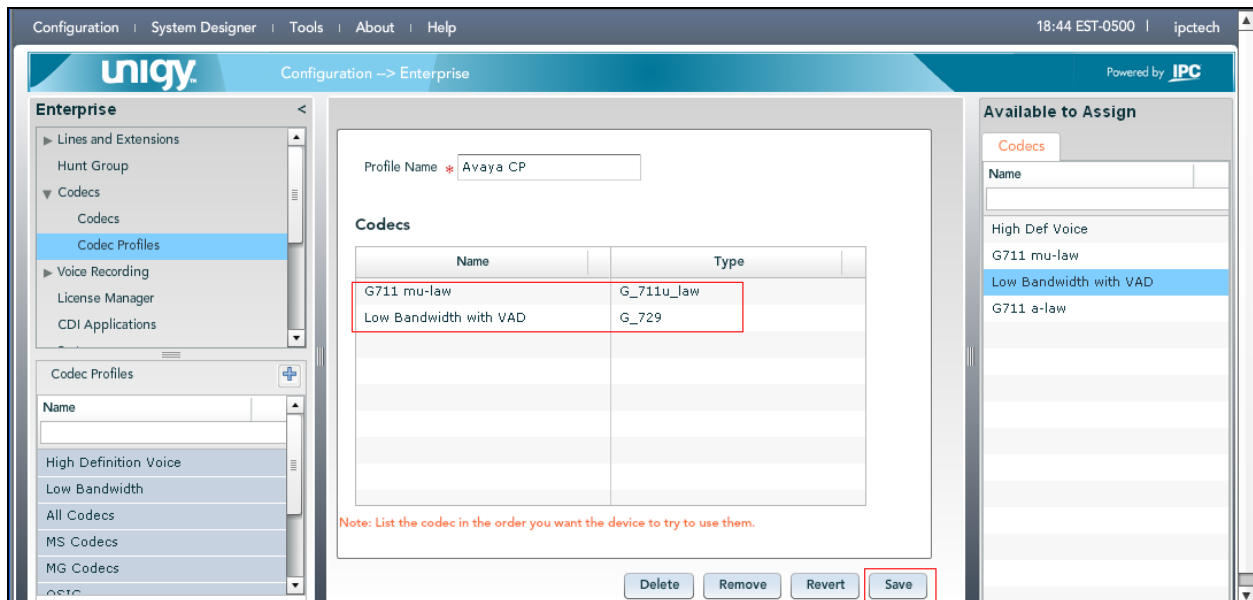
- Administer codec profile
- Assign codec profile to user
- Assign codec profile to turret

6.7.1. Administer Codec Profile

Select **Configuration → Enterprise → Codecs → Codec Profiles**, and click **Add New** in the left pane to create a new codec profile. Provide a profile name, and click **Save**.

