

RCP2-1000-CO

Remote Control Panel Operations Manual



**For use with any Paradise Datacom Compact Outdoor SSPA
or High Power Outdoor SSPA**

Teledyne Paradise Datacom
328 Innovation Blvd.
State College, PA 16803 USA
Email: sales@paradisedata.com

Phone: (814) 238-3450
Fax: (814) 238-3829
Web: www.paradisedata.com

Teledyne Paradise Datacom, a division of Teledyne Wireless LLC, is a single source for high power solid state amplifiers (SSPAs), Low Noise Amplifiers (LNAs), Block Up Converters (BUCs), and Modem products. Operating out of two primary locations, Witham, United Kingdom, and State College, PA, USA, Teledyne Paradise Datacom has a more than 20 year history of providing innovative solutions to enable satellite uplinks, battlefield communications, and cellular backhaul.

Teledyne Paradise Datacom
328 Innovation Blvd., Suite 100
State College, PA 16803 USA
(814) 238-3450 (switchboard)
(814) 238-3829 (fax)

Teledyne Paradise Datacom Ltd.
2&3 The Matchyns, London Road, Rivenhall End
Witham, Essex CM8 3HA England
+44 (0) 1376 515636
+44 (0) 1376 533764 (fax)

Information in this document is subject to change without notice. The latest revision of this document may be downloaded from the company web site: <http://www.paradisedata.com>.

Use and Disclosure of Data

The items described herein are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Proprietary and Confidential

The information contained in this document is the sole property of Teledyne Paradise Datacom. Any reproduction in part or as a whole without the written permission of Teledyne Paradise Datacom is prohibited.

All other company names and product names in this document are property of the respective companies.

Section 1: General Information	11
1.0 Introduction.....	11
1.1 Description.....	11
1.2 Equipment Supplied	12
1.3 Safety Considerations	12
1.3.1 High Voltage Hazards	12
1.3.2 Electrical Discharge Hazards.....	13
1.4 Specification Summary.....	13
 Section 2: Installation	 15
2.0 Introduction.....	15
2.1 Inspection	15
2.2 Mounting.....	15
2.3 Storage and Shipment.....	15
2.4 RCP2-1000 Interconnects	15
2.4.1 Prime Power	16
2.4.1.1 AC Power (J1) [IEC (F) socket connector]	16
2.4.1.2 48V Power Supply Option (J1) [MS3112E10-6P].....	16
2.4.1.3 Replacing a Faulted Power Supply Module.....	17
2.4.2 Serial Main (J4) [DB9 (F) connector].....	18
2.4.3 Serial Local (J5) [DB9 (M) connector].....	18
2.4.4 Service (J6) [Mini-USB connector].....	19
2.4.5 Parallel I/O (J7) [DB37 (F) connector].....	19
2.4.6 Ethernet (J9) [RJ45 connector]	19
2.5 Connection with a Remote SSPA.....	21
 Section 3: Front Panel Operation.....	 23
3.0 Introduction.....	23
3.1 RCP2-1000 Front Panel Description	23
3.1.1 System Identification.....	23
3.1.2 Fault Indicators	23
3.1.3 SSPA Online Indicator	23
3.1.4 Vacuum Fluorescent Display	24
3.1.5 Main Menu Key.....	24
3.1.6 Local / Remote Key.....	24
3.1.7 Mute / Unmute Key	24
3.1.8 Display Navigation Keys	24
3.1.9 Enter Key	24
3.2 Main Menu.....	25
3.2.1 Sys Info Menu.....	26
3.2.1.1 Sys Info - Page 1	27
3.2.1.2 Sys Info - Page 2.....	27

3.2.1.3 Sys Info - Page 3.....	28
3.2.1.4 Sys Info - Page 4.....	28
3.2.1.5 Sys Info - Page 5.....	29
3.2.1.6 Sys Info - Page 6.....	29
3.2.1.7 Sys Info - Page 7.....	30
3.2.1.8 Serial Link Statistics Info Page.....	30
3.2.1.8 IP Info - Page 1.....	31
3.2.1.9 IP Info - Page 2.....	31
3.2.1.10 IP Info - Page 3.....	31
3.2.1.11 IP Info - Page 4.....	32
3.2.1.12 SSPAID - Page 1.....	32
3.2.1.13 SSPAID - Page 2.....	32
3.2.1.14 RCP2 Firmware Info - Page 1.....	32
3.2.1.15 RCP2 Firmware Info - Page 2.....	32
3.2.1.16 RCP2 Firmware Info - Page 3.....	32
3.2.2 Panel Com Menu.....	33
3.2.2.1 Protocol.....	33
3.2.2.2 Baud Rate.....	33
3.2.2.3 Sys.Address.....	33
3.2.2.4 Interface.....	34
3.2.2.5 IP Config.....	34
3.2.2.5.1 More Menu from IP Config.....	34
3.2.2.5.2 More (SNMP Trap Information).....	35
3.2.2.6 FiberLink.....	35
3.2.3 SSPA Setup Menu.....	36
3.2.3.1 Attenuation.....	36
3.2.3.2 Redundancy.....	36
3.2.3.3 Mute.....	37
3.2.3.4 SSPAID.....	37
3.2.3.5 Att.Ctrl.....	37
3.2.3.6 More.....	37
3.2.3.7 FrwdRF.....	37
3.2.3.7.1 Type.....	37
3.2.3.7.2 Action.....	38
3.2.3.7.3 Set Level.....	38
3.2.3.8 AuxFlt.....	38
3.2.3.9 BUCFlt.....	39
3.2.3.10 FanSpeed.....	39
3.2.4 Panel Setup Menu.....	40
3.2.4.1 Buzzer.....	40
3.2.4.2 Latch.....	40
3.2.4.3 Poll.....	40
3.2.4.4 Control.....	40
3.2.4.5 PanelID.....	41
3.2.4.6 RF Units.....	41
3.2.4.7 More.....	41

3.2.4.7.1 Remote Global.....	41
3.2.4.7.2 Set Remote Addr.....	41
3.2.4.7.3 Set Time.....	41
3.2.4.7.4 Back.....	41
3.2.4.8 Back.....	41
3.2.5 Options Menu.....	42
3.2.5.1 Backup.....	42
3.2.5.2 Restore.....	42
3.2.5.3 Lamptest.....	42
3.2.5.4 Password.....	43
3.2.5.5 Reset.....	43
3.2.5.6 Back.....	44
3.2.6 LNB Calibration Menu.....	45
3.2.6.1 View.....	45
3.2.6.2 Re-Calibrate.....	45
Section 4: Theory of Operation.....	47
4.0 Introduction.....	47
4.1 Fault Analysis and Condition Tracking.....	47
4.1.1 Summary Fault.....	47
4.1.2 Power Supply Fault.....	47
4.1.3 Voltage Regulator Output Low Fault.....	48
4.1.4 High Temperature Fault.....	48
4.1.5 Low DC Current Fault.....	48
4.1.6 Low Forward RF Fault.....	48
4.1.7 BUC Fault.....	48
4.1.8 Auxiliary Fault.....	48
4.1.9 RF Switch Fault.....	49
4.1.10 Internal Mute Condition Fault.....	49
4.1.11 External Mute Condition Fault.....	49
4.1.12 Serial Connection Fault.....	49
4.2 Design Philosophy.....	50
4.2.1 Digital Core Board.....	50
4.2.2 I/O Board Assembly.....	50
4.2.3 Vacuum Florescent Display.....	50
4.2.4 Front Panel Membrane Keypad.....	51
Section 5: Serial Protocol.....	53
5.0 Overview.....	53
5.1 Serial Communication.....	54
5.1.1.1 Frame Sync Word.....	55
5.1.1.2 Destination Address.....	55
5.1.1.3 Source Address.....	55
5.1.2 Data Packet.....	55
5.1.2.1 Protocol ID.....	55
5.1.2.2 Request ID.....	56

5.1.2.3 Command.....	56
5.1.2.4 Data Tag	57
5.1.2.5 Data Address/Error Status/Local Port Frame Length	57
5.1.2.6 Data Length.....	58
5.1.2.7 Data Field.....	58
5.1.3 Trailer Packet.....	59
5.1.3.1 Frame Check.....	59
5.1.4 Timing Issues.....	59
5.2 Multiple Device Access.....	60
5.2.1 Switching between SSPA and RCP2-1000	61
5.3 Examples.....	67
5.3.1 Example 1, Get Settings	67
5.3.2 Example 2, Change Attenuation	69
5.3.3 Example 3, Change Attenuation (Packet Wrapper)	70
5.4 Remote Control through Terminal Protocol	72
5.4.1 Overview.....	72
5.4.2 Remote Terminal Set-up.....	73
5.5 Ethernet Interface	76
5.5.1 Overview.....	76
5.5.2 IPNet Interface.....	76
5.5.2.1 General Concept	76
5.5.2.2 Setting IPNet Interface	77
5.5.3 Using the RCP2-1000 Web Interface.....	80
5.5.4 SNMP Interface.....	82
5.5.4.1 Introduction	82
5.5.4.2 SNMP V3 Issues in RCP2 Controller	83
5.5.4.3 SNMP MIB Tree	85
5.5.4.4 Description of MIB Entities	86
5.5.5 Extended SNMP Operation.....	93
5.5.5.1 Extended SNMP MIB Tree	94
5.5.5.2 Extended SNMP MIB Tree Elements in Detail	96
5.5.5.3 Configuring RCP2 Unit to Work with SNMP Protocol	97
5.5.5.4 Connecting to a MIB Browser.....	98
5.6 Firmware Programming	99
5.6.1 Required Hardware.....	99
5.6.2 Required Software	99
5.6.3 Web Upgrade Procedure	100
5.6.4 USB Port Upgrade Procedure.....	102
Appendix A: Ethernet Quick Start Set-up.....	103
Appendix B: Proper 10/100 Base-T Ethernet Cable Wiring	107
Appendix C: SSPA Control with Paradise Datacom Universal M&C	111
Appendix D: Specifications.....	115

Figures

Figure 1-1: Outline drawing of RCP2-1000-CO	11
Figure 2-1: RCP2-1000-CO Rear Panel	15
Figure 2-2: Outline Drawing, Removable AC Power Supply Module	16
Figure 2-3: Outline Drawing, Removable 48V Power Supply Module.....	17
Figure 2-4: Cable connections for RCP2-1000-CO	21
Figure 2-5: Top Level Wiring Diagram.....	22
Figure 3-1: RCP2-1000-CO Front Panel.....	23
Figure 3-2: RCP2-1000-CO Menu Structure.....	25
Figure 3-3: RCP2-1000 System Info, IPInfo, SSPA ID and Panel ID Menus....	26
Figure 3-4: Panel Com Menu.....	33
Figure 3-5: SSPA Setup Menu	36
Figure 3-6: Panel Setup Menu.....	40
Figure 3-7: Options Menu	42
Figure 3-8: LNB Calibration Menu	45
Figure 4-1: No Connection Display.....	49
Figure 5-1: RCP2-1000 Remote Control Interface Stack.....	53
Figure 5-2: Basic Communication Packet.....	54
Figure 5-3: Header Sub-Packet.....	54
Figure 5-4: Data Sub-Packet	55
Figure 5-5: Trailer Sub-Packet.....	59
Figure 5-6: Connection Description Window.....	73
Figure 5-7: Connect To Window	73
Figure 5-8: COM Properties Window	74
Figure 5-9: ASCII Setup Window.....	74
Figure 5-10: Example of Terminal Mode session	75
Figure 5-11: UDP Redirect Frame Example	77
Figure 5-12: Web Interface Logon Screen.....	80
Figure 5-13: Web Interface Main Page.....	81
Figure 5-14: GetIF Application Parameters Tab	98
Figure 5-15: Getif MBrowser window, with update data in output data box	98
Figure 5-16: Web Upgrade Authentication Window.....	100
Figure 5-17: Firmware Upload Form.....	100
Figure 5-18: Proceed With Upgrade Prompt.....	101
Figure 5-19: Upload Process Message	101
Figure 5-20: Upload Completed Message	101
Figure 5-21: Windows Device Manager > Ports	102
Figure 5-22: Command Window Showing Program Prompts	102
Figure A-1: TCP/IP Properties Window	103
Figure B-1: Modular Plug Crimping Tool.....	107
Figure B-2: Transmission Line.....	107
Figure B-3: Ethernet Cable Pin-Outs	108
Figure B-4: Ethernet Wire Color Code Standards.....	109
Figure B-5: Wiring Using 568A Color Codes	109
Figure B-6: Wiring Using 568A and 568B Color Codes	109
Figure C-1: New Compact Outdoor SSPA Dialog Window	111

Figure C-2: SSPA Status Window	112
Figure C-3: SSPA Settings Window	112
Figure C-4: IP Setup Window	113

Tables

Table 1-1: RCP2-1000-CO Specification Summary.....	13
Table 2-1: 48V Power Supply Pin-Out.....	16
Table 2-2: Main Serial Port Pin Out	18
Table 2-3: Local Serial Port Pin Out	18
Table 2-4: Parallel I/O Pin Out.....	20
Table 2-5: Ethernet Port (J9) pin outs.....	19
Table 5-1: Command Byte Values.....	56
Table 5-2: Data Tag Byte Values.....	57
Table 5-3: Error Status Bytes	58
Table 5-4: Request Frame Structure	60
Table 5-5: Response Frame Structure	60
Table 5-6: System Settings Data Values for Compact Outdoor SSPA	62
Table 5-7: System Settings Data Values for RCP2-1000 Controller.....	64
Table 5-8: System Condition Addressing (Read Only)	65
Table 5-9: System Threshold Data Values (Read Only).....	66
Table 5-10: Example 1 Host PC Request String.....	67
Table 5-11: Example 1 SSPA Response String.....	68
Table 5-12: Example 2 PC Request String	69
Table 5-13: Example 2 SSPA Response String.....	69
Table 5-14: Example 3 PC Request String.....	70
Table 5-15: Example 3 PC Response String	71
Table 5-16: OSI Model for RM SSPA Ethernet IP Interface.....	78
Table 5-17: Detailed Settings for CO SSPA mode (Device Type=2)	88
Table 5-18: Detailed Settings for RCP2-1000-CO mode (Device Type=4).....	90
Table 5-19: Detailed Thresholds (common for all Device Types)	92
Table 5-20: Detailed Conditions for CO SSPA mode (Device Type = 2)	92
Table 5-21: Detailed Conditions for RCP2-1000-CO mode (Device Type=4)...	92

THIS PAGE LEFT INTENTIONALLY BLANK

1.0 Introduction

This section provides the general information for the Teledyne Paradise Datacom LLC Remote Control Panel for the Compact Outdoor SSPA and High Power Outdoor SSPA. This section describes the supplied equipment and safety precautions that should be followed in its use.

1.1 Description

The RCP2-1000-CO controller provides control of Paradise Datacom’s Compact Outdoor SSPA. The RCP2-1000-CO is used for standalone or 1:1 modes of operation. An outline drawing of the RCP2-1000-CO is shown in **Figure 1-1**.

A mimic display on the front panel indicates online and fault status of the equipment. User interface and control is provided in three forms:

- Front Panel, Local Control
- 37-pin Parallel Control Port with Contact Closures and Opto Isolated Inputs
- Serial Data Control via RS-232, RS-485 (2-wire), or Ethernet

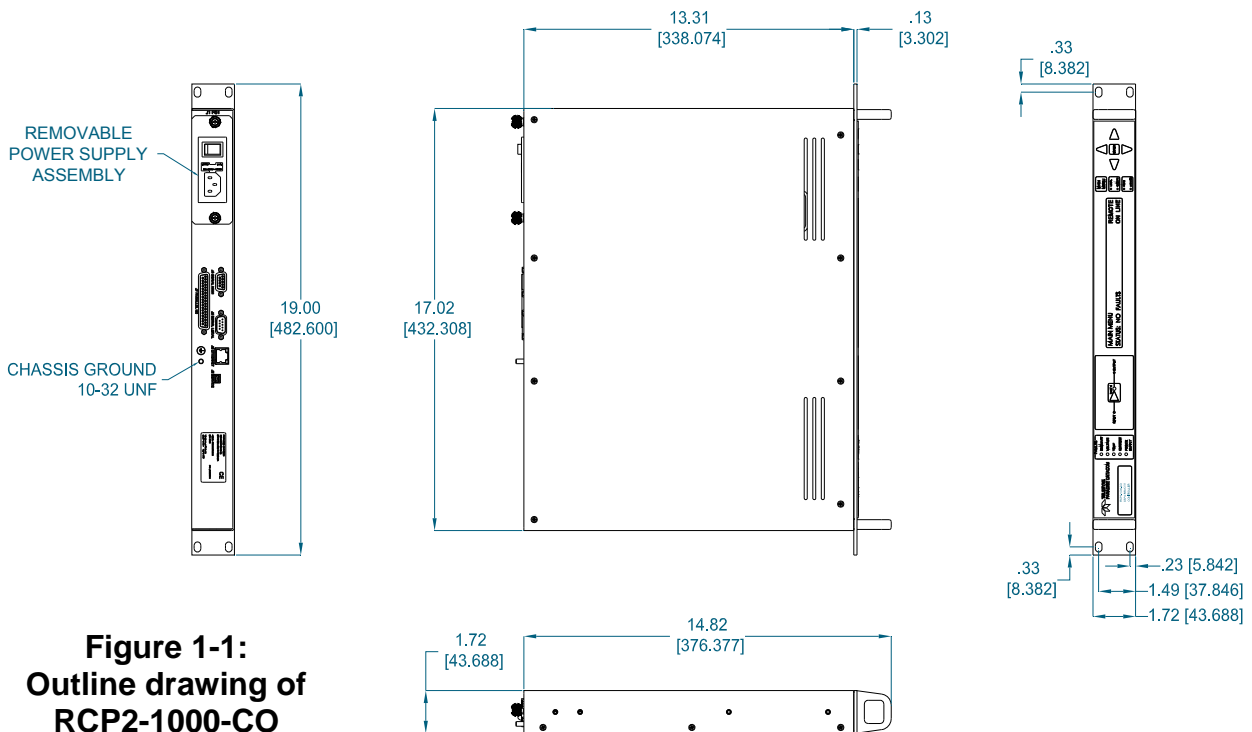


Figure 1-1:
Outline drawing of
RCP2-1000-CO

1.2 Equipment Supplied

The following equipment is supplied with each unit:

- RCP2-1000-CO Remote Control Panel (1 RU high)
- (2) IEC Line Cord Sets
- Operations Manual (209727) RCP2-1000-CO Remote Controller

Paradise Datacom can provide the following optional equipment:

- Rack Slides
- and -
- Link control cable (RCP2-1000 to Compact Outdoor SSPA) (Part number: L201747-X)
-or -
- Mating connector for Compact Outdoor and RCP2-1000

1.3 Safety Considerations

Potential safety hazards exist unless proper precautions are observed when working with this unit. To ensure safe operation, the user must follow the information, cautions and warnings provided in this manual as well as the warning labels placed on the unit itself.

1.3.1 High Voltage Hazards

High Voltage for the purpose of this section is any voltage in excess of 30 volts. Voltages above this value can be hazardous and even lethal under certain circumstances. Care should be taken when working with devices that operate at high voltage.

- All probes and tools that contact the equipment should be properly insulated to prevent the operator from coming into contact with the voltage.
- The work area should be secure and free from non-essential items.
- Operators should never work alone on high voltage devices. There should always be another person present in the same work area to assist in the event of an emergency.
- Operators should be familiar with procedures to employ in the event of an emergency, i.e. remove all power, CPR, etc.

An AC powered unit will have 115 VAC or 230 VAC entering through the AC power connector. Caution is required when working near this connector, the AC circuit breaker, or the internal power supply.

1.3.2 Electrical Discharge Hazards

A spark can not only create ESD reliability problems, it can also cause serious safety hazards. The following precautions should be taken when there is a risk of electrical discharge:

- Follow all ESD guidelines.
- Remove all flammable material and solvents from the area.
- All probes and tools that contact the equipment should be properly insulated to prevent electrical discharge.
- The work area should be secure and clear from non-essential items.
- Operators should never work alone on high voltage devices. There should always be another person present in the same work area to assist in the event of an emergency.
- Operators should be familiar with procedures to employ in the event of an emergency, i.e. remove all power, CPR, etc.

1.4 Specification Summary

Table 1-1 contains a summary of the specifications of the RCP2-1000-CO remote controller. A full list of unit specifications can be found on the specification sheet in **Appendix D**.

Table 1-1: RCP2-1000-CO Specification Summary

Configurations	RCP2-1000-CO
Fault Detection Time	20-50 msec
Alarm Input	RS-485
Parallel I/O Status Outputs Control Inputs	Form C Relay Contacts (10 sets) Contact Closure to Ground
AC Input Power	85-265 VAC, 47-63 Hz, 1 A max, > 0.93 power factor
Mechanical Dimensions	1.75 in. H x 19 in. W x 13.3 in. D [1 RU] (89 mm H x 483 mm W x 338 mm D)
Weight	5 lb (2.3 kg)
Environmental Temperature	0 - 50 °C

THIS PAGE LEFT INTENTIONALLY BLANK

2.0 Introduction

This section provides information for the initial inspection, installation and external connections for the RCP2-1000-CO remote control panel.

2.1 Inspection

When the unit is received, an initial inspection should be completed. First, ensure that the shipping container is not damaged. If it is, have a representative from the shipping company present when the container is opened. Perform a visual inspection of the equipment to make sure that all items on the packing list are enclosed. If any damage has occurred or if items are missing, contact:

Teledyne Paradise Datacom
328 Innovation Blvd., Suite 100
State College, PA 16803
Phone: +1 (814) 238-3450
Fax: +1 (814) 238-3829

2.2 Mounting

The RCP2-1000-CO Remote Control Panel is designed to be mounted in a standard EIA 9 inch equipment rack. The depth of the unit, excluding rear panel connectors, is 13.3 inches (338 mm). The height is 1.75 inches (89 mm) or 1 rack unit.

2.3 Storage and Shipment

To protect the RCP2-1000 remote control panel during storage or shipping, use high quality commercial packing methods. Reliable commercial packing and shipping companies have facilities and materials to adequately repack the equipment.

2.4 RCP2-1000 Interconnects

The RCP2-1000 remote control panel includes a variety of interconnections on the rear panel through which serial or parallel communication between it and an external amplifier is achieved. **Figure 2-1** shows a detailed drawing of the rear panel.

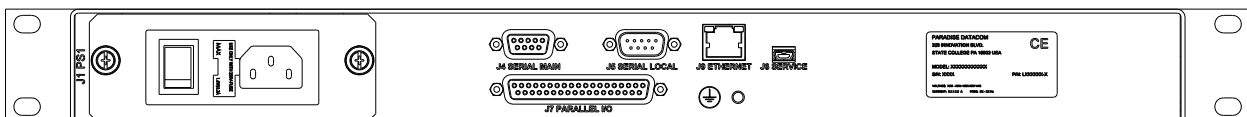


Figure 2-1: RCP2-1000-CO Rear Panel

2.4.1 Prime Power

The RCP2-1000-CO Remote Control Panel is available with standard AC input power or with the optional 48V DC input.

2.4.1.1 AC Power (J1) [IEC (F) socket connector]

The RCP2-1000-CO Remote Control Panel features a removable AC power supply module, with connector (J1) provided on the rear panel. The AC input can operate over a range of 85-265 VAC, at 47-63 Hz. An On/Off switch and a 2A 5x20mm fuse are located adjacent to the AC input connector. An 18 AWG line cord (CE American Plug) is shipped with each unit.

Contact Teledyne Paradise Datacom Support for a replacement power supply. **Figure 2-2** shows an AC Power Supply Module.