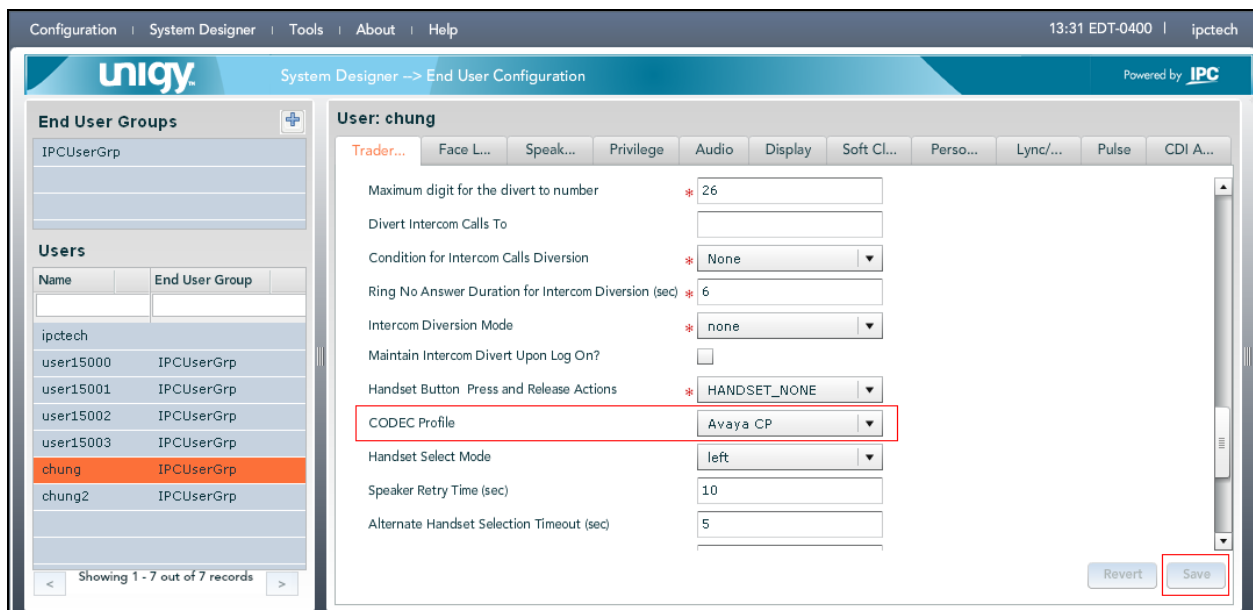


After saving the codec profile, the following screen is displayed. In the right pane, select the available codecs and drag into the **Codecs** sub-section in the middle pane, as shown below. Click **Save**.



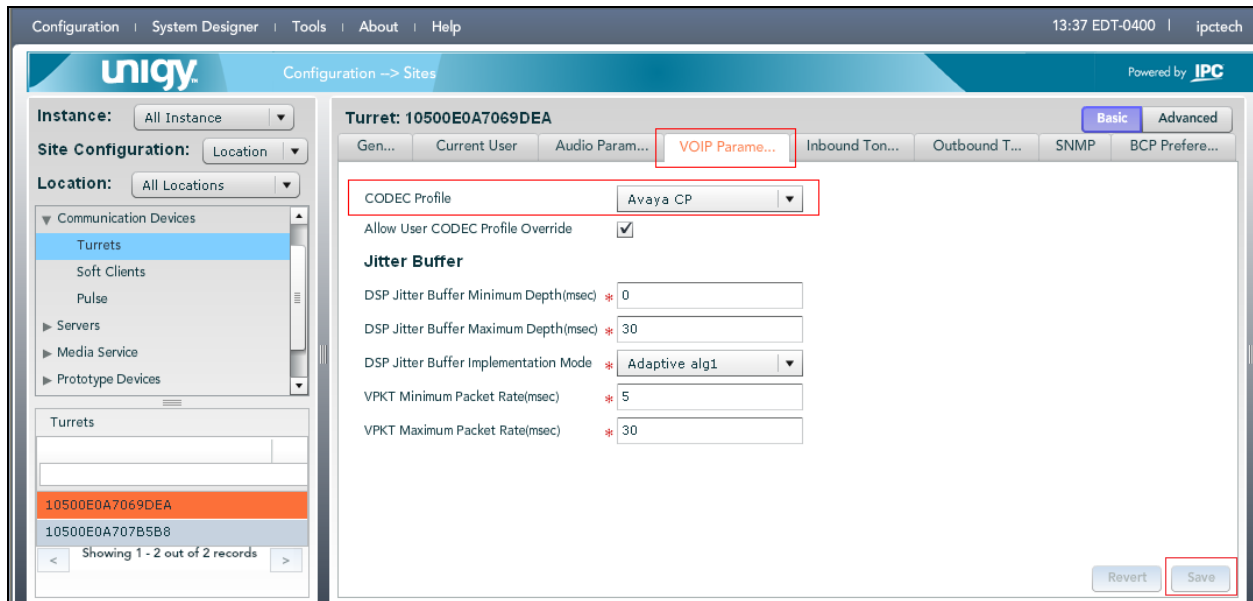
6.7.2. Assign Codec Profile to User

Select **System Designer -> End User Configuration**, and select a user to associate a codec profile with. Provide a profile name, and click **Save**.