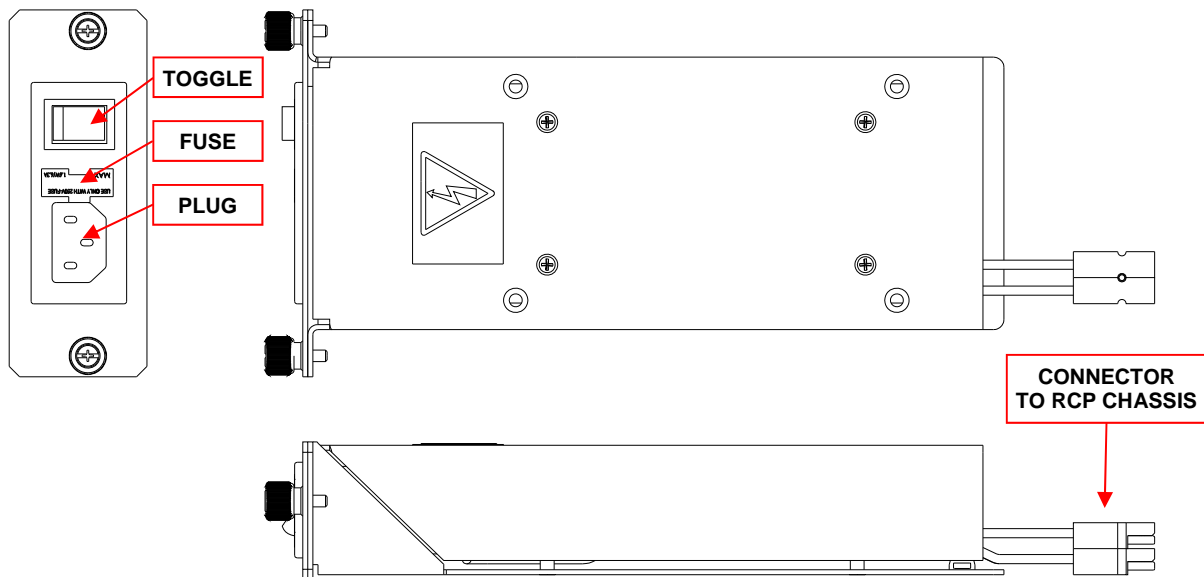


Figure 2-2: Outline Drawing, Removable AC Power Supply Module

2.4.1.2 48V Power Supply Option (J1) [MS3112E10-6P]

The RCP2-1000-CO is available with a 48V Power Supply Option, which utilizes a MS-type connector (MS3112E10-6P) for prime power input. The connector pin-out is shown in **Table 2-1**. The mating connector (MS3116F10-6S) is supplied with the unit. Current load is protected via a 6A push-to-reset circuit breaker.

Table 2-1: 48V Power Supply Pin-Out

Pin	Function
A,B	+48V
C,D	-48V
E,F	GND

Figure 2-3 shows a 48V Power Supply Module.

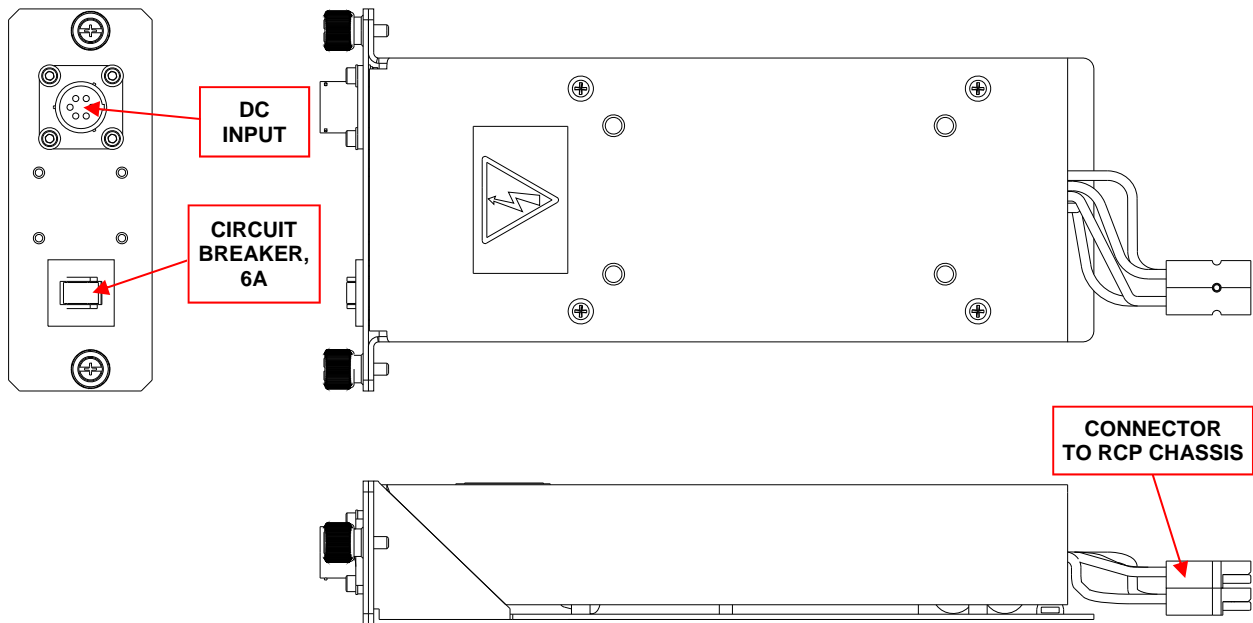


Figure 2-3: Outline Drawing, Removable 48V Power Supply Module

2.4.1.3 Replacing a Faulted Power Supply Module

To replace a faulted power supply module from the RCP chassis, perform the following steps:

1. Remove power from the module to be replaced;
2. Loosen the two captured thumbscrews securing the module to the chassis;
3. Slide the module out of the chassis;
4. Unplug the quick-disconnect power pole connectors;
5. Ensure the replacement power supply is the same type as the one being replaced;
6. Plug together the quick-connect power pole connectors;
7. Slide the module into the chassis, taking care not to pinch the power cables;
8. Tighten the two captured thumbscrews to secure the module to the chassis.

2.4.2 Serial Main (J4) [DB9 (F) connector]

A DB9 female connector serves as primary remote control interface connector. This interface allows the user to connect a PC to the RCP unit in order to access its advanced features as well as access a remote SSPA unit through its serial port. This interface is re-configurable through the front panel menu, and can be used as a RS-232 or RS-485 interface (2 or 4 wires). The RS-485 TX and RX pairs must be twisted for maximum transmission distance. A user configurable 120Ω termination resistor is provided on the same connector. **Table 2-2** shows the pin-out for the main serial port.

Table 2-2: Main Serial Port Pin Out

Pin #	Function Description
1	RS485 TX+ (HPA Transmit +)
2	RS485 TX- (HPA Transmit -)/RS232 TX
3	RS485 RX- (HPA Receive -)/RS 232 RX
4	RS485 RX+ (HPA Receive +)
5	GND
6	Service Request 1; Form C relay NC contact (Closed on HPA Summary Fault)
7	Service Request Common; Form C relay common contact
8	Service Request 2; Form C relay NO contact (Opened on HPA Summary Fault)
9	120 Ohm termination (must be connected to pin 4 in order to enable termination)

2.4.3 Serial Local (J5) [DB9 (M) connector]

A DB9 male connector serves as a serial interface with a remote Compact Outdoor SSPA. Interface parameters are set by the internal RCP hardware and cannot be reconfigured by the user. The remote SSPA serial interface must be properly set to provide connection with the RCP unit. **Table 2-3** on the following page shows the local serial port pin-out.

Table 2-3: Local Serial Port Pin Out

Pin #	Function Description
1	RS485 RX+
2	RS485 RX-
3	RS485 TX-
4	RS485 TX+
5	GND
6	
7	
8	
9	120 Ohm termination (must be connected to pin 1 in order to enable termination)

2.4.4 Service (J6) [Mini-USB Type B (F) connector]

A 5-contact Mini USB connector is used to provide flash re-programmability for the RCP controller card. In order to reload controller board firmware, connect this port to a standard PC USB port. See **Section 5.6** for a description of the firmware upgrade procedure.

2.4.5 Parallel I/O (J7) [DB37 (F) connector]

A DB37 Female type connector contains a series of contact closures, for monitoring remote SSPA faults; and opto-isolated inputs, for controlling some of the SSPA functions. Inputs react on the closure to ground. Minimal closure time - 50mS. **Table 2-4** on the following page shows details of the Parallel I/O pin-out.

2.4.6 Ethernet (J9) [RJ45 connector]

This is a RJ45 connector with integrated magnetics and LEDs. This port becomes the primary remote control interface when the Interface option is selected to "IPNet" as described in **Section 5.5.2.2**. This feature allows the user to connect the RCP to a 10/100 Base-T office Local Area Network and have full-featured Monitor & Control functions through a web interface. See **Table 2-5** for Ethernet pin outs.

Table 2-5: Ethernet Port (J9) pin outs

Pin #	Function Description
1	TX+
2	TX-
3	RX+
6	RX-
4,5,7,8	GND

Note: IP address, Gateway address, Subnet mask, IP port and IP Lock address all need to be properly selected prior to first use (see Appendix C for details).

LED lamps on the connector indicate network status. A steady Green light indicates a valid Ethernet link; a flashing Yellow LED indicates data transfer activity (on either the Transmit and Receive paths).

Table 2-4: Parallel I/O Pin Out

Pin #	Function Description
1	Closed on Power Supply Fault Form C relay NC
2	Open on Power Supply Fault Form C relay NO
20	Power Supply Fault Common
3	Auxiliary Fault\Auto-Manual Common
21	1. Standalone mode. Closed on Auxiliary Fault 2. 1:1 Redundancy Mode. Closed on Automatic switchover mode. Form C relay NC
22	1. Standalone Mode. Open on Auxiliary Fault 2. 1:1 Redundancy Mode. Closed on Manual switchover mode. Form C relay NO
4	Open on Mute. Form C Relay NC
5	Closed on Mute. Form C Relay NO
23	Mute Status Common
6	BUC Fault Common
24	Closed on BUC Fault. Form C Relay NC
25	Open on BUC Fault. Form C Relay NO
7	Closed on High Temperature Fault. Form C Relay NC
8	Open on High Temperature Fault. Form C Relay NO
26	High Temperature Fault Common
9	Regulator Low Voltage Fault\Standby-Online Common
27	1. Standalone mode. Closed on Regulator Low Voltage Fault 2. 1:1 Redundancy Mode. Closed on HPA Standby. Form C relay NC
28	1. Standalone Mode. Open on Regulator Low Voltage Fault. 2. 1:1 Redundancy Mode. Open on HPA Online Mode. Form C relay NO
10	Closed on DC Current Low Fault. Form C Relay NC
11	Opened on DC Current Low Fault. Form C Relay NO
29	DC Current Low Fault Common
12	Low Output RF Fault Common
30	Closed on Low Output RF Fault. Form C Relay NC
31	Opened on Low Output RF Fault Form C Relay NO
17	Mute/Unmute toggle input. 50mS Closure to ground to activate
35	SSPA Standby input. 50mS Closure to ground to activate
36	RCP Local/Remote toggle. 50mS Closure to ground to activate
37	Fault clear. 50mS Closure to ground to activate
19	Isolated Ground
34, 33, 32, 18, 16, 15, 14, 13	Reserved. Make No Connection.

2.5 Connection with a Remote SSPA

The RCP2-1000-CO Remote Control Panel and Compact Outdoor SSPA may be linked together through 2-wire twisted pair shielded cable (such as 24 AWG twisted pair telephone cable). The cable should be connected between port J5 “Serial Local” of the RCP2-1000 and port J4 “M&C” connector of SSPA, as shown in **Figure 2-4**. **Figure 2-5** on the following page shows the complete top level wiring diagram.

To achieve reliable communication over long distances an adequate line termination (120 ohm resistor between RS485+ and RS485- lines) must be provided on both ends of the cable. The link provides data exchange through RS485 half-duplex serial interface with 9600 Baud data rate.

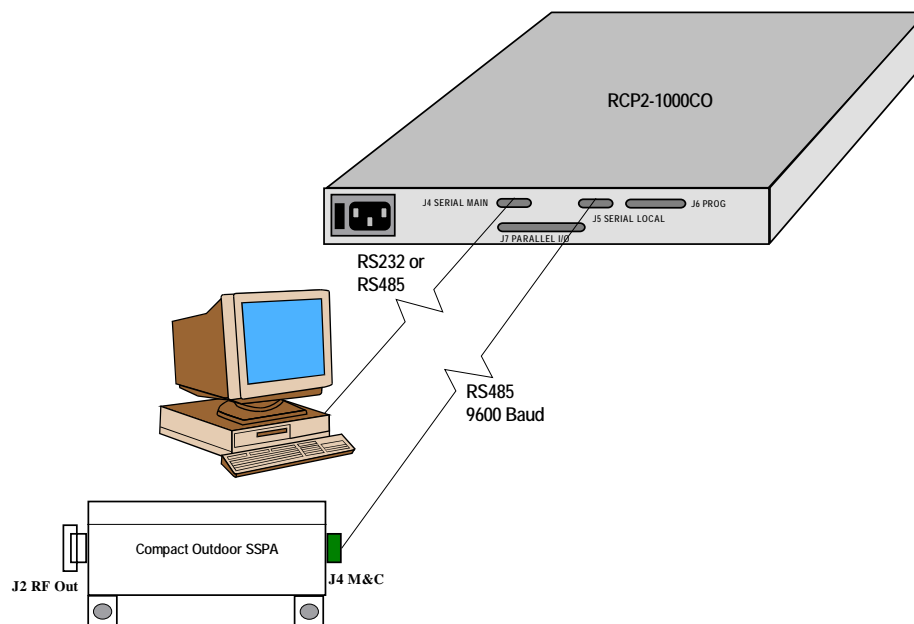


Figure 2-4: Cable Connections for RCP2-1000-CO

Data link is peer-to-peer only; connection of a secondary SSPA or RCP unit is not possible. The RCP2-1000-CO Remote Control Panel is designed to provide remote control by using second generation of Teledyne Paradise Datacom Compact Outdoor SSPA serial protocol only. In other words, the RCP2-1000-CO unit provides support only for later model SSPA units with S/N above 100,000. Earlier models of SSPA, which are utilizing different style of serial protocol, can't be controlled by the RCP2-1000-CO Remote Control Panel.

In order to achieve successful operation of the RCP unit, the Compact Outdoor SSPA or High Power Outdoor SSPA must be configured with the following parameters: Baud Rate - 9600; Serial Interface - RS485; Network Address - any. Maximum cable length is 4000 feet (1.3 km).

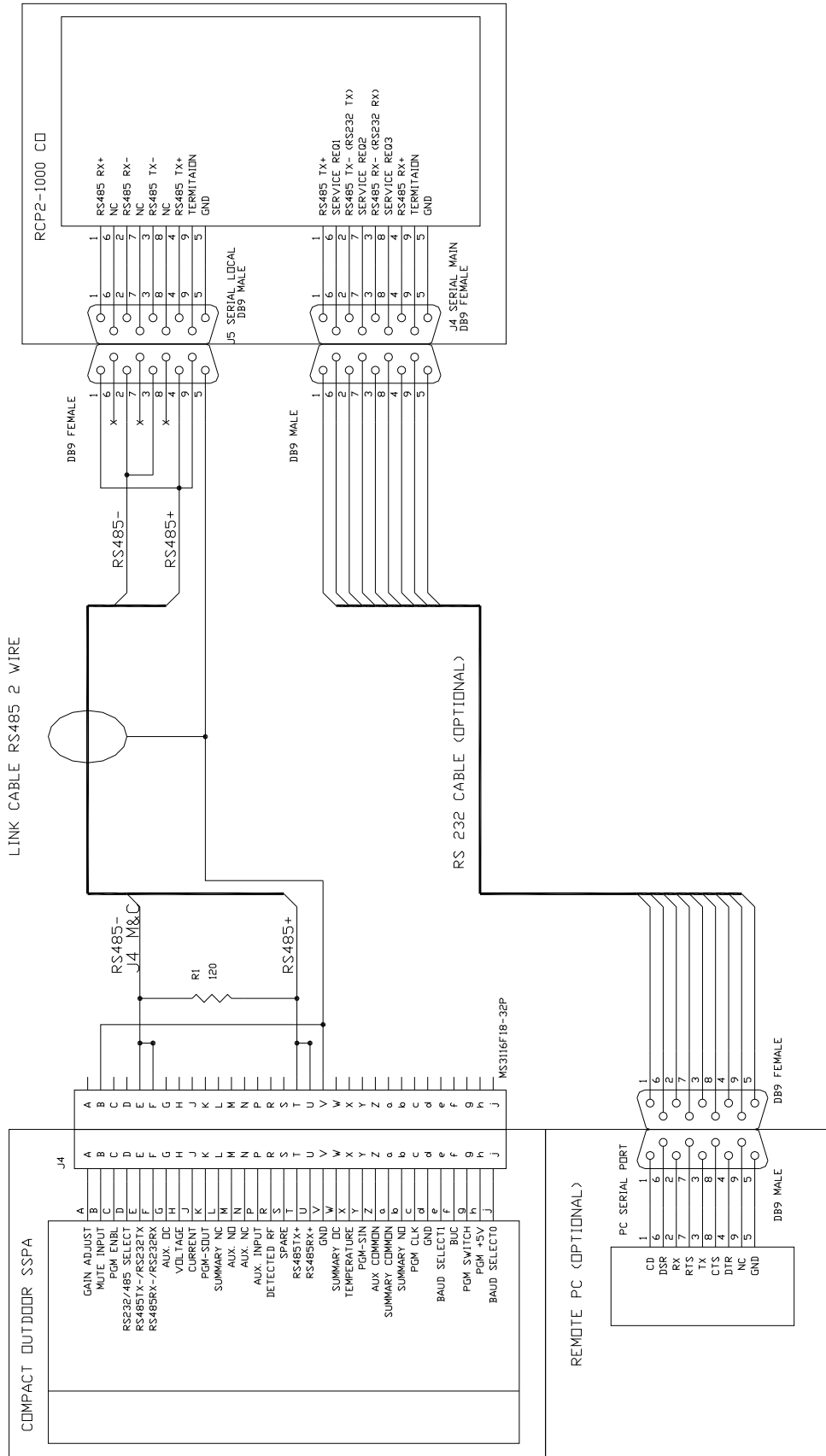


Figure 2-5: Top Level Wiring Diagram

3.0 Introduction

Control of the RCP2-1000-CO can be handled through Front Panel operation, or remotely through Parallel or Serial communication to a computer.

For Local (front panel) operation of the controller, simply toggle the Local/Remote button until the yellow LED indicator is illuminated on Local. When in Remote mode, the front panel buttons will be inoperative. The indicators and VFD display will still show the status of the system. The Local/Remote key is always operative so that the appropriate mode can be selected. Remote operation enables serial communication and parallel I/O control.

3.1 RCP2-1000 Front Panel Description

The RCP2-1000 front panel includes ten (10) LEDs to indicate the internal state of the connected unit. Five (5) fault condition LEDs on left side of the front panel reflect some of the SSPA major faults plus summary fault state. SSPA online LED will turn green when SSPA is in Online mode (1:1 Mode) or serves as AC power indicator in standalone mode. Local/Remote and Mute/Unmute LEDs show the current control mode and mute state of the SSPA.

A diagram of the Front Panel is shown in **Figure 3-1**.

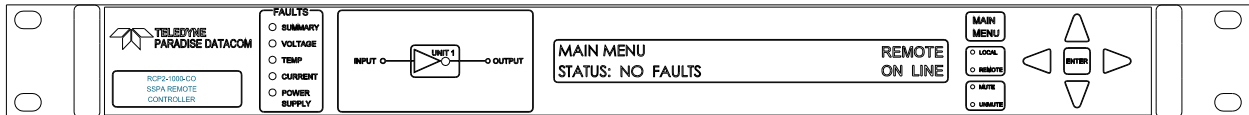


Figure 3-1: RCP2-1000-CO Front Panel

3.1.1 System Identification

A label on the lower left corner of the controller displays the model number and a brief description of the unit. The serial number is located on the rear panel of the controller.

3.1.2 Fault Indicators

The fault indicator LEDs illuminate RED when the corresponding fault condition occurs. There are fault lights for Summary, Voltage, Temperature, Current and Power Supply.

3.1.3 SSPA Online Indicator

The SSPA Online LED will turn green when the SSPA is in Online mode (1:1 Mode) or serves as an AC power indicator in standalone mode.

3.1.4 Vacuum Fluorescent Display

The 40 character by two line front panel vacuum fluorescent display (VFD) provides a quick, convenient method of selecting various operating parameters of the controller. All internal settings can be achieved via the VFD and menu structure. There is no need to access the interior of the controller to adjust or reconfigure hardware settings. The VFD also provides detailed information on fault conditions.

3.1.5 Main Menu Key

The main menu key is a convenient method for instantly returning to the VFD main menu. No matter what menu screen is currently displayed on the VFD, pressing this key returns the user to the main menu, eliminating the need to scroll backward through several menu levels. See **Section 3.2** for a complete description of the Main Menu.

3.1.6 Local / Remote Key

The Local/Remote key allows the user to disable or enable the local control keypad console. If the SSPA is in "Remote Only" mode, the unit will not react to any keystrokes except the "Local/Remote" key.

3.1.7 Mute / Unmute Key

The Mute/Unmute key provides an easy way to change the Mute state of the remote SSPA.

3.1.8 Display Navigation Keys

The display navigation keys allow easy movement through the VFD menu. **Up Arrow** (▲), **Down Arrow** (▼), **Left Arrow** (◀), and **Right Arrow** (▶) keys provide menu navigation.

3.1.9 Enter Key

The enter key is used to select a given menu item. In conjunction with the navigation keys, it is easy to locate and select a desired function.

3.2 Main Menu

The Main Menu organized in several functional subgroups, diagramed in **Figure 3-2**.

1. **Sys.Info** - will return menu pointer to the informative menu sublevel;
2. **PanelCom** - provides access to the RCP main serial port (PC Interface) communication settings;
3. **SSPASetup** - provides access to remote SSPA settings;
4. **PanelSetup** - provides access to the RCP local settings;
5. **Options** - optional RCP control.
6. **LNB Cal** - provides access to menu for calibration of attached LNBS.

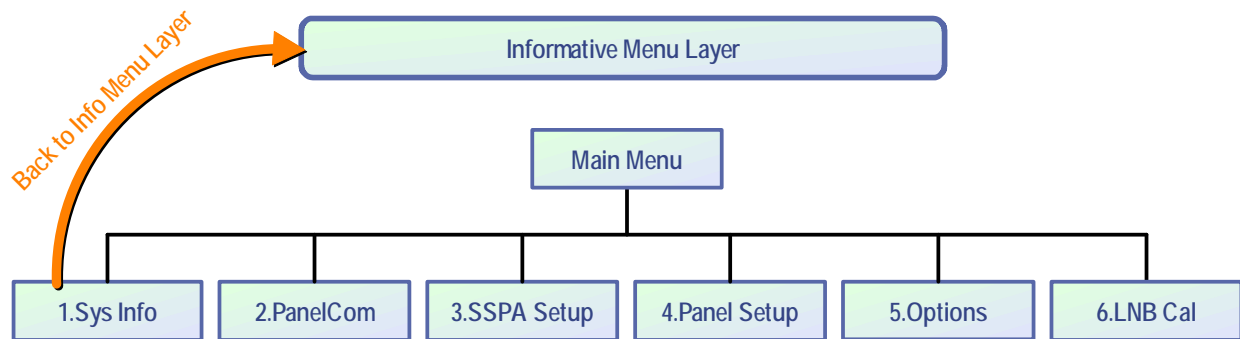


Figure 3-2: RCP2-1000-CO Menu Structure

The menu tree is accessed by pressing the Main Menu key on the front panel of the unit. Navigation through the menu structure is handled by using the **Up Arrow** (▲), **Down Arrow** (▼), **Left Arrow** (◀), and **Right Arrow** (▶) keys and the **Enter** key to select from the items shown in the front panel display.

For menus where an actual numerical value must be entered, the **Up Arrow** (▲) and **Down Arrow** (▼) keys change the number by factors of 10; the **Left Arrow** (◀) and **Right Arrow** (▶) keys change the number in increments of 1.

Note: If the **Local/Remote** key is toggled so that the Remote LED is illuminated, the **Main Menu** key, **Arrow** keys and **Enter** key are disabled. To regain local control, press the **Local/Remote** key so that the Local LED is illuminated.

If the "Fault Latch" option is selected, pressing the "Enter" button will clear all system faults.

3.2.1 Sys Info Menu

The main informative sublevel of the menu structure (**1.SysInfo**) contains eight pages, shown in **Figure 3-3**. Other menu selections offer additional information.

Pressing the **Enter** key will advance to the next page in the **1.SysInfo** menu. Pressing the **Left Arrow** (◀) or **Right Arrow** (▶) keys will open the Attenuation Select menu (see **Section 3.2.3.1**).

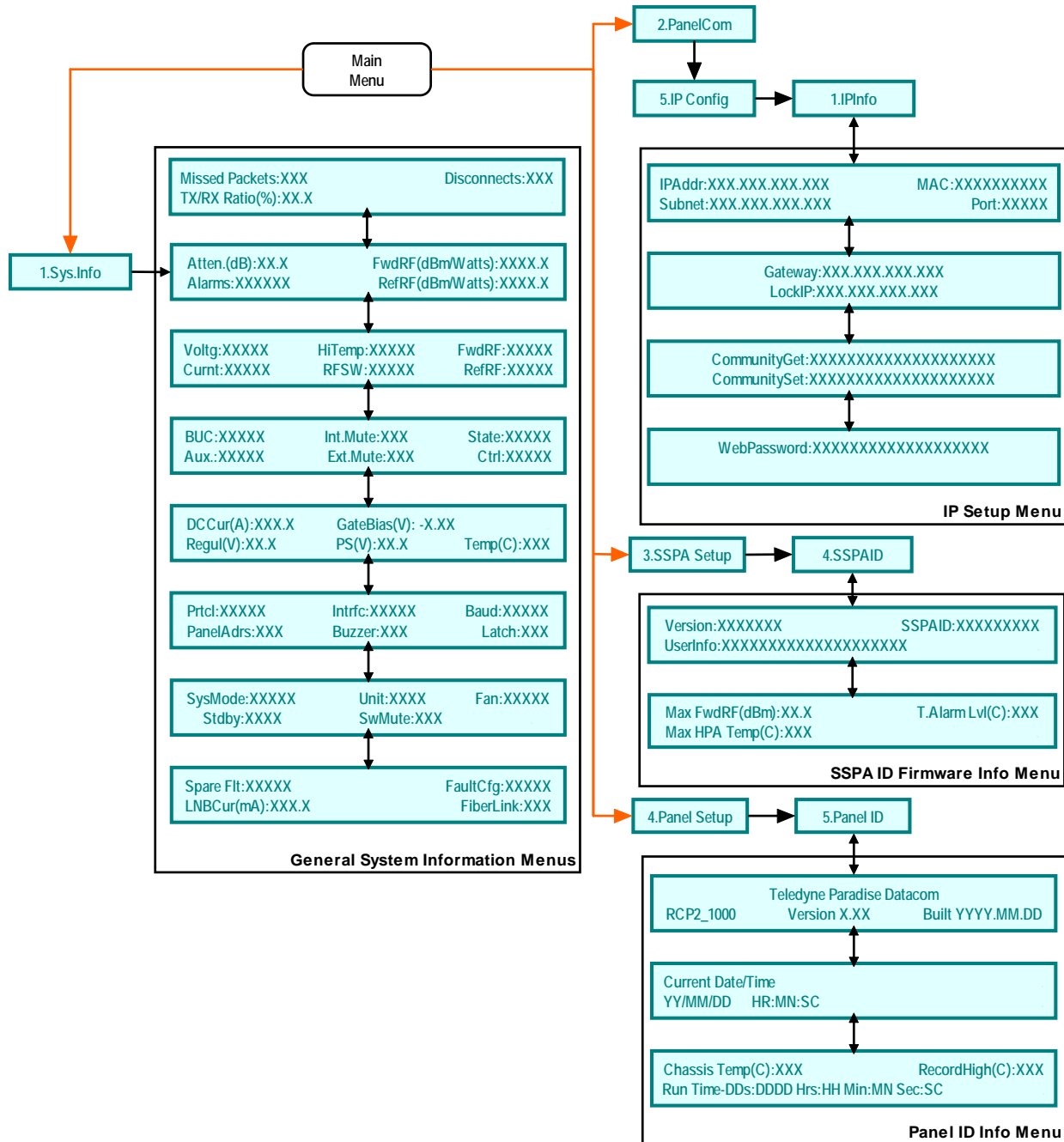


Figure 3-3: RCP2-1000 System Information, IPInfo, SSPA ID and Panel ID Menus

3.2.1.1 Sys Info - Page 1

Page 1 is the SSPA main status information page. The page shows:

- **Atten.(dB)** — HPA attenuation measured in dB with 0.1 dB accuracy;
- **FwdRF(dBm/Watts)** — Forward RF Power in dBm or Watts with accuracy of 0.1 dBm;
- **Alarms** — Alarms presence, "FAULT!" or "None" will be displayed, depending on the state of the remote SSPA;
- **RefRF(dBm/Watts)** — Reflected RF Power in dBm or Watts. Reflected RF measurement is available on selected SSPA units with firmware version 6.30 and above. Reflected RF measurement is part of the extended subset and may be turned off if not desired. This parameter will display "N/A" (not available) when the extended subset is turned off.

3.2.1.2 Sys Info - Page 2

Page 2 shows a variety of alarm statuses which may be present in the remote SSPA. The status report could show "Fault", "Normal" or "N/A".

- **Voltage** — Voltage Regulator Low, displays "Normal" if remote SSPA voltage regulator output voltage is normally operational and "Fault" if failed.
- **Current** — Low SSPA DC current. Shows "Fault" if remote SSPA detects abnormally low DC current consumed by RF module, or "Normal" under normal conditions;
- **HiTemp** — Indicates a critically high base plate temperature for the remote SSPA. Shows "Normal" if the internal HPA temperature is below the pre-set alarm threshold and "Fault" when temperature equals or exceeds the threshold.
- **RFSW** — Shows the state of the external waveguide path redundancy switch. Possible values are "Normal" and "Fault".
- **FwdRF** — Reflects the status of the Forward RF fault, if enabled. Possible values are "Normal" and "Fault".
- **RefRF** — Reflects the status of the Reflected RF fault, if the controlled HPA is equipped with a Reflected RF indicator. Possible values are "Normal" and "Fault".

3.2.1.3 Sys Info - Page 3

Page 3 shows secondary faults and conditions, which may exist in the remote SSPA

- **BUC** — Indicates BUC fault conditions of the remote SSPA (if SSPA is equipped with a BUC). Possible values are “Fault” or “Normal”;
- **AUX** — Indicates auxiliary fault conditions (if enabled). Possible values are “Fault” or “Normal”;
- **Int.Mute** — Indicates the internal muting state of the remote SSPA. Possible values are “On” or “Off”.
- **Ext.Mute** — Indicates the external muting state of the remote SSPA. Possible values are “On” or “Off”.
- **State** — SSPA online state. Possible values are “Online” or “Standby”;
- **Ctrl** — Indicates the current attenuation control style of the remote SSPA. Possible values are “Serial” or “Analog”.

3.2.1.4 Sys Info - Page 4

Page 4 shows remote SSPA summarized internal conditions

- **DCCur.(A)** — Total DC current draw by the RF module of the remote SSPA from the main power supply. This value varies depending on the power level of the HPA. If the HPA is muted, the current drops to a range of 0 to 5 A, which is normal.
- **Regul.(V)** — Voltage regulator output. In an unmuted state, depending on the SSPA model, this value should read close to 10V for GaAs based HPAs and anywhere from 20 to 55V for GaN HPAs. If the SSPA is muted, this value should be close to 0V for all HPA models.
- **GateBias(V)** — Negative RF GASFET gates bias voltage. This value varies depending on the temperature and mute state. The approximate value window is 1.5 to 7 Volts.
- **PS(V)** — Main power supply 1q output voltage with accuracy of 0.1V. Normal output voltage should be in a range of 11 to 58 V.
- **Temp.(C)** — Indicates SSPA internal MOSFETs plate temperature in degrees Centigrade;

3.2.1.5 Sys Info - Page 5

Page 5 shows various settings related to the RCP operation:

- **Prtcl.** — Current RCP remote control protocol. Value can be set to “Terminal”, if terminal mode protocol is currently active and “Normal” for string I/O type protocol, which mimics Compact Outdoor Serial Protocol .
- **Intrfc.** — Shows the selected serial port interface. Selection: “RS232”, “RS485”, “IPNet” or “SNMP”;
- **Baud** — Selected baud rate for the remote control serial port. Selection: “2400”, “4800”, “9600”, “19200”, “38400”;
- **PanelAddr.** — Displays the assigned RCP remote control network address. This value may range from 0 to 255. **Note:** Addresses 170 and 255 are reserved for global calls. See **Section 5.1.1.2** for details.
- **Buzzer** — Displays the audible alarm availability. Displays “Dis” if alarm is disabled and “Enb” if enabled.
- **Latch** — Fault latch option selection. “Dis” indicates that this option is disabled, and “Enb” indicates it is enabled. When the fault latch option is enabled, the **Enter** key on the front panel can be pressed to clear all fault conditions.

3.2.1.6 Sys Info - Page 6

Page 6 shows System-related settings.

- **SysMode** — Indicates SSPA operational mode. Value can be set to “Stdaln” for stand alone mode, “1:1” for 1:1 redundancy mode and “Dual1:1” for dual 1:1 redundancy mode;
- **Unit** — Redundancy topological factor. “HPA1” for HPA connected to the RF switch port 2 or 3 (Online Position 1 of the RF switch). “HPA2” for HPA connected to the RF switch port 1 or 4 (Online Position2 of the RF switch);
- **Fan** — Indicates selected fan speed control mode on units with fan speed control option. Possible values: “Auto”, “High”, “Low” or “Off”. On HPA units without fan speed control, this option value should be set to “Off”.
- **Stndby** — Shows the HPA standby state selection. “Hot” for hot standby operation (where the HPA retains an unmuted state during standby period) and “Cold” for cold standby (where the HPA mutes itself in standby mode and unmutes when switched back on-line).
- **SwMute** — Indicates selected Switch mute mode. Switch mute mode is available on HPAs with firmware greater than 6.55. Possible values are “On” or “Off”. For HPAs with a lower firmware version, this option must be set to “Off”.

3.2.1.7 Sys Info - Page 7

Page 7 shows settings related to Spare Fault configuration and optional fiber-optic link operation.

- **Spare Flt.** — Displays state of spare fault, Normal or Fault.
- **Fault Cfg.** — Displays the current configuration of the CO SSPA spare fault. Possible values include: “Disabled”, where the fault is disabled; “LNB Current”, fault on external LNB current window; “RF Out”, fault on forward RF window; “Gate Voltage”, fault on low gate voltage; “Reg. Voltage”, fault on low regulator voltage; “PS Voltage”, fault on low power supply voltage; and “DC Current”, fault on DC current out of window.
- **LNBCur(mA)** — Displays current consumption of externally connected to CO SSPA LNB (if equipped).
- **FiberLink** — Displays the state of the internal fiberlink circuitry. Possible values include: “Off”, “On”, or “No FSK”.

3.2.1.8 Serial Link Statistics Info Page

This page summarizes the quality of the serial control link to the remote SSPA. It is available by pressing the **Up Arrow** (▲) key at SysInfo Page 1.

- **Missed packets** — Displays the number of unanswered request packets since the last RCP2 power up or since the last ‘Clear Faults’ command initiated by the user.
- **TX/RX ratio** — Shows the percentage of successful request/response packets out of total number of sent packets. This value begins calculation upon RCP2 power up and gets reset when a ‘Clear Faults’ command is executed by the user.
- **Disconnects** — This value indicates the number of disconnect events (5 or more unanswered packets in the row) that have occurred since the last RCP2 power up or since the last ‘Clear Faults’ command.

Pressing the **Enter** key while on this page will open the Clear Faults menu (see **Section 3.2.5.5**, selection **4.ClrFlts**).

3.2.1.8 IP Info - Page 1

This page is available through the PanelCom. menu, and shows SSPA settings related to the IP interface. See **Figure 3-3**.

- **IP Address** – IP address of the SSPA. Consult your network administrator to set this address according to your LAN configuration.
- **MAC** – Medium Access Control address of the SSPA Ethernet controller. This address is factory preset.
- **Subnet** – IP subnet mask of the SSPA. Consult your network administrator to set this address.
- **IPPort** – IP port value for the SSPA. This address is valid only when IP-Net protocol is selected. The port value should not be selected outside the existing services range to avoid access conflict on the M&C PC end.

3.2.1.9 IP Info - Page 2

This page shows SSPA settings related to the IP interface.

- **Gateway** – IP Gateway address. This address is used only if access to the SSPA is provided from an outside LAN. If no such access is required, the address must be set to 0.0.0.0
- **LockIP** – This address is used to increase the security measure for the IPNet protocol. The SSPA will answer a request which comes only from a specified IP address. Set this address value to 255.255.255.255 or 0.0.0.0 to disable this feature.

3.2.1.10 IP Info - Page 3

This page shows SSPA settings related to the IP interface.

- **CommunityGet** – Security string used in SNMP protocol for Get type requests. Set this value to match the value specified in the NMS or MIB browser. Maximum string length is 20 alpha-numeric characters. The string allows read operation for the RM SSPA SNMP agent.
- **CommunitySet** – Security string used in SNMP protocol for Set type requests. Set this value to match the value specified in the NMS or MIB browser. For security reasons this string must be different than the Community Get string. Maximum string length is 20 alpha-numeric characters. The string allows write operation for the RM SSPA SNMP agent.

Community strings are essentially passwords. The user should use the same rules for selecting them as for any other passwords: no dictionary words, spouse names, etc. An alphanumeric string with mixed upper- and lower-case letters is generally a good idea.

3.2.1.11 IP Info - Page 4

This page indicates the selected password for the web page interface. A blank space indicates that the web interface will not require a password protected login.

3.2.1.12 SSPAID - Page 1

This page is available through the SSPAID menu, and provides the following information about the connected SSPA.

- **Version** — The MCU firmware revision level;
- **SSPAID** — The unique serial and model number of the SSPA;
- **UserInfo** — The user information string, which can be set over SNMP protocol.

3.2.1.13 SSPAID - Page 2

This page provides statistics of SSPA operation over time and additional SSPA information.

- **Max FwdRF(dBm)** — Displays the absolute maximum RF level registered by the RCP. This value is permanently retained in RCP2 memory until the user executes a “Clear faults” command.
- **Max HPA Temp(C)** — Displays the absolute maximum SSPA core temperature registered by the RCP. This value is permanently retained in RCP2 memory until the user executes a “Clear faults” command.
- **T.AlarmLvl(C)** — Displays the

3.2.1.14 RCP2 Firmware Info - Page 1

This page displays the RCP2 unit device type (RCP2-1000), firmware version and firmware development date build stamp.

3.2.1.15 RCP2 Firmware Info - Page 2

This page displays the time and date set on RCP2 unit

3.2.1.16 RCP2 Firmware Info - Page 3

This page shows the RCP2 chassis internal temperature, the highest measured temperature record, and the time since the last RCP2 power cycle.

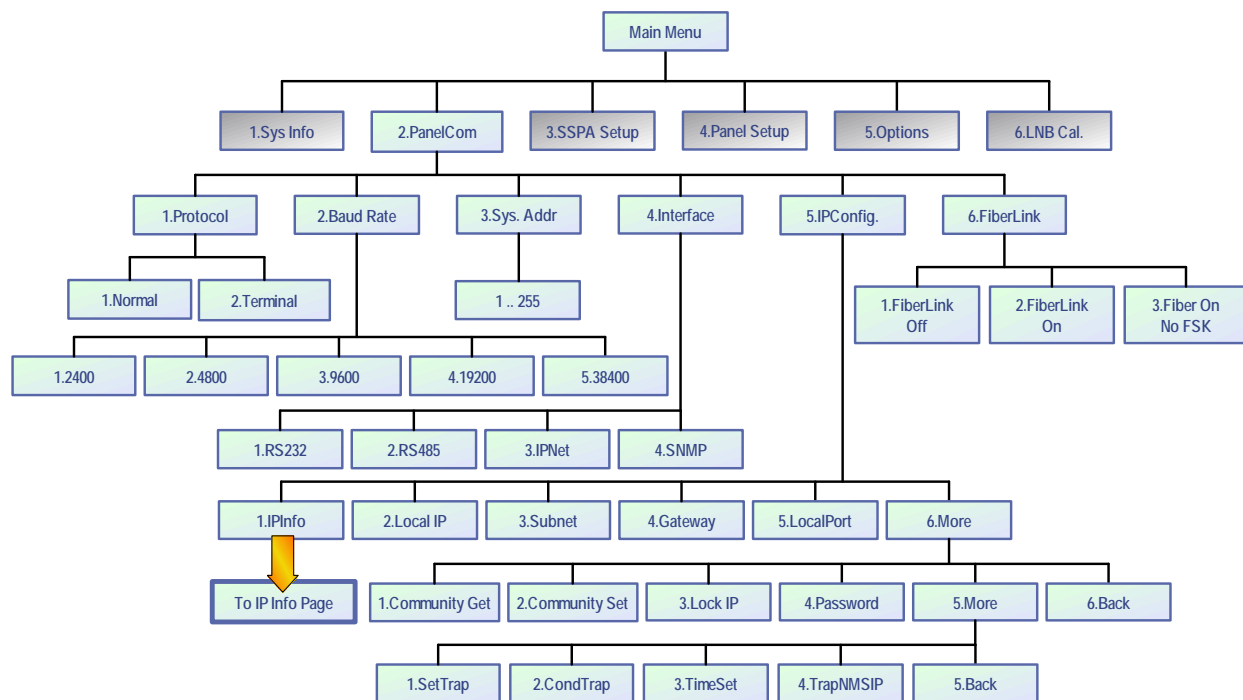


Figure 3-4: Panel Com Menu

3.2.2 Panel Com Menu

This section describes the features available which allow the user to select the parameters for the function of the RCP2 unit. Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key. See **Figure 3-4**.

3.2.2.1 Protocol

This selection sets the protocol for the main serial port (PC Interface). Available selections are: "Normal" for emulation of Compact Outdoor String Serial Protocol, and "Terminal" for terminal mode type protocol.

3.2.2.2 Baud Rate

This menu choice provides the baud rate selection for main serial port. The user can select from: 2400, 4800, 9600, 19200 and 38400 baud. Default is 9600 baud.

3.2.2.3 Sys.Address

This selection allows the user to set the RCP2 unit's unique network address. Selection range is 0 to 255; address 170 is reserved for global calls. Factory default is 0.

Note: Changes in serial communication settings from the front panel are effective immediately. Changes to these parameters over serial interface require a unit reset in order to take effect. Reset the unit by cycling power or by issuing a reset command, as described in **Section 3.2.5.5**.

3.2.2.4 Interface

This menu choice provides the selection of the physical interface of the main serial port. Choose between RS232, RS485, IPNet (Ethernet) and SNMP interfaces.

3.2.2.5 IP Config.

This menu allows the user to select between the following menu items.

Note: For each menu item below that allows the user to set an address, use the **Left Arrow** (◀) and **Right Arrow** (▶) keys on the front panel to navigate through the address field, and the **Up Arrow** (▲) and **Down Arrow** (▼) keys to increase or decrease the highlighted figure. Press the **Enter** key to lock in the new address.

- **IP Info** — Allows the user to review all IP Net Settings (as described in **Section 3.2.1.8** through **Section 3.2.1.11**);
- **Local IP** — Allows the user to set the Local IP address of the unit.
- **Subnet Mask** — Allows the user to set the Subnet Mask address of the unit;
- **Default Gateway** — Allows the user to set the Default Gateway address of the unit;
- **Local Port** — Allows the user to set the Local Port address of the unit;
- **More** — Expands to the menus detailed in **Section 3.2.2.5.1**.

3.2.2.5.1 More Menu from IP Config.

This menu allows the user to set the Community String Selection (Set/Get), the Lock IP address, and assign the Web Password.

Use the **Up Arrow** [▲] and **Down Arrow** [▼] keys to browse through selected characters. Press the **Up Arrow** [▲] and **Down Arrow** [▼] keys simultaneously to erase the selected character. Press the **Left Arrow** [◀] and **Right Arrow** [▶] keys to navigate within the string. Press the **Enter** key to save the selection.

- **Community Get** — Allows the user to set the SNMP Community Get string for the unit. Maximum length is 20 characters. Default is “**public**”.
- **Community Set** — Allows the user to set the SNMP Community Set string for the unit. Maximum length is 20 characters. Default is “**private**”.
- **Lock IP** — This selection allows user to set the IP address from which requests will be accepted by the amplifier. The LockIP selection gives the user the ability to increase the security measure for the IPNet protocol. The SSPA will answer a request which comes only from the assigned IP address. For firmware prior to version 6.00, set this address value to 0.0.0.0 or 255.255.255.255 to disable this feature.

Starting with version 6.00, the Lock IP address function has been updated to allow “Binding” and “Masking” functions. Binding” means that the first datagram retrieved for this socket will bind to the source IP address and port number. Once binding has been completed, the SSPA will answer to the bound IP source until the unit is restarted or reset. Without binding, the socket accepts datagrams from all source IP addresses. Address 0.0.0.0 allows all peers, but provides binding to first detected IP source; Address 255.255.255.255 accepts all peers, without binding. If Lock IP is a multicast address, then the amplifier will accept queries sent from any IP address of multicast group.

- **Web Password** — This selection allows the user to set the password for the web interface. Default is “**paradise**”. Erase all characters to disable password protection.
- **More** — This selection opens the menu items listed in **Section 3.2.2.5.2**.
- **Back** — This selection opens the menu items listed in **Section 3.2.2.5**.

3.2.2.5.2 More (SNMP Trap Information)

- **Set Trap**— This selection allows the user to set the Settings Trap
- **Cond Trap** — This selection allows the user to set the Conditions Trap;
- **Time Set** — This selection allows the user to set the time. Clock output format is YY/MM/DD HH:mm. Only 24-Hour format is supported at this time. Press the **Up Arrow** [▲] key to increment the value highlighted by the cursor. Press the **Down Arrow** [▼] key to decrease the value highlighted by the cursor. Press the **Right Arrow** [▶] key to move the cursor to the right; Press the **Left Arrow** [◀] key to move the cursor to the left;
- **TrapNMSIP** — This selection allows the user to set the Trap NMS IP Address;
- **Back** — This selection opens the menu items listed in **Section 3.2.2.5.1**.

3.2.2.6 FiberLink

This selection allows the user to toggle the FiberLink Off, On or On with no FSK.

- **Off** — FiberLink transceiver is disabled;
- **On** — FiberLink transceiver enabled;
- **No FSK** — FiberLink transceiver is enabled, but FSK M&C link is disabled. In this mode, the SSPA must connected to the RCP unit via the RS485 link.

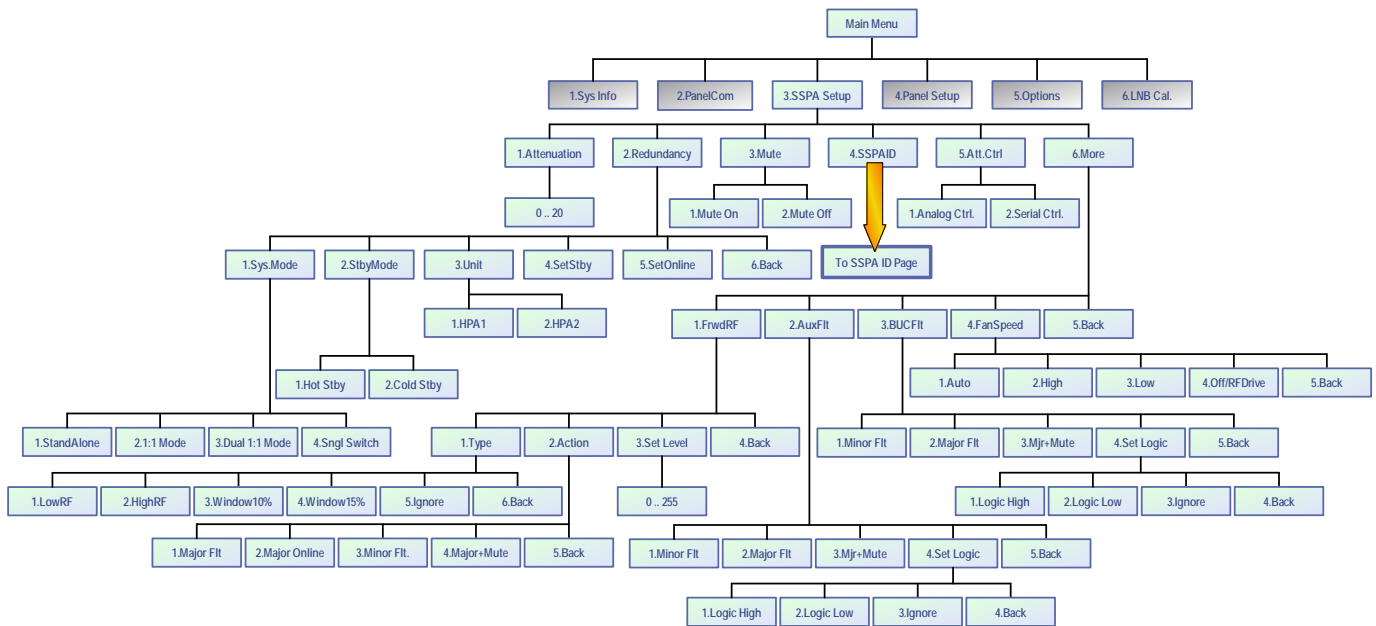


Figure 3-5: SSQA Setup Menu

3.2.3 SSQA Setup Menu

This section describes the features available on the Options menu of the controller. The operation parameters can be accessed from the VFD menu. Press the **Main Menu** key; select **3.SSPA Setup** and press the **Enter** key. See **Figure 3-5**.

3.2.3.1 Attenuation

Allows the user to change the attenuation of the remote SSQA. Range is 0 to 20 dB;

3.2.3.2 Redundancy

Provides access to redundancy related settings of the remote SSQA.

- **SysMode** — The user may select the system mode: “Standalone”, “1:1”, “Dual 1:1”, or “Single Switch”.
- **StbyMode** — The user may set the SSQA standby mode to either “Hot” or “Cold”. In hot standby mode, the HPA retains an unmuted state during standby period. In cold standby mode, the HPA mutes in standby mode and unmutes when switched back on-line.
- **Unit** — The user may assign the SSQA to either HPA1 or HPA2.
- **SetStby** — Select this menu item to set the SSQA as the standby HPA in a redundant system.
- **SetOnline** — Select this menu item to set the SSQA as the online HPA in a redundant system.
- **Back** — This selection opens the menu items listed in **Section 3.2.3**.