6.7.3. Assign Codec Profile to Turret

Navigate to **Configuration** → **Sites** → **Communication Devices** → **Turrets** and select a turret to associate a codec profile with. Click the **VoIP Parame...** tab in the right pane. Select a codec, and click **Save**.



After codecs are configured, reboot the turret.

7. Configure IPC Media Gateway

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

- Administer codecs
- Administer the TDM Bus setting

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.

7.1. Administer Codecs

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 using the appropriate credentials.

Navigate to **Configuration → VOIP → Coders And Profiles → Coders** in the left pane. Enter codecs that will be used. Click **Submit** (✓).

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-IaW	20	64	0	Disabled
G.711A-IaW	20	64	8	Disabled
G.729	20	8	18	Disabled

7.2. Administer TDM Bus

Navigate to **Configuration → VOIP → TDM → TDM Bus Settings** in the left pane. Enter codecs that will be used. During the compliance test, MuLaw was utilized. For the TDM Bus Clock Source field, set to Internal, meaning Avaya side is master and IPC side is slave. After the configuration changes, press the **Burn** button, and reset **Media Gateway**. Click **Submit**.

TDM Bus Settings	
PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
TDM Bus PSTN Auto FallBack Clock	Enable
TDM Bus PSTN Auto Clock Reverting	Disable
Idle PCM Pattern	255
Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1
TDM Bus Type	Framers

Submit

Note: Interface Companding in Avaya side is set to mulaw (Refer to Section 5.5)

8. Configure Media Manager

This section provides the procedures for administering codec. Access the Media Manager web interface by using the URL “http://,<CCM ip-address>/swms” in an Internet browser window.

Navigate to **Configuration → Node Configuration → Configure SIP Audio Codec List**, and prioritize codecs.

The screenshot displays the IPC Configuration web interface. At the top, there is a header with the IPC logo and a 'Configuration' tab. Below the header, a status bar shows 'Alarms: Critical:0 Major:0 Minor:0'. The main content area is titled 'Configure SIP Audio Codec List'. On the left, a navigation menu lists various configuration options, including 'Node Configuration', 'Show SIP Audio Codec List', 'Show H.248 Audio Codec List', 'Show MRCP', 'Show Audio Jitter Buffer', 'Templates', 'Show NFS Configuration', 'Show SNMP Agent Configuration', 'Show SNMP Trap Destinations', 'Show Date and Time', 'Show Video Configuration', 'Show Video Codec List', 'Show Video Recording Configuration', 'Show Resource Management Configuration', 'Show VoiceXML Configuration', 'Show Conference Configuration', 'Show Fax Codec List', 'Show Call Progress Analysis Configuration', 'Show Clip Path Translation', 'Show Core Allocation', 'Set Node Service Mode', 'Manage Control Protocols', 'Configure MRCP', 'Configure SIP', 'Configure H.248', 'Configure Video Jitter Buffer', 'Configure Audio Jitter Buffer', 'Templates', 'Configure Media ICMP', and 'Configure SIP Audio Codec List'. The 'Configure SIP Audio Codec List' option is selected. The main area contains seven codec configuration fields: 'Codec #1:', 'Codec #2:', 'Codec #3:', 'Codec #4:', 'Codec #5:', 'Codec #6:', and 'Codec #7:'. Each field has a dropdown menu with the following values: 'pomu', 'poma', 'g729', 'telephone-events', 'none', 'none', and 'none' respectively. Below the codec fields are 'Execute' and 'Reset Fields' buttons. At the bottom, there is an 'Output Messages:' section with a text area and a scroll bar. A 'Help?' button is located in the top right corner.