3.2.3.3 Mute

Allows the user to mute or unmute the remote SSPA.

3.2.3.4 SSPAID

Provides information about the type of the Remote SSPA. See **Section 3.2.1.12** and **Section 3.2.1.13**.

3.2.3.5 Att.Ctrl

Provides switching between analog and serial attenuation control. When set to analog mode, the user cannot control the remote SSPA attenuation from the RCP unit.

3.2.3.6 More

Provides access to the fault settings and fan speed menus, described in **Section 3.2.3.7** through **Section 3.2.3.11**.

3.2.3.7 FrwdRF

Allows the user to control the SSPA Forward RF fault function.

3.2.3.7.1 Type

This option submenu allows the user to change the desired Forward RF fault type. Submenu offers following choices:

- **LowRF** — Forward RF fault triggered on RF levels below preset level;
- **HighRF** — Forward RF fault triggered on RF levels above preset level;
- **Window10%** — Forward RF fault will be triggered if RF level falls outside a value of $\pm 10\%$ of the preset level;
- **Window15%** — Forward RF fault will be triggered if RF level falls outside a value of $\pm 15\%$ of the preset level;
- **Ignore** — Forward RF fault is disabled and not triggered by any RF level.

3.2.3.7.2 Action

This option submenu allows the user to change the effect of a registered Forward RF fault on SSPA functionality.

- **Major Flt** — Forward RF fault will set SSPA Summary alarm when registered;
- **Major Online** — This option can be used when remote SSPA is configured in 1:1 or Dual 1:1 redundancy mode. In these modes, a Forward RF fault will be triggered only if the SSPA unit is in the “Online” configuration and outputting RF to the antenna feed. A fault will be ignored for the “Standby” unit. If the SSPA is in “Standalone” mode, this option is the same as a “Major Flt”;
- **Minor** — Forward RF fault function is isolated from the SSPA Summary alarm. Summary alarm will not be affected by the current state of the Forward RF fault;
- **Major+Mute** — In this configuration, the SSPA Summary alarm will be triggered when a Forward RF fault is detected. The SSPA also will be forced to a mute state. The Forward RF fault will be latched by the SSPA to prevent mute function oscillation. If this condition is triggered by a RF Fault, the user will need to disable the Forward RF fault in order to clear the fault and unmute SSPA;

3.2.3.7.3 Set Level

This selection allows the user to set the desired Forward RF level. This level is used as the trigger threshold for a Forward RF fault.

3.2.3.8 AuxFlt

Allows user to control SSPA Auxiliary fault function.

- **Minor Flt** — This selection sets the Auxiliary fault as minor fault, which will not trigger an SSPA Summary fault;
- **Major Flt** — Sets Auxiliary fault as major fault. Registered fault condition will trigger SSPA Summary fault;
- **Major+Mute** — In this configuration SSPA summary alarm will be triggered when Auxiliary fault is detected. Also SSPA will be forced to a mute state.
- **Set Logic** — Allows the user to set the trigger condition for the SSPA Auxiliary fault. Selections include: “Logic High”, where an Auxiliary fault will be registered if logic high level detected on SSPA auxiliary input pin; “Logic Low”, where an Auxiliary fault will be registered if logic low level detected on SSPA auxiliary input pin; “Ignore”, where the SSPA Auxiliary fault function is disabled.

3.2.3.9 *BUCFlt*

Allows user to control SSPA frequency Block Up Converter (BUC) fault function. Sub menu allows following options to select:

- **Minor Flt** — Sets BUC fault as minor fault, which not triggering SSPA summary fault;
- **Major Flt** — Sets BUC fault as major fault. Registered fault condition will trigger SSPA Summary fault;
- **Major+Mute** — In this configuration SSPA summary alarm will be triggered when BUC fault is detected. Also SSPA will be forced to a mute state.
- **Set Logic** — Allows the user to set the trigger condition for the SSPA BUC fault. Selections include: “Logic High”, where a BUC fault will be registered if a logic high level is detected on the SSPA auxiliary input pin; “Logic Low”, where a BUC fault will be registered if a logic low level is detected on the SSPA auxiliary input pin; or, “Ignore”, where the SSPA BUC fault function is disabled.

3.2.3.10 *FanSpeed*

Option allows user to control SSPA fan speed function (if equipped). The following selections are available: Auto, High, Low or Off/RFDrive. Consult the SSPA product manual for details.

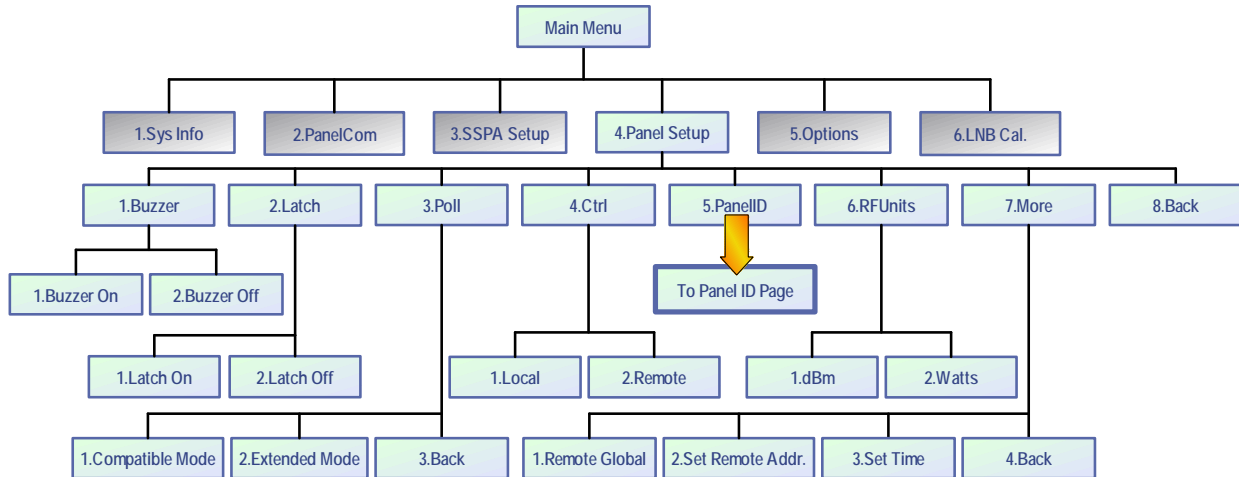


Figure 3-6: Panel Setup Menu

3.2.4 Panel Setup Menu

This section describes the features available on the Panel Setup menu of the controller. The operation parameters can be accessed from the VFD menu. Press the **Main Menu** key; select **4.Panel Setup** and press the **Enter** key. See **Figure 3-6**.

3.2.4.1 Buzzer

Allows the user to enable or disable the audible alarm buzzer;

3.2.4.2 Latch

This menu controls the RCP2 fault latch function. When enabled (Latch On), the unit will retain a detected fault condition until the user executes a “Clear Fault” command (see **Section 3.2.5.5**, selection **4.ClrFlts**).

3.2.4.3 Poll

Allows the user to select type of serial polling sequence. Possible selections include:

- **Compatible mode**— This option sets the RCP2 to work with legacy CO SSPA products. This mode must be selected for SSPAs with serial number 399,999 and below. Extended serial protocol fields such as Reflected RF detector reading are disabled in this mode
- **Extended mode** — This mode could be used for newer CO SSPA products with serial number 400,000 and above. This mode must be enabled to work with SSPA units equipped with a Reflected RF detector.

3.2.4.4 Control

Allows the user to switch between Local and Remote control.

3.2.4.5 PanelID

Provides information about the RCP2-1000 unit, serial number and firmware version of the unit's controller board and some other additional information. See **Section 3.2.1.14** through **Section 3.2.1.16**.

3.2.4.6 RF Units

Select the type of unit (dBm or Watts) displayed on the information menu.

3.2.4.7 More

Provides access to settings described in **Section 3.2.4.7.1** through **Section 3.2.4.7.4**.

3.2.4.7.1 Remote Global

When selected, this setting allows the user to connect the RCP unit to any available SSPA, regardless of its unique serial address. However, in this case, only one SSPA unit can be connected to the serial bus between the SSPA and RCP unit. This setting was the default mode for older generation RCP units.

3.2.4.7.2 Set Remote Addr.

This selection allows the user to define the address of the remote SSPA. Multiple SSPA units can be attached to the same RS485 bus and the RCP2 unit can connect to any particular one as needed .

3.2.4.7.3 Set Time

This selection allows the user to set the time of the internal clock of the RCP2 unit. Clock output format is YY/MM/DD HH:mm. Only 24-Hour format is supported at this time. Press the **Up Arrow** [▲] key to increment the value highlighted by the cursor. Press the **Down Arrow** [▼] key to decrease the value highlighted by the cursor. Press the **Right Arrow** [▶] key to move the cursor to the right; Press the **Left Arrow** [◀] key to move the cursor to the left; Press the **Enter** key to accept the displayed time. User set time is power dependent. A backup capacitor is used to keep the clock running while the unit is powered down. The clock will need to be reset if the unit remains without power longer than 5 hours.

3.2.4.7.4 Back

Returns to the Panel Setup Sub-Menu (**Section 3.2.4**).

3.2.4.8 Back

Returns to the Main Menu (**Section 3.2**).

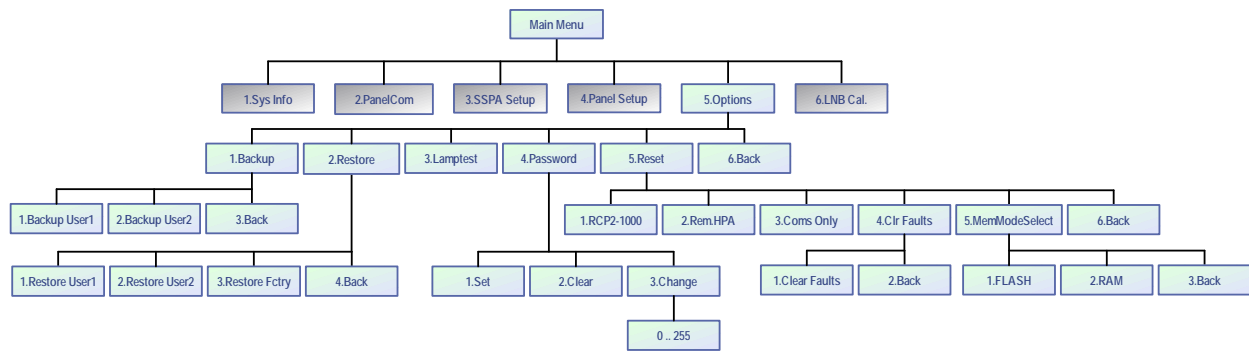


Figure 3-7: Options Menu

3.2.5 Options Menu

This section describes the features available on the Options menu of the controller. The operation parameters can be accessed from the VFD menu. Press the **Main Menu** key; select **5.Options** and press the **Enter** key. See **Figure 3-7**.

3.2.5.1 Backup

Allows the operator to back up all settings to nonvolatile memory. There are two repositories for saved settings. Menu selections include:

- **1.Backup User1** — Select to save current settings to User1 repository;
- **2.Backup User2** — Select to save current settings to User2 repository;
- **3.Back** — Returns to Options Sub-Menu (**Section 3.2.5**).

3.3.5.2 Restore

Allows the user to restore saved settings from a previous backup or factory pre-set. Menu selections include:

- **1.Restore User1** — Select to restore settings saved in User1 backup;
- **2.Restore User2** — Select to restore settings saved in User2 backup;
- **3.Restore Fctry** — Select this item to restore factory default settings;
- **4.Back** — Returns to Options Sub-Menu (**Section 3.2.5**).

3.2.5.3 LampTest

This selection activates all LED indicators on the front panel, including the Fault Indicators, Amplifier Selection, Signal Path Mimic Display, Local/Remote Key and Auto/ Manual Key. Press the **Enter** key to exit the Lamp Test.

3.2.5.4 Password

Allows the user to set, clear, or change a password that prohibits others from changing controller settings. Menu selections include:

- **1.Set** — Enables password protection; uses last saved number (1-255);
- **2.Clear** — Disables password protection;
- **3.Change** — Allows user to define the password. A number from 1-255 can be selected. Use the front panel navigation keys to set the number. The **Up Arrow** (▲) and **Down Arrow** (▼) keys change the number by factors of 10. The **Left Arrow** (◀) and **Right Arrow** (▶) keys change the number in increments of 1; Press the **Enter** key to accept the new password.
- **4.Back** — Returns to the Options Sub-Menu (**Section 3.2.5**).

3.2.5.5 Reset

Allows the user to reset the controller hardware to activate certain settings. For example, when the IP Address is modified the unit must be reset for it to use the new IP Address. Firmware version 6.00 allows multiple reset levels for the unit:

- **1.RCP Unit** — Resets all hardware on the removable M&C card of the unit. All communication links to remote M&C will be dropped until reset process is complete. The unit will start up using currently selected communication parameters (IP address, baud rate, etc). Command of a remote HPA system will not reset. However, power supplied by the unit to LNAs/LNBs will be turned off during reset and turned back on after reset is completed;
- **2.HPA Sys.** — Sends full reset command to remote control HPA system
- **3.Coms only** — Resets only communication parameters. Remote COM and IP links will be dropped and re-enabled with currently selected parameters;
- **4.ClrFaults** — Clears all latched faults and remaining fault history information. Unit remains fully operational during the process;
- **5.MemMode** — Allows alternate settings retention function. Two choices are allowed:
 - **FLASH** — Default mode. Without user intervention, the unit will retain this mode of operation. All changes to settings setup performed over local or remote interface will be backed up to EEPROM within 3 seconds. If the unit experiences a power cycle or reset, the last saved set of settings will be applied to the unit upon each power up or I/O card reset. Any EEPROM device has a limited ability to endure write cycles. Maximum write cycles for units with firmware version prior to 6.00 is 150,000 times. After exceeding this limit, the unit will operate in RAM mode, utilizing a default set of settings on each power up.

-
- Firmware version above 6.00 allows a minimum of 3,000,000 write cycles before opting out to RAM mode;
- RAM — In this mode, the unit will not backup any settings changes to internal EEPROM. This mode is optional and needs to be set by the user every time when the unit endures a power cycle or I/O card reset. This mode is beneficial when frequent changes are necessary to the unit state (such as mute/unmute or attenuation changes). Since any EEPROM device has limited write cycles, RAM mode allows the user to execute unlimited settings changes. If the unit experiences a power or reset cycle in RAM mode, it will use the last saved settings setup before RAM was engaged.

3.2.5.6 Back

Returns to the Main Menu (**Section 3.2**).

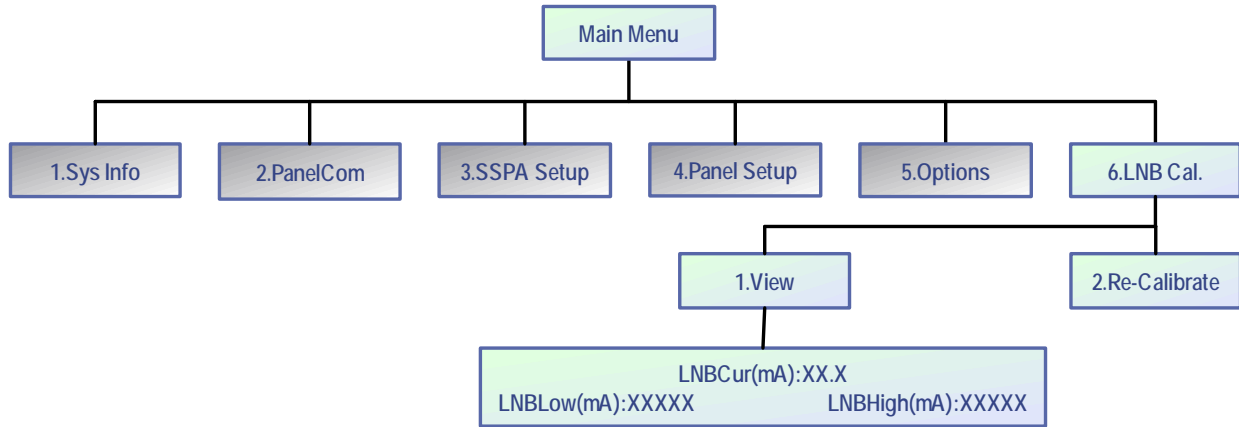


Figure 3-8: LNB Calibration Menu

3.2.6 LNB Calibration Menu

This section describes the features available on the LNB Cal. menu of the controller. The operation parameters can be accessed from the VFD menu. Press the **Main Menu** key; select **6.LNB Cal.** and press the **Enter** key. See **Figure 3-8**.

3.2.6.1 View

When this selection is chosen, the VFD displays the current draw (in mA) of an LNB connected to the remote SSPA, as well as the lowest and highest current measurements.

Press the **Up Arrow** (▲) key to return to the previous menu. Press the **Left Arrow** (◀) key or **Right Arrow** (▶) key to open the Attenuation Select menu (see **Section 3.2.3.1**).

3.2.6.2 Re-Calibrate

Select and press the **Enter** key to calibrate the system LNB at the current level.

THIS PAGE LEFT INTENTIONALLY BLANK

4.0 Introduction

The RCP2-1000-CO Remote Control Panel was designed to provide easy remote Monitor and Control for the Teledyne Paradise Datacom Compact Outdoor Solid State Power Amplifier (SSPA), and may also be used to control a remote High Power Outdoor SSPA. The unit is designed to fit a standard 1 rack unit high, 19" wide EIA rack. The Remote Control Panel allows the user to remotely access the SSPA to verify its internal conditions and provide necessary adjustments to its settings.

4.1 Fault Analysis and Condition Tracking

The RCP2-1000-CO Remote Control Panel provides detection and display of the Compact Outdoor SSPA and provides the ability to track faults locally. The remote control panel outputs the following SSPA faults: Low Regulator Voltage Fault, High Temperature Fault, Low DC Current Fault, Auxiliary Fault, RF Switch, BUC fault (if applied) and Summary Fault. Faults that are local to the Remote Control Panel (not implemented on the SSPA itself) provide additional control over remote interface: Low RF Fault, Power Supply Fault.

The Remote Control Panel also monitors various internal conditions of the remote SSPA, such as: Base plate temperature, Power supply output voltage, SSPA DC Current consumption, Regulator output voltage, RF Output level, Gate Drive Voltage, Muting, Attenuation and internal redundancy control (if applied).

In addition, the Remote Control Panel features an audible alarm and fault latching capability. Fault output varies and is provided in different forms: relay contact closure, front panel LED and (or) VFD indication, Serial data protocol field.

4.1.1 Summary Fault

This fault reflects the overall state of the remote SSPA. Only "major" faults affect the summary fault state. Some faults may or may not affect the summary fault depending on the remote SSPA settings as well as RCP settings. Fault state signaling: Front Panel LED; Front Panel VFD; Serial Protocol Field, Form C contact closure.

4.1.2 Power Supply Fault

Major fault. Fault implemented on the RCP2-1000-CO only. Remote SSPA won't track this condition. Fault effective if the SSPA internal power supply has an output voltage lower than 10 volts. Fault threshold value is fixed at the factory and can't be changed by user. Fault state signaling: Front Panel LED; Front Panel VFD; Serial Protocol Field, Form C contact closure.

4.1.3 Voltage Regulator Output Low Fault

Fault effective when remote SSPA internal voltage regulators drop the output voltage below 8 Volts. Fault always retains its last state when SSPA muted. Fault threshold value is factory fixed and can't be changed by user. Fault state signaling: Front Panel LED; Front Panel VFD; Serial Protocol Field, Form C contact closure (in Standalone mode only).

4.1.4 High Temperature Fault

This fault is set when the remote SSPA's base plate reaches a dangerously high temperature. Fault state signaling: Front Panel LED; Front Panel VFD; Serial Protocol Field, Form C contact closure.

4.1.5 Low DC Current Fault

Major Fault. This fault is set when the remote SSPA indicates abnormally low current consumption. Fault always retains its last state when the SSPA is muted. The fault threshold value is factory fixed and can't be changed by user. Fault state signaling: Front Panel LED; Front Panel VFD; Serial Protocol Field, Form C contact closure.

4.1.6 Low Forward RF Fault

Fault is local to the RCP2-1000-CO unit. Fault alerts the user when the output power falls below the threshold value. Threshold value is adjustable by the user with 1 dBm steps. Fault handling is adjustable by user. Selection for fault handling: Alert Only (Minor Fault), Fault (Major Fault), Ignore (No Fault tracking); Settings are available through the front panel menu and remote control protocol. Fault state signaling: Front Panel VFD; Serial Protocol Field, Form C contact closure.

4.1.7 BUC Fault

This fault is available only for Compact Outdoor SSPAs with the internal BUC option. In general, a BUC fault is a major fault. Fault state signaling: Front Panel VFD; Serial Protocol Field, Form C relay contact closure.

4.1.8 Auxiliary Fault

User configurable fault. Fault condition occurs when HPA senses change of the state on external auxiliary fault input line. Fault effect depends from the customer settings for this fault. Fault state signaling: Front Panel VFD; Serial Protocol Field, Form C contact closure (in Standalone mode only).

4.1.9 RF Switch Fault

In Redundant mode, the SSPA always tracks the position of the RF switch(es). The user is informed about the RF switch state through front panel VFD and serial protocol. If switch position for any reason can't be reliably determined, SSPA declares RF switch fault state.

4.1.10 Internal Mute Condition Fault

The SSPA Mute condition is invoked by a command from the operating front panel mute button of the RCP2-1000-CO, or by command on the serial line. The mute state will retain its last state even if the SSPA or RCP unit was turned off for period of time. Condition state signaling: Front Panel VFD; Serial Protocol Field, Form C contact closure (in conjunction with external mute condition).

4.1.11 External Mute Condition Fault

The SSPA Mute condition involves a hardware bypass of the mute circuitry. The possible cause of this type of condition is an open contact for external mute on SSPA M&C connector or an over-temperature shutdown. External Mute has a priority over internal mute. In other words, if the SSPA is muted externally, its mute state can't be changed by operating the buttons on front panel of the RCP, or by a command on the serial line. Condition state signaling: Front Panel VFD; Serial Condition state signaling: Front Panel VFD; Serial Protocol Field, Form C contact closure (in conjunction with external mute condition).

4.1.12 Serial Connection Fault

If serial communication can't be reliably established with a remote SSPA unit, the RCP unit will declare a Serial Connection fault condition. This condition sets all major alarms and the summary state to the fault state. In addition, the front panel VFD will display "No Connection!!" See **Figure 4-1**. The display will automatically clear if a connection is successfully established. This condition will not prevent the user from browsing through RCP menus to observe the last read parameters of the remote unit.



Figure 4-1: No Connection Display

4.2 Design Philosophy

The RCP2-1000-CO Remote Control Panel was designed to achieve a new level in high reliability, maintenance-free operation. A tightly integrated modular assembly approach has been used to realize a versatile controller while maintaining its user friendly operator interface.

Four basic building blocks are combined in the RCP2-1000-CO Remote Control Panel:

1. Digital Core Board
2. I/O Board Assembly
3. Vacuum Florescent Display
4. Front Panel Membrane Keypad

4.2.1 Digital Core Board

The Digital Core Board is microprocessor based control assembly providing all control functions of the RCP2 unit. This board features RS485 serial interfaces to connect the RCP2 to a remotely controlled SSPA unit, as well as a selectable RS232/RS485 interface to connect the RCP2 unit to a management and control system.

The board also supports the Ethernet 10/100 Base-T interface. All interfaces feature full galvanic isolation from the RCP2 chassis ground. As an added measure, all lines on the serial interfaces are connected to surge protection TVS devices.

4.2.2 I/O Board Assembly

The I/O Board Assembly contains the primary (hardware) interface circuitry of the Remote Control Panel. It is physically attached to the Digital Core Board by two 40-pin headers. The ten (10) Form C relays and opto isolated inputs for the parallel I/O interface are included on this board assembly. The board also provides a physical connection between the liquid crystal display (VFD), front panel membrane keypad, and the Digital Core Board.

4.2.3 Vacuum Florescent Display

The RCP provides a large two line by 40 character alphanumeric display. This provides an extremely user friendly interface. The display is directly interfaced to the microcontroller via the address and data bus. Virtually all of the controller's setup and adjustments are accessible from the display. There is no need to access the interior of the controller to make any setup changes.

4.2.4 Front Panel Membrane Keypad

The front panel membrane keypad is a densely integrated array of LEDs and switches that comprise an important part of the user friendly interface. A great deal of human engineering has gone into the design of this membrane panel.

A full complement of alarm indicators are provided along with the display. Four separate navigation buttons along with a separate **Enter** key allow the user to easily navigate the firmware menu on the display. Separate buttons have been provided for frequently used functions further enhancing the controller's ease of use.

THIS PAGE LEFT INTENTIONALLY BLANK

5.0 Overview

A system, which includes a RCP2-1000 Controller and Compact Outdoor SSPA, can be managed from a remote computer over a variety of remote control interfaces (see **Figure 5-1**).

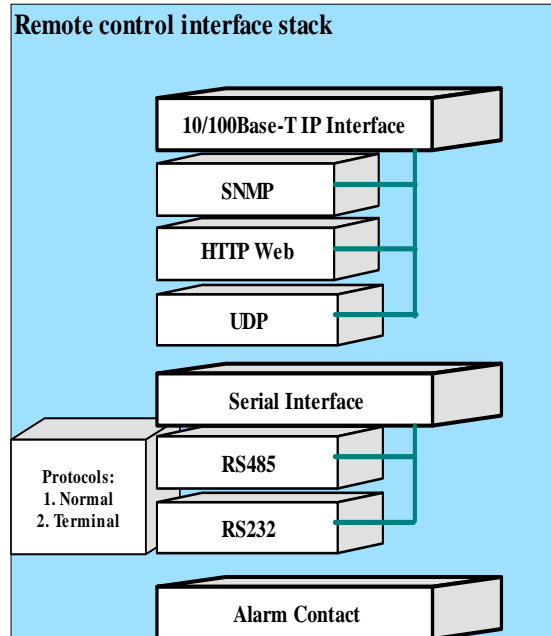


Figure 5-1: RCP2-1000 Remote Control Interface Stack

The serial interface supports both RS232 and RS485 standards. The control protocol supports two formats: the Normal serial protocol for Compact Outdoor SSPA (with some minor exceptions, as detailed in **Section 5.1**); and an ASCII based protocol suitable for HyperTerminal applications (see **Section 5.3**). Serial interface is equipped with overvoltage and overcurrent protection and benefits from full galvanic isolation from the chassis ground for extra protection.

The Ethernet interface provides the ability to control the system through: IPNet interface (UDP encapsulated Normal Compact Outdoor serial protocol – **Section 5.5.2**); SNMP V1 (**Section 5.5.4**) or HTTP Web interface (**Section 5.5.3**).

When making changes to the system operation over a remote interface, keep in mind the RCP2-1000 is not the final target for parameter changes. Requested parameter changes will not be reflected instantly on the RCP2-1000. The controller will resend data to the SSPA and change internal data after confirmation from the SSPA.

Serial protocol format is set at no parity, 8 bit with 1 stop bit. Baud rate is selectable through the front panel.

If using a Terminal mode protocol, the RCP2-1000 provides remote menu access through a HyperTerminal program or through an actual hardware terminal.

The Ethernet interface is fixed to the industry standard 10/100 Base-T standard. Normally, straight-through Cat5E/Cat6 cable is used to connect the RCP2-1000 to a network hub, and crossover Cat5E/Cat6 is used to connect directly to a computer's Ethernet port.

Upon start-up, the unit automatically is set to emulate the Paradise Datacom Compact Outdoor SSPA Protocol. All parameters set through this protocol will be redirected to the remote SSPA. However, some parameters can be remotely set on RCP2-1000 unit itself. In this case, device type switch tag needs to be set appropriately. Refer to **Section 5.2** for more information.

5.1 Serial Communication

This section describes the normal communication protocol between the RCP2-1000 and a host computer over RS232/RS485 serial interface. Serial port settings on host computer must be configured for 8 bit data at no parity, with 1 stop bit. Baud rate should match selected baud rate parameter on RCP2-1000 unit.

The unit will only respond to properly formatted protocol packets. The basic communication packet is shown in **Figure 5-2**. It consists of a Header, Data, and Trailer sub-packet.

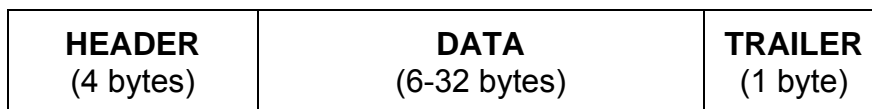


Figure 5-2: Basic Communication Packet

5.1.1 Header Packet

The Header packet is divided into 3 sub-packets which are the Frame Sync, Destination Address, and Source Address packets, as shown in **Figure 5-3**.

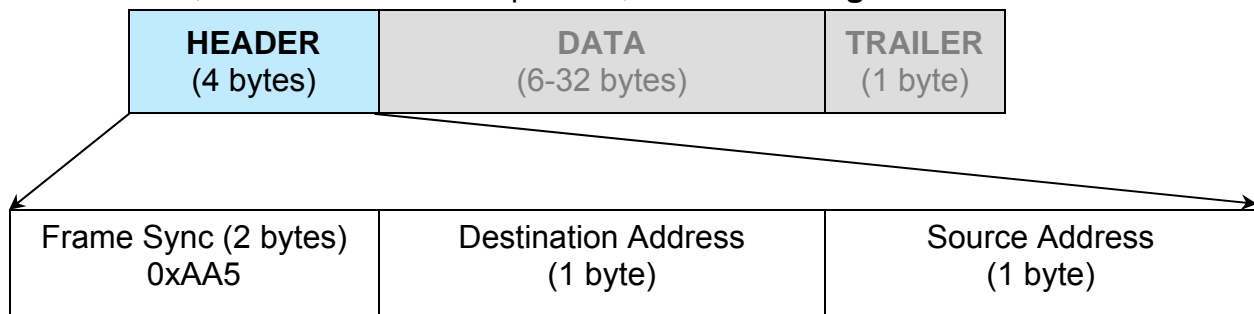


Figure 5-3: Header Sub-Packet

5.1.1.1 Frame Sync Word

The Frame Sync word is a two byte field that marks the beginning of a packet. This value is always 0xAA55. This field provides a means of designating a specific packet from others that may exist on the same network. It also provides a mechanism for a node to synchronize to a known point of transmission.

5.1.1.2 Destination Address

The destination address field specifies the node for which the packet is intended. It may be an individual or broadcast address. The broadcast address is 0xFF or 0xAA (see **Section 5.2**). This is used when a packet of information is intended for several nodes on the network. The broadcast address can be used in a single device connection when the host needs to determine the address of the amplifier. The RCP2-1000 unit will reply with its unique address.

5.1.1.3 Source Address

The source address specifies the address of the node that is sending the packet. All unique addresses, except the broadcast address, are equal and can be assigned to individual units. The host computer must also have a unique network address.

5.1.2 Data Packet

The data sub-packet is comprised of 6 to 32 bytes of information. It is further divided into seven fields as shown in **Figure 5-4**. The first six fields comprise the command preamble while the last field is the actual data.

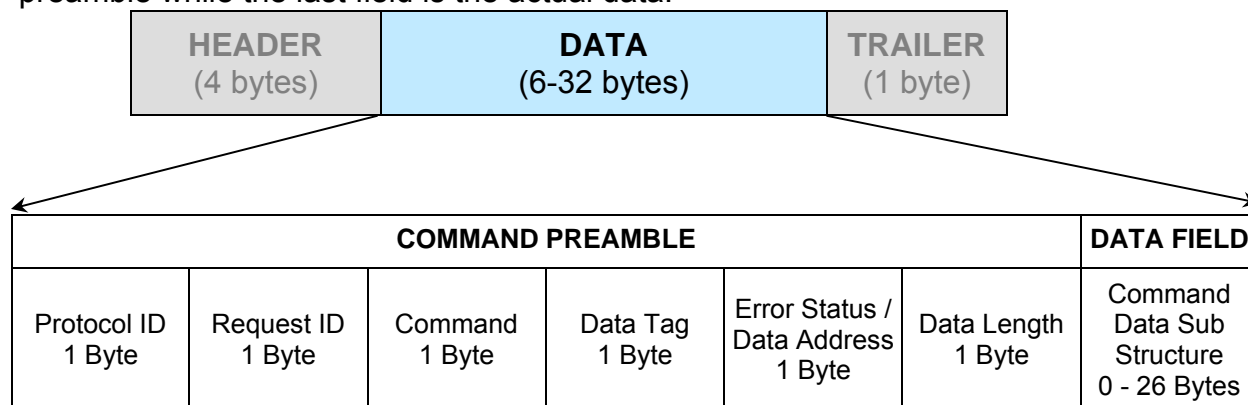


Figure 5-4: Data Sub-Packet

5.1.2.1 Protocol ID

This field provides backward compatibility with older generation equipment protocol. It should normally be set to zero. This field allows the unit to auto-detect other protocol versions, which may exist in the future.

5.1.2.2 Request ID

This is an application specific field. The amplifier will echo this byte back in the response frame without change. This byte serves as a request tracking feature.

5.1.2.3 Command

The RCP2 protocol is a table based protocol. It allows the user to view and modify data tables located on the controlled device. Throughout the remainder of this description, “sender” will refer to the host PC, and “receiver” will refer to the RCP2-1000 unit.

Sender and receiver are limited to two commands and two command responses. The Get Request command issued by a command sender allows monitoring of existing conditions and parameters on the receiver. The Get Request frame should not have any bytes in the Data Field and be no longer than 11 bytes.

The Response frame from the receiver will contain a Get Response designator in the Command field. If the receiver does not detect any errors in the Get Request frame, the requested data will be attached to the response frame. The length of the Get Response frame varies by the amount of attached data bytes. It may contain 11+N bytes where N is the amount of requested data bytes from a particular table, specified in Data Length field.

The Set Request command allows the sender to actively change parameters for the receiver’s internal configuration. The Set Request frame must contain a number of bytes in the Data Field as specified in Data length field. The frame size must be 11+N bytes, where N is the length of the attached data structure. The receiver will respond with a frame where the command field will be set to a Set Response designator. The frame length is equal to the Request frame.

The byte value for each command is given in **Table 5-1**.

Table 5-1: Command Byte Values

Command Name	Command Byte Value
Set Request	0
Get Request	1
Set Response	2
Get Response	3

Table 5-2: Data Tag Byte Values

Tag Name	Data Tag Byte Value	Minimum valid length of the Data Field	Description
System Settings Tag	0	1 Byte	This tag allows accessing various system settings on remote unit. Host access status: Full Read/Write access. Settings can be modified at any time. Some of the settings may require hardware reset of the remote RCP unit.
System Thresholds Tag	1	2 Bytes	This tag allows access to the critical unit thresholds. Host access status: Tag have read only status.
System Conditions Tag	3	1 Byte	This tag allows access to the unit's internal conditions flags, such as fault status or current system status. Host access status: Read only. This type of the data can not be set or modified remotely.
ADC Channels Access Tag	4	2 Bytes	ADC legacy access. Don't use for new development
Reserved	6	N/A	This tag is reserved
Reserved	2	N/A	This tag is reserved.
Reserved	5	N/A	This tag is reserved for factory use only
Special Command Tag (v.6.00)	10	N/A	This tag is reserved for factory use only

5.1.2.4 Data Tag

The RCP2 internal structure is organized in several tables, all of which share similar functionality and internal resources. To access the various tables, the data tag must be specified in the request frame. The data associated with certain tags is read only. Therefore only the “Get” command request would be allowed to access these data tags. The RCP2-1000 will return an error on attempts to issue a “Set” request to a read-only table tag. Various tables may contain values formatted either in 1 or 2 bytes format. The Packet Wrapper Tag provides direct access to the RCP2 Local Port and has no table association. The data tag byte values are given in **Table 5-2**.

5.1.2.5 Data Address / Error Status / Local Port Frame Length

This field is a tag extension byte and specifies the first table element of the tagged data. If the Data Length is more than 1 byte, then all subsequent data fields must be accessed starting from the specified address. For example, if the requestor wants to access the amplifier's unique network address, it should set data tag 0 (System settings tag) and data address 8 (see System Settings Details table). If the following Data Length field is more than 1, then all subsequent Settings will be accessed after the Unique Network Address.

Important! In the Response Frame Data Address field replaced with the Error Status information. The various error codes are given in **Table 5-3**.

Table 5-3: Error Status Bytes

Error Code name	Byte Value	Possible Cause
No Errors	0	Normal Condition, no errors detected
Data Frame Too Big	1	Specified Data length is too big for respondent buffer to accept
No Such Data	2	Specified Data Address is out of bounds for this tag data
Bad Value	3	Specified value not suitable for this particular data type
Read Only	4	Originator tried to set a value which has read only status
Bad Checksum	5	Trailer checksum not matched to calculated checksum
Unrecognizable error	6	Error presented in originator frame, but respondent failed to recognize it. All data aborted.

In the case of a Packet Wrapper request frame (Tag 6), the data address field is used to specify the number of bytes returned by RCP unit in response frame from local port. Byte collecting from the local port starts immediately after the wrapped frame is sent. There is no time-out, and the response frame is not sent back to the host PC until a specified number of bytes is collected from the Local Port. A new request sent by the PC host will cancel byte collecting and all collected bytes will be discarded.

5.1.2.6 Data Length

This byte value specifies the number of bytes attached to a Data Field. For a Get command, it specifies the number of data bytes that has to be returned by the RCP unit to a host PC in the Response frame. For a Set command, the value of this byte specifies the number of data fields to be accessed starting from the address specified in the Data Address byte. In general, Data Length value plus Data Address must not exceed the maximum data size particular tag.

5.1.2.7 Data Field

The actual data contained in the packet must be placed in this field. The "Get Request" type of command must not contain any Data Field. "Get Request" will be rejected if any data is present in the Data Field. Generally, the Bad Checksum error code will be added to the response from the unit. In case the data length is 2 bytes, each data word is placed in the frame with its least significant byte first. All data with length of 2 bytes must be represented as integer type with maximum value range from 32767 to (-32767). Formatting of data bytes for the Packet Wrapper frame is not important for the RCP unit. All data bytes will be redirected to the RCP2-1100 local port without any modification.

5.1.3 Trailer Packet

The trailer component contains only one byte called the Frame Check Sequence. This field provides a checksum during packet transmission. See **Figure 5-5**.

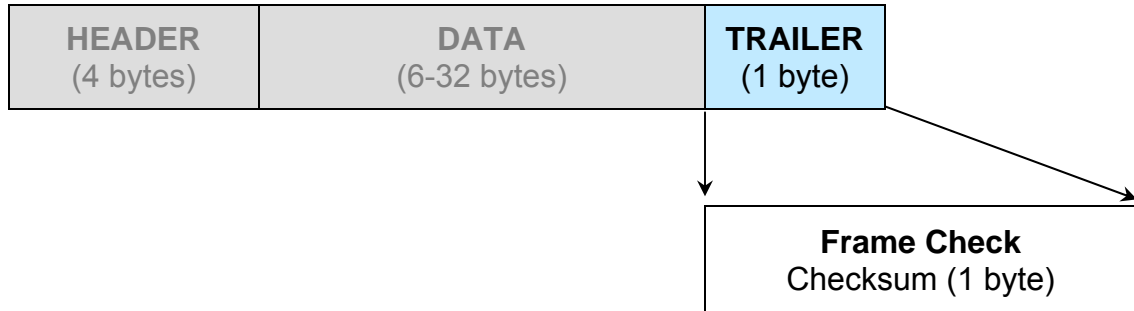


Figure 5-5: Trailer Sub-Packet

5.1.3.1 Frame Check

This value is computed as a function of the content of the destination address, source address and all Command Data Substructure bytes. In general, the sender formats a message frame, calculates the check sequence, appends it to the frame, then transmits the packet. Upon receipt, the destination node recalculates the check sequence and compares it to the check sequence embedded in the frame. If the check sequences are the same, the data was transmitted without error. Otherwise an error has occurred and some form of recovery should take place. In this case the amplifier will return a packet with the “Bad Checksum” error code set. Checksums are generated by summing the value of each byte in the packet while ignoring any carry bits. A simple algorithm is given as:

```
Chksum=0
FOR byte_index=0 TO byte_index=packet_len-1
    Chksum=(chksum+BYTE[byte_index]) MOD 256
NEXT byte_index
```

5.1.4 Timing Issues

There is no maximum specification on the inter-character spacing in messages. Bytes in messages to amplifier units may be spaced as far apart as you wish. The amplifier will respond as soon as it has collected enough bytes to determine the message. Generally, there will be no spacing between characters in replies generated by units. The maximum length of the packet sent to the amplifier node should not exceed 64 bytes, including checksum and frame sync bytes. Inter-message spacing, must be provided for good data transmission. The minimum spacing should be 100 ms. This time is required for the controller to detect a “Line Cleared” condition with half duplex communications. Maximum controller respond time is 200 ms.

5.2 Multiple Device Access

Regardless of unit type, **Table 5-4** comprises the Request Frame Structure and **Table 5-5** consists of the Response Frame Structure for communication between the unit and a remote PC.

Table 5-4: Request Frame Structure

Byte	Tag	Description
1	0xAA	Frame Sync 1
2	0x55	Frame Sync 2
3	Destination Address	- // -
4	Source Address	-// -
5	Protocol Version	Protocol Compatibility Byte, must be set 0
6	Request ID	Service Byte
7	Command	0 Set Request; 1 Get Request
8	Data Tag	0 System Settings; 1 System Thresholds; 2 Reserved; 3 Conditions; 4 ADC Data, 5 Reserved;
9	Data Address	Setting number, Sensor command, EEPROM address
10	Data Length	Total length of the data, valid values: 1 – 10
11+N	Data	Actual Data
11+N+1	Checksum	Dest. Address + Source Address + Protocol Version + Request ID + Command + Data Tag + Data Address + Data Length + Data

Table 5-5: Response Frame Structure

Byte	Tag	Description
1	0xAA	Frame Sync 1
2	0x55	Frame Sync 2
3	Destination Address	- // -
4	Source Address	-// -
5	Protocol Version	Protocol Compatibility Byte, must be set 0
6	Request ID	Service Byte
7	Command	2 Set Response; 3 Get Response
8	Data Tag	0 System Settings; 1 System Thresholds; 2 Reserved; 3 Conditions; 4 ADC Data, 5 Reserved;
9	Error Status	0 – No Errors, 1- Too Big, 2 No Such Data, 3 Bad Value, 4 Read Only, 5 Bad Checksum; 6 Unrecognized Error
10	Data Length	Total length of the data, valid values: 1 – 10
11+N	Data	Actual Data
11+N+1	Checksum	Dest. Address + Source Address + Protocol Version + Request ID + Command + Data Tag + Data Address + Data Length + Data

5.2.1 Switching between SSPA and RCP2-1000

The RCP unit provides remote control access to the SSPA monitor and control parameter tables as well as to a table related to the RCP2-1000 unit itself. Switching device control tables can be achieved by setting the Device type data field in the System settings table (Data Address 0). By default, control tables are set to access a remote controlled SSPA unit (see **Table 5-6**). The controller will emulate the SSPA protocol in full, with one exclusion — the system threshold table becomes read only (the SSPA has read/write status for this table).

If the Device type is set to RCP2-1000 by a remote Host, the values in the Settings table will represent RCP2-1000 units rather than the remote Compact Outdoor SSPA (see **Table 5-7**). To return to the default table, set the Device Type data field back to the SSPA, or reset the controller unit. When a device type switch occurs, the global call address is also changed from 0xAA for the SSPA, or to 0xFF for the RCP2-1000. The other tables remain unchanged and can be accessed at any time.

The Device type field also can be used for automatic detection of remote equipment. RCP2-1000 units with firmware versions earlier than 4.00 have no support for the device type field. Polling this data field value on older units will return an error.

System conditions are detailed in **Table 5-8** and thresholds are described in **Table 5-9**. These tables are common for both the RCP2-1000 and the Compact Outdoor SSPA.

Table 5-6: System Settings Data Values for Compact Outdoor SSPA

Data Address	# Bytes	Description	Limits and Byte Values
0	1	Device Type (Note: Changing device type will change parameters table. This table is for Device Type 2 CO SSPA)	Compact Outdoor SSPA = 2 (Current table); RCP2-1000CO=4 (Settings table changes to Table 5-7)
1	1	System Operation Mode	Single Amplifier = 255; Dual 1:1 = 1; 1:1 Redundant = 0
2	1	System Hierarchical Address	HPA 1= 0; HPA 2= 255
3	1	Unit Start Up State (in Redundancy)	Standby Amplifier = 0 On Line Amplifier = 1
4	1	Mute State	Mute Clear (Transmit Enable) = 255 Mute Set (Transmit Disable) = 0
5	1	Attenuation Level (dB down from maximum gain)	[1 value for every 0.1 dB] 0 dB attenuation = 0 20 dB attenuation = 200
6	1	Module Gain Control Authority	Serial Port Gain Control = 255 External Analog Voltage Gain Control = 0
7	1	Amplifier Network Address	0 to 255
8	1	High Temperature Alarm Threshold	0 to 125 (in °C)
9	1	SSPA module Calibration Mode	Temperature Compensated = 255 (normal state) Calibration Mode = 0
10	1	SSPA Spare Fault Status	Ignore Spare Fault = 255 Fault on value of window on ADC channel = 0 to 7 Fault on External Mute = 8
11	1	SSPA Spare Fault Handling	Minor Fault (no effect on Summary Fault) = 255 Major Fault (Triggers Summary Fault) = 0 Major Fault with Mute (Transmit Disabled) = 1
12	1	SSPA Auxiliary Fault Status	Ignore Auxiliary Fault = 255 Fault on Logic Low State = 1 Fault on Logic High State = 0 Startup in Low Z State = 2 Startup in High Z State = 3
13	1	SSPA Auxiliary Fault Handling	Minor Fault (No effect on Summary) = 255 Major Fault (Triggers Summary Fault) = 0 Major Fault with Mute (Transmit Disabled) = 1 Minor Fault with Mute = 2 (version 3.50)
14	1	Block Up Converter Fault Status	Ignore BUC Fault = 255 Fault on Logic Low State = 1 Fault on Logic High State = 0
15	1	Block Up Converter Fault Handling	Minor Fault (no effect on Summary Fault) = 255 Major Fault (Triggers Summary Fault) = 0 Major Fault with Mute (Transmit Disabled) = 1

(continued)

Table 5-6: System Settings Data Values for Compact Outdoor SSPA (continued)

Data Address	# Bytes	Description	Limits and Byte Values
16	1	Protocol Select (keep value selected to Normal protocol, not recommended to change in system with RCP2-1000CO controller)	Normal Protocol = 255 Terminal Mode = 0 Binary Mode = 1 SierraCom Protocol = 2
17	1	Baud Rate Select (keep value selected to 9600 Baud, not recommended to change in system with RCP2-1000CO controller)	9600 = 255; 38400 = 0; 19200 = 1; 4800 = 2; 2400 = 3
18	1	Reflected RF Fault Handling	Minor Fault = 0; Major Fault = 1; Disabled =255
19		Reflected RF Fault Threshold	0 - 80 dBm. Value used as High threshold.
20	1	Standby Mode	Hot standby=255; Cold standby=0
22	1	Forward RF Fault Status	Disabled =255; Fault on low RF threshold = 0 10% Forward RF power window = 1 15% Forward RF power window = 2 Fault on High RF threshold = 3
23	1	Forward RF Fault Handling	Minor Fault (no effect on Summary Fault) = 255 Major Fault (Triggers Summary Fault) = 0 Fault Online Unit Only = 1 Major Fault + Mute = 2
24	1	Forward RF Fault Threshold	0-80 dBm. Value used as Low, Window center point or High threshold, depending on Forward RF Fault status setting.
25	1	Fan Speed Control	Fan Speed Low = 0; Fan Speed High = 1; Fan Speed Auto = 2; Off/Default (RF Level Control) = 255
26	1	Switch Mute	Switch Mute Off = 255; Switch Mute On = 0

Table 5-7: System Settings Data Values for RCP2-1000 Controller

Data Address	# Bytes	Description	Limits and Byte Values
0	1	Device Type (Note: Changing device type will change the parameters table.)	Compact Outdoor SSPA = 2 (Settings table changes to Table 5-6); RCP2-1000CO = 4 (Current Table)
1	1	Reserved	Factory use only
2	1	Remote SSPA address	0 - 255. Setting address to 170 for global call
3	1	Control Mode	1. Local = 0; 2. Remote = 1
4	1	Polling mode	1. Compatible = 0; 2. Extended
5	1	Reserved	Factory use only
6	1	Main serial port protocol	1.Normal=0; 2.Terminal=1
7	1	Main serial port baud rate	1 1. 9600=0; 2.2400=1; 3. 4800=2; 4. 19200=3; 5.38400=4
8	1	Network Address	Valid Values 0 -254
9	1	Remote control interface type	1.RS232=0; 2.RS485=1; 3.IPNet=2; 4.SNMP=3
10	1	FiberLink interface	1.Off=0; 2.On=1
11 - 12	2	Reserved	Factory use only
13	1	Fault Latch	1.Disable=0; 2.Enable=1
14 - 15	2	Reserved	Factory use only
16	1	Menu Password	Valid Values=0..255
17	1	Reserved	Factory use only
18	1	Audible Alarm Buzzer	1.Disable=0; 2.Enable=1
19	1	Menu Password Protection	1.Disable=0; 2.Enable=1
20	1	RF Units (VFD Menu only)	1.dBm=0; 2.Watts=1
21-23	3	Reserved	Factory use only
24	1	Low Forward RF (RCP2-1000 only)	1.Disable=0; 2.Major Fault=1; Minor Fault=2
25-26	2	Reserved	Factory use only
27	1	Reserved	Factory use only
28	1	Reserved	Factory use only
29 - 32	4	IP Address (MSB – LSB)	Settings required for normal operation of IP interface. Consult network administrator for a proper setup. All settings physically located on the RCP2-1000 unit. Changes to these settings effective only after controller restart.
33 - 25	4	IP Gateway (MSB – LSB)	
36 - 40	4	Subnet Mask (MSB – LSB)	
41 - 42	2	Receive IP Port (MSB – LSB)	
43 - 46	4	IP Lock Address (MSB – LSB)	

Table 5-8: System Condition Addressing (Read Only)

Data Address	# Bytes	Description	Limits and Byte Values
1	2	Present DAC value (Read Only in Temp Co Mode)	0 to 1023
2	2	Present Temperature	± 125
3	2	Fault, Mute, and State Conditions	<p>2-Byte Value 0 fault clear; 1 fault set 0 mute clear; 1 mute set 0 standby state, 1 online state 0 external reference, 1 internal reference</p> <p>Lower Byte Bit 0 = Summary Fault Bit 1 = High Temp Fault Bit 2 = Low DC Current Fault Bit 3 = Low DC Voltage Fault Bit 4 = External Mute Status Bit 5 = Internal Mute Status Bit 6 = Reserved, always 0 Bit 7 = Reserved, always 0</p> <p>High Byte Bit 0 = Block Up Converter Fault Bit 1 = Spare Fault Bit 2 = Auxiliary Fault Bit 3 = EEprom Cal Table Fault Bit 4 = RF Switch Control 1 state Bit 5 = RF Switch Control 2 state Bit 6 = Reserved, always 0 Bit 7 = Unit On Line State</p>
4	2	Present Attenuation Level	1bit per 0.1 dB attenuation Low Byte: 0 to 200 High Byte: always 0
5	2	Present RF Power Level Output is dBm x 10 i.e., 455 = 45.5 dBm	0 to 1023
6	2	SSPA DC Current	200 Amp maximum 1 value = 0.1 Amp
7	2	Regulator DC Voltage	15 Volt maximum 1 value = 0.1 Volt
8	2	Power Supply Voltage	15 Volt maximum 1 value = 0.1 Volt
9	2	Transistor Gate Voltage	0 to 10 volt range Use 2's compliment integer math 1 value = 0.1 Volt

Note: This table is common for both RCP2-1000 and Compact Outdoor SSPA and will not change when the device type is switched.