After codecs are prioritized, reboot **CCM**.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager and IPC UnigyV2.

9.1. Verify Avaya Aura® Communication Manager

From the Communication Manager SAT interface, verify the status of the ISDN trunk group by using the “status trunk n” command, where “n” is the ISDN trunk group number administered in **Section 5.6**. Verify that all trunks are in the “in-service/idle” state as shown below.

status trunk 80				Page 1
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0080/001	01A0901	in-service/idle	no	
0080/002	01A0902	in-service/idle	no	
0080/003	01A0903	in-service/idle	no	
0080/004	01A0904	in-service/idle	no	
0080/005	01A0905	in-service/idle	no	
0080/006	01A0906	in-service/idle	no	
0080/007	01A0907	in-service/idle	no	
0080/008	01A0908	in-service/idle	no	
0080/009	01A0909	in-service/idle	no	
0080/010	01A0910	in-service/idle	no	
0080/011	01A0911	in-service/idle	no	
0080/012	01A0912	in-service/idle	no	
0080/013	01A0913	in-service/idle	no	
0080/014	01A0914	in-service/idle	no	

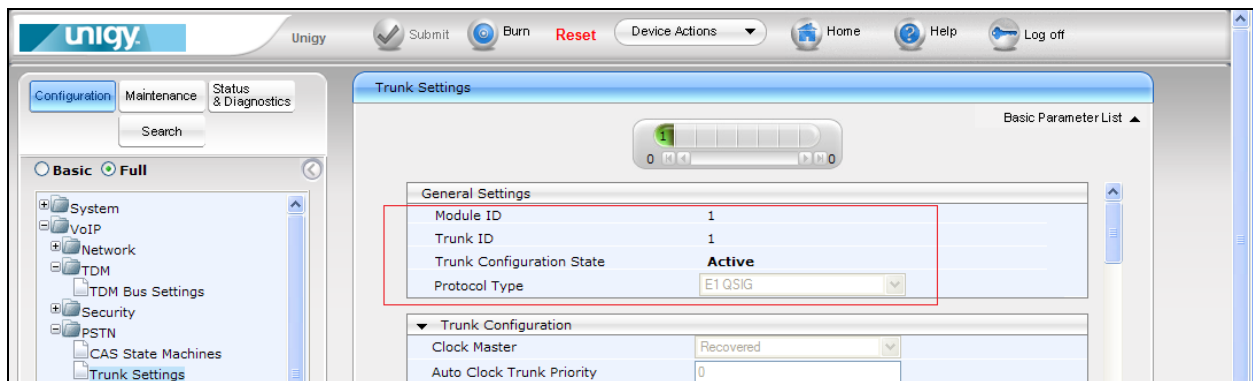
Verify the status of the ISDN signaling groups by using the “status signaling-group n” command, where “n” is the ISDN signaling group number administered in **Section 5.7**. Verify that the signaling group is “in-service” as indicated in the **Group State** and **Level 3 State** fields shown below.

status signaling-group 80	
STATUS SIGNALING GROUP	
Group ID: 80	Active NCA-TSC Count: 0
Group Type: isdn-pri	Active CA-TSC Count: 0
Signaling Type: facility associated signaling	
Group State: in-service	
Primary D-Channel	
Port: 01A0916	Level 3 State: in-service
Secondary D-Channel	
Port:	Level 3 State: no-link

9.2. Verify IPC UnigyV2

From the Media Gateway web interface, select **VoIP → PSTN → Trunk Settings** to display the **Trunk Settings** screen.

Toward the top of the screen, click the applicable trunk port, in this case “1”. Verify that the **Trunk Configuration State** is “Active”, as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for IPC UnigyV2 to successfully interoperate with Avaya Aura® Communication Manager 5.2.1 using QSIG trunks. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *UnigyV2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

©2013 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.