Table 5-9: System Threshold Data Values (Read Only)

Data Address	# Bytes	Description	Limits and valid values
1	2	Low Current Fault Threshold	Minimum value = 0 Maximum value = 1023
2	2	Spare Fault Window Lower Limit	Minimum value = 0 Maximum value = 1023
3	2	Spare Fault Window Upper Limit	Minimum value = 0 Maximum value = 1023
4	2	Low Current Fault Threshold (Slave Side)	Minimum value = 0 Maximum value = 1023
5	2	Low Regulator Voltage Threshold (Master Side)	Minimum value = 0 Maximum value = 1023
6	2	Low Regulator Voltage Threshold (Slave Side)	Minimum value = 0 Maximum value = 1023

Note: This table is common for the RCP2-1000, Compact Outdoor SSPA. These values are for internal use only.

5.3 Examples

5.3.1 Example 1, Get Settings

Table 5-10 shows an example of a communication exchange between a PC and RCP2-1000 unit.

- RCP2-1000 Network Address = 5
- Host Computer Network Address = 10
- Request ID = 0x6F

Table 5-10: Example 1 Host PC Request String

Byte Position	Byte Value (Hex)	Description
1	AA	Frame Sync Byte 1
2	55	Frame Sync Byte 2
3	5	Destination Address of RCP unit
4	A	Source address of Request originating PC Host
5	0	Protocol Version Compatibility Field must always be 0
6	6F	Request ID byte is set by originator, will be echoed back by respondent
7	1	Command field for “Get” type request
8	0	“SSPA Settings” tag indicates which data from respondent required in response frame
9	1	Data Address field indicates the beginning data address inside of the “SSPA Settings” data set to 1 (first element)
10	A	Data Length field indicates how many data bytes of the “SSPA Settings” requested from the amplifier
11	8A	Arithmetic checksum of bytes number 3 through 10

The RCP2-1000 replies with the response string of **Table 5-11**.

Table 5-11: Example 1 SSPA Response String

Byte Position	Byte Value (Hex)	Description
1	AA	Frame Sync Byte 1
2	55	Frame Sync Byte 2
3	A	Destination Address of PC request originator
4	5	Source address of Responding Amplifier
5	0	Protocol Version Compatibility Field must always be 0
6	6F	Echo of the Originator's Request ID byte
7	3	Command field for "Get" type response
8	0	"SSPA Settings" tag indicates which data from respondent included in response frame.
9	0	Data Address field omitted and replaced with Error status code. 0 in this field indicates absence of errors.
10	A	Data Length field indicates how many data bytes of the "SSPA Settings" requested from the SSPA (12 is all available data of "System Conditions" type).
11	0	Data field 1 contains data element 1 of "System Conditions" data type
12	255	Data field 2 contains data element 2 of "System Conditions" data type
13	1	Data field 3 contains data element 3 of "System Conditions" data type
14	255	Data field 4 contains data element 4 of "System Conditions" data type
15	0	Data field 5 contains data element 5 of "System Conditions" data type
16	255	Data field 6 contains data element 6 of "System Conditions" data type
17	5	Data field 7 contains data element 7 of "System Conditions" data type
18	50	Data field 8 contains data element 8 of "System Conditions" data type
19	0	Data field 9 contains data element 9 of "System Conditions" data type
20	3	Data field 10 contains data element 10 of "System Conditions" data type
21	8F	Arithmetic checksum of bytes 3 through 20

5.3.2 Example 2, Change Attenuation

Change SSPA Attenuation to 20 dB (55dB gain) through the RCP2-1000 settings control table

- RCP2-1000 Network Address = 5
- Host Computer Network Address = 10
- Request ID = 0x6F

Table 5-12: Example 2 PC Request String

Byte Position	Byte Value (hex)	Description
1	AA	Frame Sync Byte 1
2	55	Frame Sync Byte 2
3	5	Destination Address of the unit
4	A	Source address of Request originating PC Host
5	0	Protocol Version Compatibility Field must be always 0
6	6F	Request ID is 111
7	0	Command "Set request" designator
8	0	Data tag "0" indicates access to SSPA Settings
9	5	Data address 5 indicates access to SSPA attenuation
10	1	Data length is 1 byte
11	C8	Data 200 - 20.0 dB x 10 attenuation
12	4C	Arithmetic checksum of bytes 3 to 11

Table 5-13: Example 2 SSPA Response String

Byte Position	Byte Value (hex)	Description
1	AA	Frame Sync Byte 1
2	55	Frame Sync Byte 2
3	A	Destination Address of PC request originator
4	5	Source address of the respondent
5	0	Protocol Version Compatibility Field must be always 0
6	6F	Echo of the Originator's Request ID byte
7	2	"Set Response" designator
8	0	Data Tag "0" was accessed
9	0	Data address omitted and replaced with error status "0" – no errors.
10	1	Data length is 1 byte
11	C8	Data 200 - 20.0 dB x 10 attenuation successfully set
12	49	Arithmetic checksum of bytes 3 to 11

5.3.3 Example 3, Change Attenuation (Packet Wrapper)

Change SSPA Attenuation to 15.6 dB (59.4dB gain) through packet wrapper request

- RCP2-1000 Network Address = SSPA Network Address = 1
- Host Computer Network Address = 100
- Request ID = 0x6F

Table 5-14: Example 3 PC Request String

Byte Position	Byte Value (hex)	Description
1	0xAA	Frame A Sync Byte 1
2	0x55	Frame A Sync Byte 2
3	0x01	Destination Address of the RCP2-1000 unit
4	0x64	Source address of Request originating PC Host
5	0x00	Protocol Version Compatibility Field must be always 0
6	0x6F	Request ID is 111
7	0x00	Command "Set request" designator
8	0x06	Tag indicates Packet Wrapper request
9	0x0C	Data length indicates Packet Wrapper is 12 bytes long
10	0x0C	Expected length of response packet from CO SSPA is 12 bytes long
11	0xAA	Frame B Sync Byte 1, first byte of encapsulated frame B
12	0x55	Frame B Sync Byte 2
13	0x01	Destination Address of the CO SSPA unit
14	0x64	Source address of Request originating PC Host
15	0x00	Protocol Version Compatibility Field must be always 0
16	0x6F	Request ID is 111
17	0x00	Command "Set request" designator
18	0x00	Tag 0 indicates access to SSPA System Settings table
19	0x05	Data address 5 indicates access to SSPA attenuation
20	0x01	Data length is 1 byte long
21	0x9C	Data field sets attenuation level to 15.6dBm (156 divided by 10)
22	0x76	Checksum of wrapped packet, byte position 12 to 21, last byte of frame B
23	0xDD	Checksum of entire packet, byte positions 3 to 22, last byte of frame A

Table 5-16: Example 3 PC Response String

Byte Position	Byte Value (hex)	Description
1	0xAA	Frame A Sync Byte 1
2	0x55	Frame A Sync Byte 2
3	0x64	Destination Address of the PC Host
4	0x01	Source address of Response originating RCP2-1000 unit
5	0x00	Protocol Version Compatibility Field must be always 0
6	0x6F	Returned request ID is 111
7	0x02	Command "Set response" designator
8	0x06	Tag indicates Packet Wrapper request
9	0x00	Error code 0 indicates no errors found in request frame
10	0x0C	Length of captured response packet from CO SSPA is 12 bytes long
11	0xAA	Frame B Sync Byte 1, first byte of encapsulated frame B
12	0x55	Frame B Sync Byte 2
13	0x64	Destination Address of the PC Host
14	0x01	Source address of Response originating CO SSPA unit
15	0x00	Protocol Version Compatibility Field must be always 0
16	0x6F	Request ID is 111
17	0x02	Command "Set response" designator
18	0x00	Tag 0 indicates access to SSPA System Settings table
19	0x00	Error code 0 indicates no errors found in request frame
20	0x01	Data length is 1 byte long
21	0x9C	Data field confirms setting attenuation level to 15.6dBm (156 divided by 10)
22	0x73	Checksum of wrapped packet, byte position 12 to 21, last byte of frame B
23	0xCD	Checksum of entire packet, byte positions 3 to 22, last byte of frame A

5.4 Remote Control through Terminal Protocol

The RCP2-1000 utilizes Terminal Mode Serial Protocol (TMSP) as a secondary serial protocol for Management and Control through a Remote Serial Interface.

5.4.1 Overview

TMSP allows the user to access internal RCP2-1000 functions via a remote ASCII Terminal or its equivalent (such as HyperTerminal for Windows). TMSP is accomplished through either the RS-232 or RS-485, half duplex, serial communication link. Navigation through TMSP is identical to front panel menu navigation. See **Section 3.2**.

U.S. ASCII encoded character strings are used to represent commands and data messages. A remote terminal or controller initiates a communication session and the RCP2-1000 unit takes action and returns a report of requested status. The RCP2-1000 will not initiate communication and will transmit data only when commanded to do so. Prior to establishing a session with a RCP2-1000, this mode must be enabled through the front panel menu.

The remote terminal must be configured with serial settings that match the RCP2-1000 serial port settings. For example, if the RCP2-1000 is set at 9600 Baud, the remote terminal must be also configured as an ASCII terminal at 9600 Baud, no parity, 8 bit data with 1 stop bit serial connection. The RCP2-1000 will not echo back any incoming characters, so local echo must be enabled on the remote terminal.

To establish a remote control session with the RCP2-1000 terminal, the user must type **UNIT#XXX** in the terminal window, where XXX is the RCP2-1000 unique network address or the global call address (255). Press “Enter” on the keyboard.

The RCP2-1000 should answer with **Unit#XXX OnLine** and display the first menu screen on the following lines. After a remote session is successfully established, the unit will remain connected as long as needed.

The session is organized in as menu selection with active keys. To help the user navigate through the menu, a help string with the list of active keys always follows the menu strings. For example, the following string will be the last transmission on all informative menu screens (**Note:** All key commands must be in upper case):

“Active Keys(U)p+Enter; (D)own+Enter;(C)learFlt; (M)enu+Enter; (E)nd+Enter”

To refresh the screen on the remote terminal, simply press the “Enter” key. To end a session with the RCP2-1000, press the “E” and then “Enter” keys.

Important! If multiple RCP2-1000 units are networked on the same serial link, do not establish a session with more than one RCP2-1000 at a time. If you do so, you will not get a valid response from the unit.

5.4.2 Remote Terminal Set-up

The following procedure will guide the user through the setup of a remote terminal, using Windows 95/98 HyperTerminal software. Prior to configuring the PC, the RCP2-1000 must be connected to the PC COM port and configured to use TMSP at 9600 Baud.

1. Start the Windows HyperTerminal Program (default Windows location at Programs → Accessories → HyperTerminal).
2. At the prompted window, type the name of your serial connection (“Compact Outdoor SSPA” for example), and then click “OK.” See **Figure 5-6**.

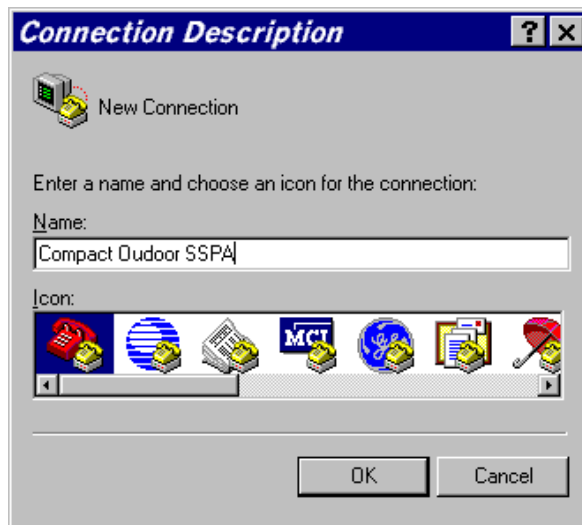


Figure 5-6: Connection Description window

3. Select a direct connection to the PC communication port (Com1 for example), to communicate with the RCP2-1000, and then click “OK.”. See **Figure 5-7**.

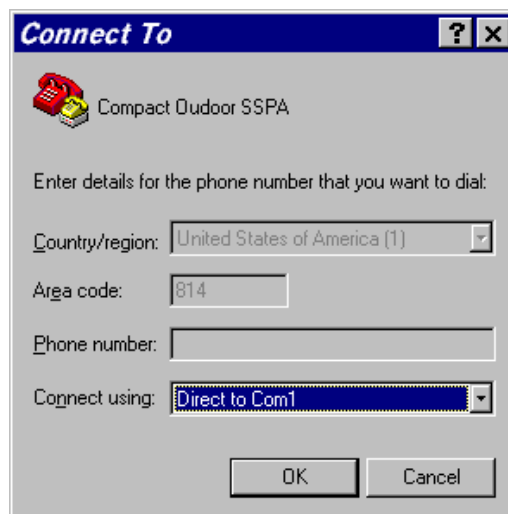


Figure 5-7: Connect To Window

-
4. On the next dialog window, choose the following settings: Bits per Second – 9600; Data bits – 8; Parity – None; Stop bits – 1; Flow control – none. Then click “OK.” See **Figure 5-8**.

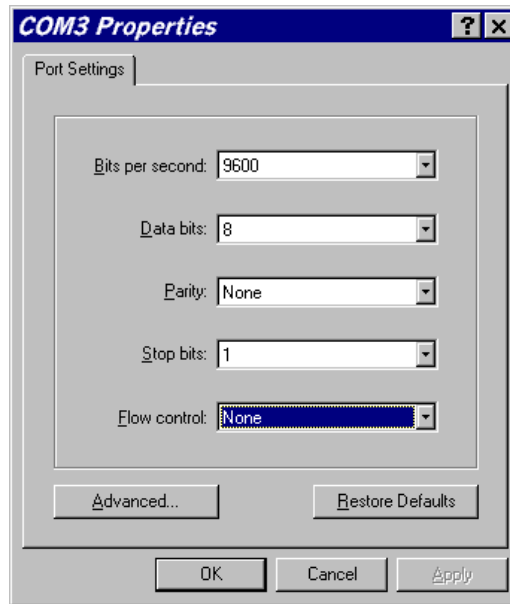


Figure 5-8: COM Properties Window

5. The RCP2-1000 will not normally echo back characters typed by the user in the Terminal window. For added security and convenience, it is recommended to turn on Local Echo on HyperTerminal itself. To do so, from the HyperTerminal top menu select as followed: File > Properties > Settings > ASCII setup. The resulting window is shown on **Figure 5-9**. Check the box marked “Echo typed characters locally” and click “OK.” Due to a software bug on some Windows versions this feature does not properly work even when checked. To fix the bug, download the latest version of HyperTerminal from <http://www.hilgraeve.com>. Do not use a version of Hyperterminal earlier than 6.3.

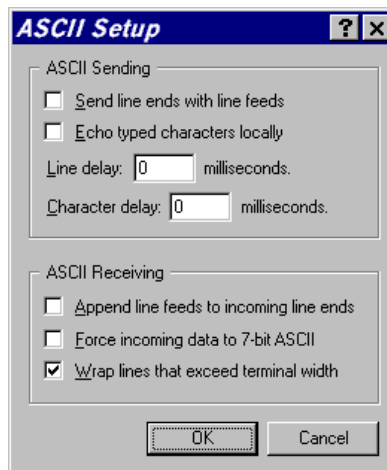


Figure 5-9: ASCII Setup Window

Your PC is now configured to communicate with the Compact Outdoor SSPA in Terminal mode. To establish a session with RCP2-1000 , type **UNIT#170**.

Note: On a RS485 network, avoid using the global address (170). Instead, use the unique RCP2-1000 address.

An example of the terminal mode session shown on **Figure 5-10**.

```
UNIT#001
Welcome! Unit#001 Online

Atten.(dB):00.0   FwdRF( dBm):147.0
  Alarms:Normal  RefRF( dBm):00.0
(B)ack; + Enter lrearFlt;(U)p;(D)own;(M)enu;(E)nd;D

Voltg:Normal HiTemp:Normal FwdRF:Normal
Curnt:Normal RFSW:Normal RefRF:Normal
Active Keys:(C)lrearFlt;(U)p;(D)own;(M)enu;(E)nd;(B)ack; + Enter
D

BUC:Normal Int.Mute:Clear State:OnLine
AUX:Normal Ext.Mute:Set Ctrl:PC Ctr
Active Keys:(C)lrearFlt;(U)p;(D)own;(M)enu;(E)nd;(B)ack; + Enter
D

DCCur(A):00.0 GateBias(V):-06.4
Regul(V):00.0 PS(V):00.5 Temp(C):+31
Active Keys:(C)lrearFlt;(U)p;(D)own;(M)enu;(E)nd;(B)ack; + Enter
-
```

Figure 5-10: Example of Terminal Mode session

5.5 Ethernet Interface

5.5.1 Overview

The RCP Ethernet port (J9) supports several IP network protocols to provide a full featured remote M&C interface over an Ethernet LAN.

- IPNet protocol — redirection of standard Paradise Datacom LLC serial protocol over UDP transport layer protocol. This protocol is fully supported in Paradise Datacom LLC's Universal M&C software.
- SNMPv1 protocol — protocol intended for integration into large corporate NMS architectures.
- HTTP Web interface — designed to allow platform independent remote control function for a single RCP2-1000 unit

To utilize either of the protocols listed above, the relevant interface option has to be turned on. Refer to **Section 5.5.2** (Setting IPNet interface), **Section 5.5.4** (Configuring unit to work with SNMP protocol) and **Section 5.5.3** Web interface for details.

Of course, standard IP level functions such as ICMP Ping and ARP are supported as well. There is currently no support for dynamic IP parameters settings (DHCP).

5.5.2 IPNet Interface

5.5.2.1 General Concept

Satcom system integrators are recognizing the benefits of an Ethernet IP interface. These benefits include:

- Unsurpassed system integration capabilities;
- Widely available and inexpensive set of support equipment (network cable; network hubs);
- Ability to control equipment over Internet;
- Ease of use

Implementation of the raw Ethernet interface is not practical due to the limitations it places on M&C capabilities by the range of a particular LAN. It is more practical to use an Ethernet interface in conjunction with the standard OSI (Open System Interconnect) model to carry a stack of other protocols. In an OSI layered stack, an Ethernet interface can be represented as a Data Link layer. All upper layers are resolved through a set of IP protocols. In order to keep data bandwidth as low as possible (which is important when M&C functions are provided through a low-bandwidth service channel) the IP/UDP protocol set is used as the Network/Transport layer protocol on Paradise Datacom SSPAs.

UDP (User Datagram Protocol) was chosen over TCP (Transmission Control Protocol) because it is connectionless; that is, no end-to-end connection is made between the RCP2-1000 unit and controlling workstation when datagrams (packets) are exchanged. Paradise Datacom provides a Windows™-based control application to establish UDP-based Ethernet communication with the RCP2-1000. The control application manages the exchange of datagrams to ensure error-free communication. An attractive benefit of UDP is that it requires low overhead resulting in minimal impact to network performance. The control application sends a UDP request to RCP2-1000 unit and waits for response. The length of time the control application waits depends on how it is configured. If the timeout is reached and the control application has not heard back from the agent, it assumes the packet was lost and retransmits the request. The number of the retransmissions is user configurable.

The Paradise Datacom RCP2-1000 Ethernet IP interface can use UDP ports from 0 to 65533 for sending and receiving. The receiving port needs to be specified through the front panel menu. For sending, it will use the port from which the UDP request originated. Of course, it is up to the user to select an appropriate pair of ports that are not conflicting with standard IP services. Paradise Datacom recommends usage of ports 1038 and 1039. These ports are not assigned to any known application.

As an application layer protocol (which actually carries meaningful data), the standard RCP2-1000 serial protocol was selected. This protocol proves to be extremely flexible and efficient. It is also media independent and can be easily wrapped into another protocol data frame. An example of the UDP frame with encapsulated Paradise Datacom protocol frame is shown on **Figure 5-11**.

UDP Header (8 bytes)	SSPA Serial Protocol Frame (11+N Bytes, 0<N<128)	CRC 16 checksum
--------------------------------	--	---------------------------

Figure 5-11: UDP Redirect Frame Example

This set of Ethernet IP protocols is currently supported by Paradise Datacom Universal M&C package (Compact Outdoor SSPA). The software package is supplied on CD with the controller unit, or can be downloaded by registered users of the company web site, <http://www.paradisedata.com>.

5.5.2.2 Setting IPNet Interface

All IP-related menu items are consolidated under **Main Menu > 2.Panel Com.**

The RCP2 controller supports multiple simultaneous interface. Typically all available IP interfaces (IpNet, Web HTTP, SNMP) are enabled when RS232 or RS485 modes are selected. It is possible to disable some of the IP-related interfaces: Selecting IPNet interface will keep IPNet interface open and disable SNMP interface. Response. Vice versa selecting SNMP interface will keep SNMP port open, but will disable IPNet interface. Web HTTP interface remains available in all modes.

Table 5-16: OSI Model for RM SSPA Ethernet IP Interface

OSI Layer	Protocol	Notes
Application	Paradise Datacom RCP2-1000 serial protocol	Frame structure described in Section 5.1 – 5.2
Transport	UDP	Connectionless transport service. MTU on target PC must be set to accommodate largest SSPA Serial Protocol Frame. Set MTU to a value larger than 127 bytes.
Network	IP	ARP, RARP and ICMP Ping protocols supported by RM SSPA controllers. Static IP Address only, no DHCP support.
Data Link	Ethernet	10/100 Base-T Network
Physical	Standard CAT5 (CAT 6) Network Cable	Maximum node length 100 m

Prior making a connection through Ethernet IP interface, the following IP parameters need to be set: IP Port address, Default Gateway, Subnet Mask, Receive IP Port and IP lock address. The IP Lock address is a security measure.

The function of the Lock IP parameter varies depending on the value:

- When the Lock IP is set to 255.255.255.255, allows unrestricted connection to all peers without binding. "Binding" means that the first datagram received for this socket will bind to the source IP address and port number. Without binding, the socket accepts datagrams from all source IP addresses and port numbers.
- Setting Lock IP to 0.0.0.0 allow connection for all peers, with binding to first one.
- Setting Lock IP to a specific IP address will limit connection just to this specific host.
- For other parameters (IP address, Gateway, Subnet, IP port) contact your network system administrator for assistance.

Important! If you are planning to access the RCP2-1000 through the Internet, you must exercise the appropriate security measures. It is strongly recommended to put RCP2-1000 units behind a protective Firewall or set up a VPN link for remote access.

After selecting the IP parameters, the user may select specific interface or keep all IP interfaces enabled simultaneously

To keep all IP interfaces active select one of the serial interfaces by enabling the RS232/485 port:

Press the **Main Menu** key; select **2.Panel Com** and press the **Enter** key; select **4.Interface** and press the **Enter** key; select either **1.RS232** or **2.RS485** and press the **Enter** key.

To select specific IP interface select:

Press the **Main Menu** key; select **2.Panel Com** and press the **Enter** key; select **4.Interface** and press the **Enter** key; select either **3.IPNet** or **4.SNMP** and press the **Enter** key.

In this case serial interface will remain active and default to RS485 option.

You may adjust any IP settings when the IPNet interface is turned on as needed, without losing your IP link. All new settings will become effective only after a RCP2-1000 controller hardware reset (Press the **Main Menu** key; select **5.Options** and press the **Enter** key; select **6.Reset** and press the **Enter** key; select **1.RCP2-1000** and press the **Enter** key; or cycle power to the unit).

The type of enabled serial protocol can be selected by choosing the "Normal" or "Terminal" protocol options. This setting will only affect protocol support for RS232/RS485 interfaces. IP interface selection will remain unchanged.

The RCP2-1000 Ethernet port can be connected to a network hub through straight through network cable or directly to a work station NIC card through a null-modem or cross-over cable (Rx and Tx lines are crossed). As soon as an Ethernet interface has been selected as the primary interface, you should be able to verify the network connection to the unit by using the Ping command from your host workstation.

To do so on a Windows based PC, open a Command Prompt window and type PING and the dot delimited IP address of the RCP2-1000, then press the Enter key. If the unit is successfully found on the network, the request statistic will be displayed.

PING XXX.XXX.XXX.XXX

If the unit does not answer on the ping command, check all hardware connections and verify that the IP settings on your host workstation and the RCP2-1000 match your network parameters. On a Windows-based PC you may also check ARP table entries. The new IP address of the RCP2-1000 may be set to another PC or network equipment with a different MAC address. Open a Command Prompt window and type "ARP

-a”, the press Enter. The current table will be displayed. If you see the RCP2-1000 IP address entry in the table, delete it by issuing the command "ARP -d XXX.XXX.XXX.XXX" and press Enter (XXX.XXX.XXX.XXX is the IP address of the RCP2-1000 unit). Now try the PING command again. More information about how to set up a network connection with the RCP2-1000 can be found in **Appendix B**.

5.5.3 Using the RCP2-1000 Web Interface

The RCP2-1000 web interface is designed to mimic the interface of the Compact Outdoor SSPA. Under this interface, the RCP2-1000 unit is completely transparent for the end user.

Starting with firmware version 6.00, the RCP2 web interface no longer needs to have a pre-installed Java application to operate. The web interface uses a standard hypertext transfer protocol on port 80. The web interface is compatible with most modern web browsers, such as Firefox, Chrome or Internet Explorer, which support asynchronous JavaScript XML transactions (aka AJAX).

To connect to RCP2 internal web page, the user must make sure Web/IPNet interface is enabled on the device and that an IP address has been assigned to the unit. Connect the unit to an Ethernet network or directly to a PC 10/100Base-T adapter and then open a web browser.

Enter the IP address of the unit into the address bar of the browser. A security login window will appear. In the User Name field, enter admin, the default User Name. See **Figure 5-12**. The User Name is fixed and cannot be changed by the operator.

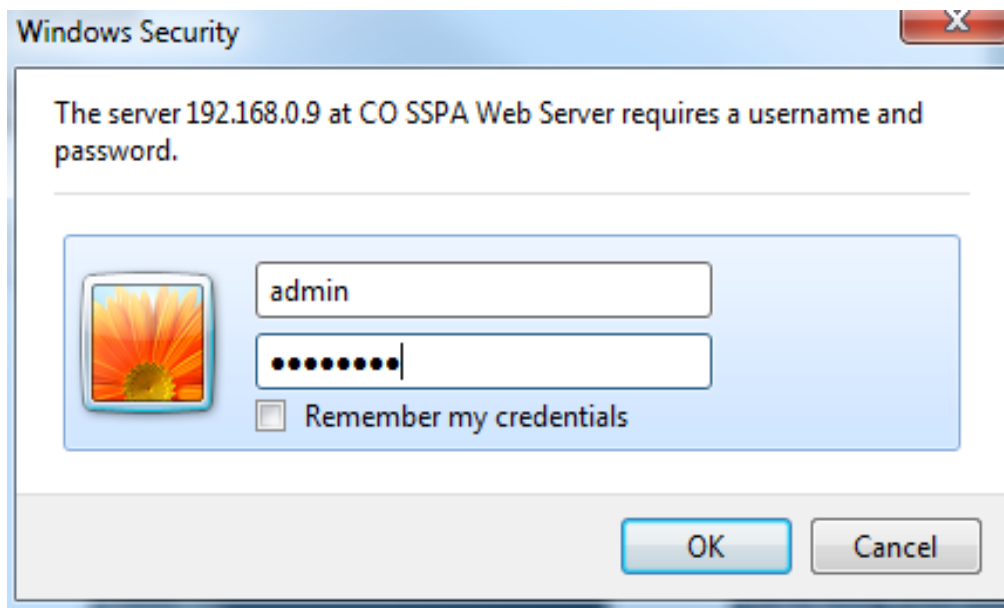


Figure 5-12: Web Interface Logon Screen

In the Password field, enter the web password assigned to the unit. The factory default password is **paradise**. The User Name and Password are case sensitive. The password may be changed at any time and may comprise up to 15 alpha-numeric characters. Click on the [Log In] button to open the M&C control in the web browser (**Figure 5-13**).

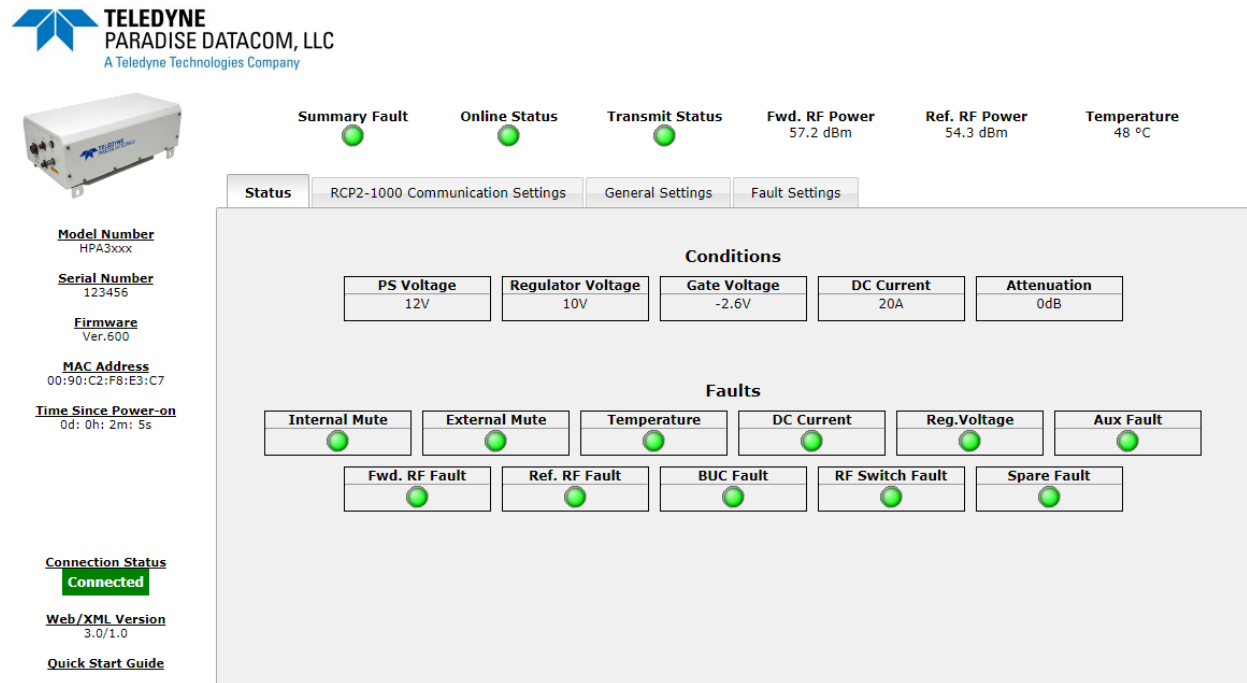


Figure 5-13: Web Interface Main Page

To select another password, enter the following selection on the RCP2-1000 front panel: Press the **Main Menu** key; select **2.Panel Com** and press the **Enter** key; select **3.IPNet** and press the **Enter** key; select **5.Ipconfig** and press the **Enter** key; select **6.More** and press the **Enter** key; select **4.WebPassword** and press the **Enter** key.

Select the appropriate password by using the navigation buttons. To erase a character, press and hold the **Up Arrow (▲)** and **Down Arrow (▼)** keys simultaneously. If no password is selected (all characters erased during password selection through the password select menu),

5.5.4 SNMP Interface

5.5.4.1 Introduction

SNMP-based management was initially targeted for TCP/IP routers and hosts. However, the SNMP-based management approach is inherently generic so that it can be used to manage many types of systems. This approach has become increasingly popular for remote management and control solutions for various SSPA systems.

Paradise Datacom devices with Ethernet interface support the most popular SNMPv1 format (SMIv1, RFC1155), SNMP Get, SNMP GetNext and SNMP Set commands. SNMP Traps are currently unsupported.

In order to utilize SNMP protocol, the user has to enable this feature through the front panel or by remote serial protocol. SNMP uses the UDP fixed port 161 for sending and receiving requests.

The definition of managed objects described in MIB. The MIB file is available for download from the Software Downloads section of the Paradise Datacom web site, <http://www.paradisedata.com>.

As with the serial protocol, the RCP2-1000 MIB allows access to a remote Compact Outdoor SSPA (default state) as well as to the RCP2-1000 unit itself. To switch between those devices' MIBs, the proper Device Type has to be selected (OID - 1.3.6.1.4.1.20712.1.4).

The Teledyne Paradise Datacom MIB is a table-based MIB, and is the same for all devices. The MIB table is designed to follow the same pattern as the tables for serial protocol. For additional information about OID values, refer to **Table 7-11** through **Table 7-13**. The text values in the tables help automatic value parsing within NMS or make the values readable through an MIB browser. All text value OIDs follow the same pattern:

1. For settings or parameters with discreet values:
SettingName'ValueName1=xxx, ...,ValueNamex=xxx
Example: ControlMode'Local=0,Remote=1
2. For settings or parameters with continuous values:
SettingName'LowLimit..HighLimit
Example: NetworkAddress'0..255

5.5.4.2 SNMP V3 Issues in Teledyne Paradise Datacom RCP2 Controller

Simple Network Management Protocol (SNMP) is an interoperable standards-based protocol that allows for external monitoring of the Content Engine through an SNMP agent.

A SNMP-managed network consists of three primary components: managed devices, agents, and management systems. A managed device is a network node that contains a SNMP agent and resides on a managed network. Managed devices collect and store management information and use SNMP to make this information available to management systems that use SNMP. Managed devices include routers, servers, switches, bridges hubs, computer hosts, and printers.

An agent is a software module that has local knowledge of management information and translates that information into a form compatible with SNMP: the Management Information Base (MIB). The agent can send traps, or notification of certain events, to the manager. Essentially, a Teledyne Paradise Datacom SSPA is considered a “SNMP agent”.

A manager is a software module that listens to the SNMP notifications sent by SNMP agents. The manager can also send requests to an agent to collect remote information from the Management Information Base (MIB).

The communication between the agent and the manager uses the SNMP protocol, which is an application of the ASN.1 BER (Abstract Syntax Notation 1 with Basic Encoding Rules), typically over UDP (for IP networks).

- Version 1 (SNMPv1, described in RFC 1157) is the initial implementation of SNMP.
- Version 2 (SNMPv2c, described in RFC 1902) is the second release of SNMP. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3, described in RFC 2271 through RFC 2275) is the most recent version of SNMP.

SNMP V1

SNMP version 1 is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de-facto network-management protocol in the Internet community. The Teledyne Paradise Datacom RCP2 family of products utilizes the most popular implementation, SNMP V1 over UDP transport layer.

SNMP V2

SNMPv2 (RFC 1441–RFC 1452) revises version 1 and includes some improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced GetBulkRequest, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.

The format of the trap message was also changed in SNMPv2. To avoid these compatibility issues, the trap mechanism was not implemented in the Teledyne Paradise Datacom SSPA MIB.

SNMP V3

Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology. SNMPv3 primarily added security and remote configuration enhancements to SNMP. Many embedded controllers and microprocessors that are used in electronic components such as amplifier modules do not have support for SNMP V2 or V3. This is due to the extensive memory resources required by the computation intensive cryptographic security of SNMP V3.

For this reason V3 has not gained widespread support amongst embedded MCU platform manufacturers. Existing port implementations are limited to very powerful ARM5 or above cores, running under full-scale OS systems (Linux, Android, etc.). At large, these configurations require external bulk RAM/FLASH to operate. This requirement ultimately affects the minimum device startup time (tens of seconds, due to the large boot BIOS) and working temperature range (mostly indoor).

As noted in Cisco's release notes about SNMP V3:

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Therefore, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received, or the request times out. Traps are sent only once, while an inform can be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

(<http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html>, last visited on 22 January 2015.)

5.5.4.3 SNMP MIB Tree

```
--paradiseDatacom(1.3.6.1.4.1.20712)
|
|--deviceINFO(1)
| |
| |-- r-n OctetString deviceId(1)
| |-- rwn OctetString deviceLocation(2)
| |-- r-n OctetString deviceRevision(3)
| |-- r-n Enumeration deviceType(4)
|
|--devices(2)
|
| |--paradiseDevice(1)
| |
| | |--settings(1)
| | |
| | | |--settingsEntry(1) [settingIndex]
| | | |
| | | | |-- rwn Integer32 settingIndex(1)
| | | | |-- rwn Integer32 settingValue(2)
| | | | |-- r-n OctetString settingTextValue(3)
| | |
| | |--thresholds(2)
| | |
| | | |--thresholdsEntry(1) [thresholdIndex]
| | | |
| | | | |-- rwn Integer32 thresholdIndex(1)
| | | | |-- r-n Integer32 thresholdValue(2)
| | | | |-- r-n Enumeration thresholdStatus(3)
| | | | |-- r-n OctetString thresholdText(4)
| | |
| | |--conditions(3)
| | |
| | | |--conditionsEntry(1) [conditionsIndex]
| | | |
| | | | |-- rwn Integer32 conditionsIndex(1)
| | | | |-- r-n Integer32 conditionsValue(2)
| | | | |-- r-n Counter conditionsEventCount(3)
| | | | |-- r-n OctetString conditionsText(4)
| | |
| |--paradiseDeviceA(2)
|
| |--paradiseDeviceB(3)
|
| |--paradiseDeviceC(4)
|
|--modem(5)
```

5.5.4.4 Description of MIB Entities

deviceINFO

This field includes general device information.

deviceID

Octet string type; maximum length -60; field specifies device model and serial number; read only access; OID -1.3.6.1.4.1.20712.1.1

deviceLocation

Octet string type; maximum length 60; field allow customer to store information about device physical location or any other textual information related to the device; read/write access; OID -1.3.6.1.4.1.20712.1.2

deviceRevision

Octet string type; maximum length 60; field specifies device firmware revision; read only access; OID -1.3.6.1.4.1.20712.1.3

deviceType

Enumeration, integer type; field allows simple detection of SNMP device type. Values: rmsspa(1), cossipa(2), rcp2fprc(3), rcp21000co(4), rcp21000rm(5), rcp21000rcp(6), buc(7); read/write access. The High Power Outdoor SSPA also utilizes device type 2 (cossipa). Switching devicetype between cossipa and rcp21000co will change the settings table content. Setting the ID to any other value will default type to cossipa. OID -1.3.6.1.4.1.20712.1.4

devices

This field is subdivided into 5 branches: paradiseDevice, paradiseDeviceA, paradiseDeviceB, paradiseDeviceC and modem. paradiseDevice branch currently is used for all Paradise Datacom LLC SNMP enabled device except Modem. See the Evolution Modem manual for specific MIB information. Branches for Device A, B and C are reserved for future use.

paradiseDevice

Field contents tables hold specific device information: Settings, Thresholds and Conditions. All table formats follow a common pattern: Index, Value, TextValue. The threshold table has an additional column for parameter validation. The conditions table has an extra column for event counters.

The Index column provides general table indexing; the Value column presents the current value of the relevant parameter; the TextValue column provides information about parameter name, measurement units and limits.

Value "1" in the validation column of the thresholds table indicates that relevant parameter is valid under the current system configuration; value "2" indicates that parameter is invalid or "Not available".

The event counter column of the conditions table indicates how many times a value of a relevant parameter changed its state since system power-up.

settings

Table contains current device configuration and provides device management. For detailed settings table info for SNMP device, see **Table 5-17** if deviceType is set to cospa (note that only the first 20 values of this table are valid); and see **Table 5-18** if deviceType is set to rcp21000co. Read/write access for settings-Value column.

thresholds

Table provides information about device internal limits and subsystems info. For detailed threshold table information, refer to **Table 5-19**. Read only access.

conditions

Table contents device fault status information. For detailed conditions table info, refer to **Table 5-20** if deviceType is set to cospa; ; and see **Table 5-21** if deviceType is set to rcp21000co. Read only access.

Table 5-17: Detailed Settings for CO SSPA mode (Device Type=2)

settingIndex/settingValue	settingTextValue	Value OID	Description
1/INTEGER	SystemMode'1:1=0,Dual'1:1 = 1,StandAlone=255	1.3.6.1.4.1.20712.2.1.1.1.2.1	System Operation mode
2/INTEGER	SystemHierarchicalAddress'HPA1=0,HPA2=255	1.3.6.1.4.1.20712.2.1.1.1.2.2	System Hierarchical Address
3/INTEGER	CurrentState'UnitStandby=0,UnitOnline=255	1.3.6.1.4.1.20712.2.1.1.1.2.3	Unit Start Up State in Redundancy
4/INTEGER	MuteOn=0,Off=255	1.3.6.1.4.1.20712.2.1.1.1.2.4	Mute State
5/INTEGER	SSPAAttenuation(dBx10)'0..200	1.3.6.1.4.1.20712.2.1.1.1.2.5	Attenuation Level
6/INTEGER	GainControl'Analog=0,Serial=255	1.3.6.1.4.1.20712.2.1.1.1.2.6	Module Gain Control Authority
7/INTEGER	NetworkAddress'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.7	Amplifier Network Address
8/INTEGER	HighTempAlarmThreshold(C)'0..100	1.3.6.1.4.1.20712.2.1.1.1.2.8	High Temperature Alarm Threshold
9/INTEGER	CalibrationMode'On=0,Off=255	1.3.6.1.4.1.20712.2.1.1.1.2.9	SSPA module Calibration Mode
10/INTEGER	SpareFaultCheck'ADCC'0-7=0..7,Ext.Mute=8,Ignore=255	1.3.6.1.4.1.20712.2.1.1.1.2.10	SSPA Spare Fault Status
11/INTEGER	SpareFaultAction'MajorFault=0,Fault+Mute=1,MinorFault=255	1.3.6.1.4.1.20712.2.1.1.1.2.11	SSPA Spare Fault Handling
12/INTEGER	AuxFaultCheck'LogicHigh=0,LogicLow=1,Ignore=255	1.3.6.1.4.1.20712.2.1.1.1.2.12	SSPA Auxiliary Fault Status
13/INTEGER	AuxFaultAction'MajorFault=0,Fault+Mute=1,MinorFault=255	1.3.6.1.4.1.20712.2.1.1.1.2.13	SSPA Auxiliary Fault Handling
14/INTEGER	BUCFaultCheck'LogicHigh=0,LogicLow=1,Ignore=255	1.3.6.1.4.1.20712.2.1.1.1.2.14	Block Up Converter Fault Status
15/INTEGER	BUCFaultAction'MajorFault=0,Fault+Mute=1,MinorFault=255	1.3.6.1.4.1.20712.2.1.1.1.2.15	Block Up Converter Fault Handling
16/INTEGER	ProtocolSelect'Terminal=0,Compatible25pin=1,Normal=255	1.3.6.1.4.1.20712.2.1.1.1.2.16	Protocol Select
17/INTEGER	BaudRate'38400=255,19200=1,4800=2,2400=3,9600=255	1.3.6.1.4.1.20712.2.1.1.1.2.17	Baud Rate Select
18/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.18	Field reserved for factory use
19/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.19	Field reserved for factory use
20/INTEGER	StandbyMode'ColdStandby=0,HotStandby=255	1.3.6.1.4.1.20712.2.1.1.1.2.20	Standby Mode
21/INTEGER	BUCReference'Autoswitch = 0,External = 1,Internal = 2,NA=255	1.3.6.1.4.1.20712.2.1.1.1.2.21	Field reserved for factory use
22/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.22	Field reserved for factory use
23/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.23	Field reserved for factory use
24/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.24	Field reserved for future use
25/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.25	Field reserved for future use
26/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.26	Field reserved for future use
27/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.27	Field reserved for future use
28/INTEGER	Reserved'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.28	Field reserved for future use

Table 5-17: Detailed Settings (continued from previous page)

setting Index/ settingValue	settingTextValue	Value OID	Description
29/INTEGER	IPAddress-Byte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.29	Device IP address byte1 (MSB)
30/INTEGER	IPAddress-Byte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.30	Device IP address byte2
31/INTEGER	IPAddress-Byte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.31	Device IP address byte3
32/INTEGER	IPAddress-Byte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.32	Device IP address byte4 (LSB)
33/INTEGER	IPGate-WayByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.33	Device Gateway address byte1 (MSB)
34/INTEGER	IPGate-WayByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.34	Device Gateway address byte2
35/INTEGER	IPGate-WayByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.35	Device Gateway address byte3
36/INTEGER	IPGate-WayByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.36	Device Gateway address byte4 (LSB)
37/INTEGER	IPSubnet-Byte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.37	Device Subnet Mask byte1 (MSB)
38/INTEGER	IPSubnet-Byte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.38	Device Subnet Mask byte2
39/INTEGER	IPSubnet-Byte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.39	Device Subnet Mask byte3
40/INTEGER	IPSubnet-Byte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.40	Device Subnet Mask byte4 (LSB)
41/INTEGER	IPPortByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.41	Device Port address byte1 (MSB) (required only for IPNet Interface)
42/INTEGER	IPPortByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.42	Device Port address byte2 (LSB) (required only for IPNet Interface)
43/INTEGER	IPLockByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.43	Device IP lock address byte1 (MSB) (required only for IPNet Interface)
44/INTEGER	IPLockByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.44	Device IP lock address byte2 (required only for IPNet Interface)
45/INTEGER	IPLockByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.45	Device IP lock address byte3 (required only for IPNet Interface)
46/INTEGER	IPLockByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.46	Device IP lock address byte4 (LSB) (required only for IPNet Interface)

Table 5-18: Detailed Settings for RCP2-1000-CO mode (Device Type=4)

settingIndex/ settingValue	setting TextValue	Value OID	Description
1/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.1	Field reserved for future use
2/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.2	Field reserved for future use
3/INTEGER	ControlMode'Local=0,Remote=1	1.3.6.1.4.1.20712.2.1.1.1.2.3	Control Mode
4/INTEGER	VFDLite'Off=0,Low=1,Med=2,High=3	1.3.6.1.4.1.20712.2.1.1.1.2.4	VFD back light intensity
5/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.5	Field reserved for future use
6/INTEGER	Protocol'Normal=0,Terminal=1	1.3.6.1.4.1.20712.2.1.1.1.2.6	Main serial port protocol
7/INTEGER	Baud'9600=0,2400=1,4800=2,19200=3,38400=4	1.3.6.1.4.1.20712.2.1.1.1.2.7	Main serial port baud rate
8/INTEGER	NetworkAddress'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.8	Network Address
9/INTEGER	Interface'RS232=0,RS485=1,IPNet=2,SNMP=3	1.3.6.1.4.1.20712.2.1.1.1.2.9	Type of remote control interface
10/INTEGER	FiberLink'Off=0,On=1	1.3.6.1.4.1.20712.2.1.1.1.2.10	Fiberlink interface
11/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.11	Field reserved for future use
12/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.12	Field reserved for future use
13/INTEGER	FaultLatch'Disable=0,Enable=1	1.3.6.1.4.1.20712.2.1.1.1.2.13	Fault Latch
14/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.14	Field reserved for future use
15/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.15	Field reserved for future use
16/INTEGER	UserPassword'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.16	Menu Password
17/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.17	Field reserved for future use
18/INTEGER	Buzzer'Off=0,On=1	1.3.6.1.4.1.20712.2.1.1.1.2.18	Audible Alarm Buzzer
19/INTEGER	SystemPassword'Off=0,On=1	1.3.6.1.4.1.20712.2.1.1.1.2.19	Menu Password Protection
20/INTEGER	RFUnits'dBm=0,Watts=1	1.3.6.1.4.1.20712.2.1.1.1.2.20	RF Units (VFD Menu only)
21/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.21	Field reserved for factory use
22/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.22	Field reserved for factory use
23/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.23	Field reserved for factory use
24/INTEGER	LowFwdRFFHtHandle'Ignore=0,Major=1,Minor=2	1.3.6.1.4.1.20712.2.1.1.1.2.24	Low Forward RF (RCP2-1000 only)
25/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.25	Field reserved for future use
26/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.26	Field reserved for future use
27/INTEGER	LowForwardRFthreshold(dBm)'0..'80	1.3.6.1.4.1.20712.2.1.1.1.2.27	Low Fwd. RF threshold (RCP2-1000 only)
28/INTEGER	Reserved'0..'255	1.3.6.1.4.1.20712.2.1.1.1.2.28	Field reserved for future use

Table 5-18: Detailed Settings (continued from previous page)

settingIndex/ settingValue	settingTextValue	Value OID	Description
29/INTEGER	IPAddressByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.29	Device IP address byte1 (MSB)
30/INTEGER	IPAddressByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.30	Device IP address byte2
31/INTEGER	IPAddressByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.31	Device IP address byte3
32/INTEGER	IPAddressByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.32	Device IP address byte4 (LSB)
33/INTEGER	IPGateWayByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.33	Device Gateway address byte1 (MSB)
34/INTEGER	IPGateWayByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.34	Device Gateway address byte2
35/INTEGER	IPGateWayByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.35	Device Gateway address byte3
36/INTEGER	IPGateWayByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.36	Device Gateway address byte4 (LSB)
37/INTEGER	IPSubnetByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.37	Device Subnet Mask byte1 (MSB)
38/INTEGER	IPSubnetByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.38	Device Subnet Mask byte2
39/INTEGER	IPSubnetByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.39	Device Subnet Mask byte3
40/INTEGER	IPSubnetByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.40	Device Subnet Mask byte4 (LSB)
41/INTEGER	IPPortByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.41	Device Port address byte1 (MSB) (required only for IPNet Interface)
42/INTEGER	IPPortByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.42	Device Port address byte2 (LSB) (required only for IPNet Interface)
43/INTEGER	IPLockByte1'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.43	Device IP lock address byte1 (MSB) (required only for IPNet Interface)
44/INTEGER	IPLockByte2'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.44	Device IP lock address byte2 (required only for IPNet Interface)
45/INTEGER	IPLockByte3'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.45	Device IP lock address byte3 (required only for IPNet Interface)
46/INTEGER	IPLockByte4'0..255	1.3.6.1.4.1.20712.2.1.1.1.2.46	Device IP lock address byte4 (LSB) (required only for IPNet Interface)

Table 5-19: Detailed Thresholds (common for all Device Types)

thresholdIndex/ thresholdValue	thresholdTextValue	Value OID	Description
1/INTEGER	LowCurrentThreshold'0..1023	1.3.6.1.4.1.20712.2.1.2.1.2.1	Low Current Threshold
2/INTEGER	SpareFaultLowLimitThreshold'0..1023	1.3.6.1.4.1.20712.2.1.2.1.2.2	Spare Fault Low Limit Threshold
3/INTEGER	SpareFaultHighLimitThreshold'0..1023	1.3.6.1.4.1.20712.2.1.2.1.2.3	Spare Fault High Limit Threshold

Table 5-20: Detailed Conditions for CO SSPA mode (Device Type = 2)

conditionIndex/ conditionValue	conditionTextValue	Value OID	Description
1/INTEGER	DACCount'0..1023	1.3.6.1.4.1.20712.2.1.3.1.2.1	Tempcomp DAC control output
2/INTEGER	SSPACoreTemperature(C)'-100..100	1.3.6.1.4.1.20712.2.1.3.1.2.2	SSPA core temperature
3/INTEGER	FaultStateAgregateValue'0-65535	1.3.6.1.4.1.20712.2.1.3.1.2.3	Aggregate Fault State of SSPA
4/INTEGER	SSPAAgregateAttenuation(dBx10)'0..200	1.3.6.1.4.1.20712.2.1.3.1.2.4	Current SSPA Attenuation Level
5/INTEGER	ForwardRFPower(dBmx10)'0..800	1.3.6.1.4.1.20712.2.1.3.1.2.5	Forward RF Forward output (dBm)
6/INTEGER	SSPADCCurrent(Ampx10)'0..10000	1.3.6.1.4.1.20712.2.1.3.1.2.6	SSPA DC current consumption
7/INTEGER	RegulatorVoltage(Voltx10)'0..600	1.3.6.1.4.1.20712.2.1.3.1.2.7	DC Regulator Output Voltage
8/INTEGER	PSVoltage(Voltx10)'0..600	1.3.6.1.4.1.20712.2.1.3.1.2.8	Main Power Supply Voltage
9/INTEGER	GASFETGateVoltage(Voltx10)'0..200	1.3.6.1.4.1.20712.2.1.3.1.2.9	RF FET Bias Gate voltage

Table 5-21: Detailed Conditions for RCP2-1000-CO mode (Device Type=4)

conditionIndex/ conditionValue	conditionTextValue	Value OID	Description
1/INTEGER	DACCount'0..1023	1.3.6.1.4.1.20712.2.1.3.1.2.1	DAC control output
2/INTEGER	SSPACoreTemperature(C)'-100..100	1.3.6.1.4.1.20712.2.1.3.1.2.2	SSPA core temperature
3/INTEGER	FaultStateAgregateValue'0-65535	1.3.6.1.4.1.20712.2.1.3.1.2.3	Aggregate Fault State of SSPA
4/INTEGER	SSPAAgregateAttenuation(dBx10)'0..200	1.3.6.1.4.1.20712.2.1.3.1.2.4	Current SSPA Attenuation Level
5/INTEGER	ForwardRFPower(dBmx10)'0..800	1.3.6.1.4.1.20712.2.1.3.1.2.5	Forward RF Forward output (dBm)
6/INTEGER	SSPADCCurrent(Ampx10)'0..10000	1.3.6.1.4.1.20712.2.1.3.1.2.6	SSPA DC current consumption
7/INTEGER	RegulatorVoltage(Voltx10)'0..600	1.3.6.1.4.1.20712.2.1.3.1.2.7	Power Supply Regulator Output Voltage
8/INTEGER	PSVoltage(Voltx10)'0..600	1.3.6.1.4.1.20712.2.1.3.1.2.8	Power Supply Voltage
9/INTEGER	GASFETGateVoltage(Voltx10)'0..200	1.3.6.1.4.1.20712.2.1.3.1.2.9	RF FET Bias Gate voltage

5.5.5 Extended SNMP Operation

The RCP2 controller is equipped with a DigitalCore5 control board and utilizes firmware version 6.00 and above. These units feature an extended SNMP MIB and support SNMP traps. This extended MIB covers several OID objects related to SNMP trap functions.

These units allow independent functioning of two SNMP traps (asynchronous notifications): Fault trap and Conditions trap. Both traps can be enabled or disabled by the operator. The operator can also specify how many times the same trap notification will be sent back to the SNMP manager.

The SNMP manager IP address is also selectable by the operator. This IP address must be specified in the relevant OID branch. Every trap message is marked by the fixed trap community string “trap”. This community name is not user selectable.

The Fault trap allows asynchronous notification of the RCP2 fault state change. When enabled, trap notification will be sent to a manager every time either the summary fault state or a fault type is changed. The Last Fault Time ticks counter will be reset each time the summary fault changes its state to “Alarm” or when a new fault condition is detected. This counter also resets itself during device power-up. If no faults are present after device power-up, Fault Trap will issue a “Cold Start” notification to the manager.

The Condition Trap allows the unit to generate asynchronous notifications independent from the unit fault state. Currently, the following conditions can be used for this trap triggering: Forward RF Level (each remotely controlled HPA or System RF level can be selected), Reflected RF Level (for remote systems equipped with a Reflected RF sensor), DC Current level (each remotely controlled HPA can be selected), PS Voltage level (both internal PS units can be selected), Temperature (each remotely control HPA can be selected or Ambient temperature sensor if equipped), LNA/LNB current. To enable this trap, set the Condition Trap Resend option to a non-zero value and determine the upper and lower limits for the condition window. Window values must be selected according to the relevant selected condition measured by the unit. For example: Temperature must be selected in degrees, RF power in tenth of dBms, etc. After successful configuration, the RCP2 will generate a notification every time the selected condition is outside the selected measurement window. For units with multiple measured parameters, the relevant condition location must be selected (i.e., units with two power supplies use 1 for PS1, and 2 for PS2). For other conditions, this value is “don’t care”. Both traps will send a “Device Up Time” time stamp with every trap notification.

5.5.5.1 Extended SNMP MIB Tree

```
--paradiseDatacom(1.3.6.1.4.1.20712)
|
|--deviceINFO((1.3.6.1.4.1.20712.1)
||
|+-- r-n OctetString deviceId(1.3.6.1.4.1.20712.1.1)
|+-- r-wn OctetString deviceLocation(1.3.6.1.4.1.20712.1.2)
|+-- r-n OctetString deviceRevision(1.3.6.1.4.1.20712.1.3)
|+-- r-n Enumeration deviceType(1.3.6.1.4.1.20712.1.4)
|+--deviceTimeTicks(1.3.6.1.4.1.20712.1.5)
||
|+-- r-n TimeTicks deviceUpTime(1.3.6.1.4.1.20712.1.5.1)
|+-- r-n TimeTicks deviceFaultTime(1.3.6.1.4.1.20712.1.5.2)
|
|--deviceCounters(1.3.6.1.4.1.20712.1.6)
||
|+-- r-n Counter deviceSFaultCounter(1)
|
|--deviceFaultState(1.3.6.1.4.1.20712.1.7)
||
|+-- r-n Enumeration deviceSummaryFault(1)
|+-- r-n Enumeration deviceLastFault(2)
|
|--deviceTrapedCondition(1.3.6.1.4.1.20712.1.8)
||
|+-- r-n Integer32 deviceTrappedConditionValue(1)
|
|--deviceTrapControl(1.3.6.1.4.1.20712.1.9)
||
|+-- r-wn IpAddress deviceManagerIP(1)
|+-- r-wn Integer32 deviceFaultsTrapResend(2)
|+-- r-wn Integer32 deviceConditionTrapResend(3)
|+-- r-wn Enumeration deviceConditionToMonitor(4)
|+-- r-wn Integer32 deviceConditionULimit(5)
|+-- r-wn Integer32 deviceConditionLLimit(6)
|+-- r-wn Integer32 deviceConditionLocation(7)
|
|--deviceTraps(1.3.6.1.4.1.20712.1.10)
|
|+-- (1.3.6.1.4.1.20712.1.10.0)
|
|+--deviceFaultsTrap(1.3.6.1.4.1.20712.1.10.0.11)
|[deviceUpTime,deviceSummaryFault,deviceLastFault]
|
|+--deviceConditionTrap(1.3.6.1.4.1.20712.1.10.0.12)
```

```
|
|--devices(2)
|
|--paradiseDevice(1)
|
|
|--settings(1)
|
|
|--settingsEntry(1) [settingIndex]
|
|
|-- rwn Integer32 settingIndex(1)
|-- rwn Integer32 settingValue(2)
|-- r-n OctetString settingTextValue(3)
|
|--thresholds(2)
|
|
|--thresholdsEntry(1) [thresholdIndex]
|
|
|-- rwn Integer32 thresholdIndex(1)
|-- r-n Integer32 thresholdValue(2)
|-- r-n Enumeration thresholdStatus(3)
|-- r-n OctetString thresholdText(4)
|
|--conditions(3)
|
|--conditionsEntry(1) [conditionsIndex]
|
|-- rwn Integer32 conditionsIndex(1)
|-- r-n Integer32 conditionsValue(2)
|-- r-n Counter conditionsEventCount(3)
|-- r-n OctetString conditionsText(4)
|
|--paradiseDeviceA(2)
|
|--paradiseDeviceB(3)
|
|--paradiseDeviceC(4)
|
|--modem(5)
```

5.5.5.2 Extended SNMP MIB Tree Elements in Detail

deviceRevision — Octet string type; maximum length 60; field specifies device firmware revision; read only access; OID -1.3.6.1.4.1.20712.1.3

deviceUpTime — Device total up time in hundredths of a second;

deviceFaultTime — Time elapsed since deviceLastFault last state change in hundredths of second;

deviceSFaultCounter — Counts number of Summary alarms since device power up;

deviceSummaryFault — Enumerated value of device last detected fault condition. The following enumerated values are possible: coldStart(1), overTemp(2), badRegltr(3), lowDCCur(4), aux(5), buc(6), lna(7), hpa(8), lowFwdRF(9), highRefRF(10), nPlusOne (11), badPS(12), timeOut(13), other(14), noFaults(15);

deviceTrappedConditionValue — Condition value trapped by deviceConditionTrap;

deviceManagerIP — Trap recipient IP address;

deviceFaultsTrapResend — Defines how many times deviceFaultsTrap will repeat the message. 0 - Disables trap triggering;

deviceConditionTrapResend — Defines how many times condition trap will repeat the message. 0 - Disables trap triggering

deviceConditionToMonitor — Enumerated value. Object defines which condition to trap. The following enumerations are possible: fwdRF(1), dcCurrent(2), voltagePS(3), temperature(4), lnaCur(5), refRF(6);

deviceConditionULimit — Conditions upper trap limit. Trap will be sent when the condition exceeds this limit.

deviceConditionLLimit — Conditions lower trap limit. Trap will be sent when condition falls below this limit.

deviceConditionLocation — Parameter specifying condition measuring location in device containing multiple location of the same type (multiple PS, HPAs, LNAs etc.). Set to 0 for system-wide conditions, 1, ... n for relevant unit. For devices with single condition location parameter is “don’t care”, for system wide parameters (System RF power, Ambient temperature etc. select 4).

deviceFaultsTrap — Trap fires deviceFaultsTrapResend times when deviceLastFault or deviceSummaryFault state changes.

5.5.5.3 Configuring RCP2-1000 Unit to Work with SNMP Protocol

1. Set up the unit IP address. Select the following sequence from the SSPA Main Menu: Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key; select **5.IP Setup** and press the **Enter** key; select **2.LocalIP** and press the **Enter** key. Use the navigation keys to adjust the unit IP address. Press the **Enter** key when complete;
2. Set up the unit gateway address. Select the following sequence from the SSPA Main Menu: Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key; select **5.IP Setup** and press the **Enter** key; select **4.Gateway** and press the **Enter** key. Use the navigation keys to adjust the unit gateway address. If no gateway is needed, set the address to 0.0.0.0. Press the **Enter** key when complete;
3. Set up the unit subnet mask. Select the following sequence from the SSPA Main Menu: Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key; select **5.IP Setup** and press the **Enter** key; select **3.Subnet** and press the **Enter** key. Use the navigation keys to adjust the unit subnet mask. Press the **Enter** key when complete;
4. Set up the unit Community Set and Get strings. Select the following sequence from the SSPA Main Menu: Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key; select **5.IP Setup** and press the **Enter** key; select **6.More** and press the **Enter** key; select **1.CommunitySet** (or **2.CommunityGet**) and press the **Enter** key. Use the navigation keys to adjust the unit community strings information. Press the **Right Arrow** (▶) or **Left Arrow** (◀) key to move the cursor to the next or previous character in the string. Press and hold the **Up Arrow** (▲) or **Down Arrow** (▼) key to scroll through the alpha-numeric characters at the position of the cursor. Press the **Enter** key when complete. Press and hold the **Down Arrow** (▼) key and then press **Up Arrow** (▲) key to erase unwanted characters;
5. Set up the unit interface to SNMP. Select the following sequence from the SSPA Main Menu: Press the **Main Menu** key; select **2.PanelCom** and press the **Enter** key; select **4.Interface** and press the **Enter** key; select **4.SNMP** and press the **Enter** key. Restart the unit by cycling power or by selecting the Reset option from the front panel menu.
6. SNMP protocol now is set and ready to be used.

5.5.5.4 Connecting to a MIB Browser

For a MIB browser application example, we will be using the freeware browser Getif, version 2.3.1. There are many other browsers available for download from <http://www.snmplink.org/Tools.html>.

1. Copy the provided MIB file into the Getif Mibs subfolder.
2. Start the Getif application.
3. Select the unit IP address and community strings in the relevant text boxes on the Parameters tab (see **Figure 5-14**) and then click the Start button.

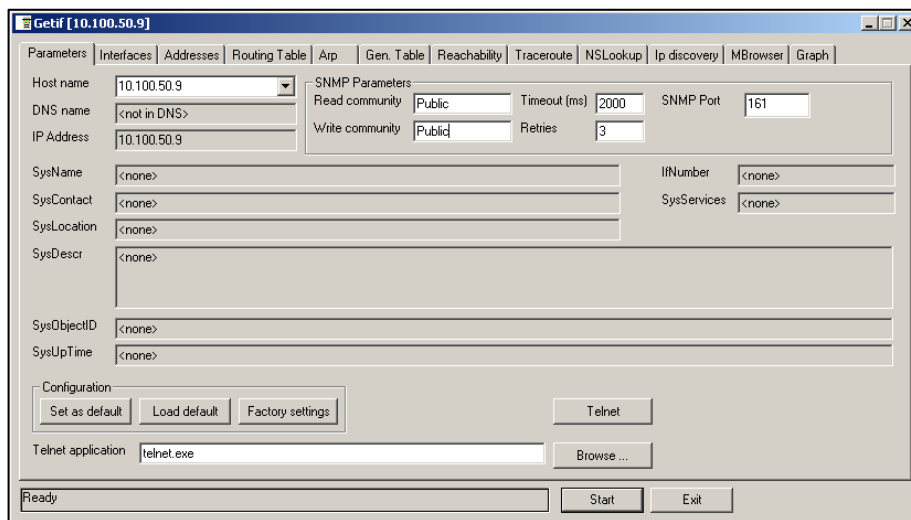


Figure 5-14: GetIF Application Parameters Tab

4. Select the MIBBrowser tab.
5. Click on 'iso main entity' on the MIB tree, then click the Start button.
6. See update data in output data box (**Figure 5-15**).

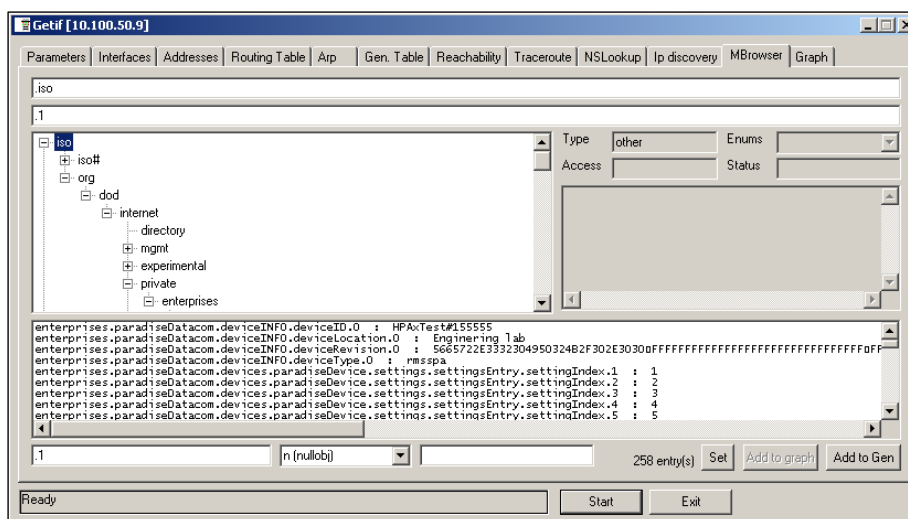


Figure 5-15: Getif MBrowser window, with update data in output data box

5.6 Firmware Programming

Teledyne Paradise Datacom's digital engineers continually strive to improve the performance of RCP2 software and firmware. As this occurs, software and firmware upgrades are made available.

The DigiCore5 controller board allows two methods for upgrading the unit firmware:

- Upgrade over HTTP link by using web browser;
- Over programming USB connector J1;

The web upgrade is performed over the RCP2 IP port and does not require any special software. It can be performed through any suitable web browser.

Upgrade over the USB port requires the installation of specific hardware USB drivers and batch scripts.

5.6.1 Required Hardware

The following equipment/hardware is necessary to perform the firmware upgrade.

- Depending on type of upgrade: Win7/XP PC with USB port or PC with available 10/100 Base-T port;
- Mini USB cable or Ethernet patch cable;

5.6.2 Required Software

For web upgrade:

- Web browser (IE, Chrome or Firefox);

For USB upgrade:

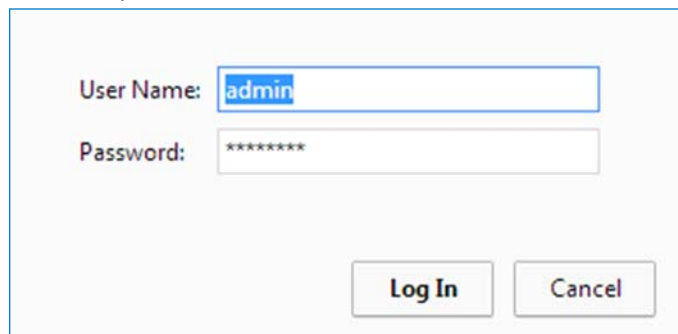
- USB FTDI VCP drivers. Drivers need to be installed before making a connection between the PC and the SSPA USB programming port. Visit the FTDI web page (<http://www.ftdichip.com/Drivers/VCP.htm>) for the latest set of virtual COM port (VCP) drivers.
- RCP2 field programming utility. Contact Teledyne Paradise Datacom technical support to obtain the latest version. The Field Programming utility is typically not required for installation.
- Firmware image upgrade file: code.bin.

5.6.3 Web Upgrade Procedure

The web upgrade is the preferred method of upgrading the firmware.

Upgrading unit with incompatible firmware image may damage the equipment hardware. To ensure the proper firmware image file is used, contact Teledyne Paradise Datacom technical support. Write down your current firmware version. You may want also request image file of the current firmware in case it becomes necessary to revert back to the original.

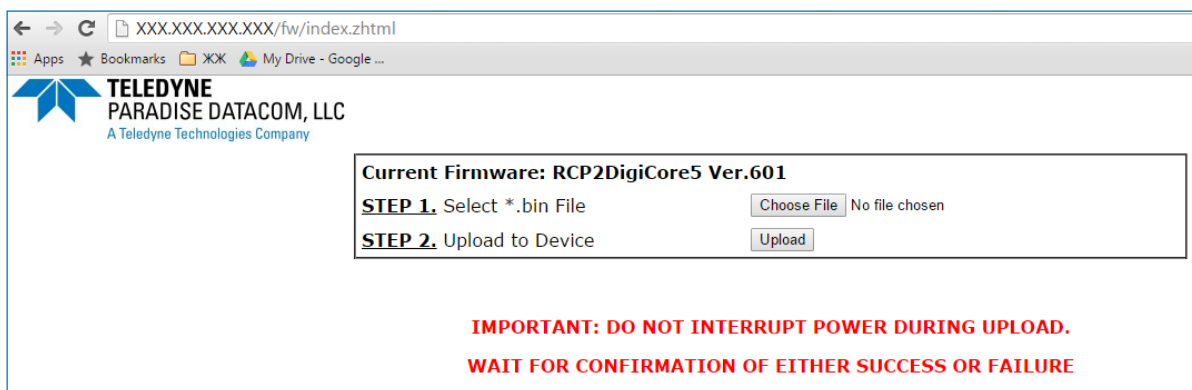
1. Connect the unit to a 10/100 Base-T network or to a PC 10/100 Base-T network adapter. See **Appendix A**.
2. Open a web browser window (Chrome, Firefox or IE are preferred). Enter the following address in the location window of the browser:
XXX.XXX.XXX.XXX/fw/
where XXX.XXX.XXX.XXX is the IPv4 address of the unit. Press Enter.
3. The Upload Form is password protected. An authentication window should come up to ensure authorization. Use “admin” as user name and the web logon password (default password is “paradise”). Click the “Log in” button (see **Figure 5-16**).



A screenshot of a web browser's authentication window. It features two input fields: "User Name:" with the text "admin" entered, and "Password:" with seven asterisks. Below the fields are two buttons: "Log In" and "Cancel".

Figure 5-16: Web Upgrade Authentication Window

4. The firmware upload form will load in the browser window (See **Figure 5-17**). Click the “Choose File” button and select the firmware image code.bin file provided by technical support.



A screenshot of a web browser displaying the firmware upload form. The browser's address bar shows "XXX.XXX.XXX.XXX/fw/index.shtml". The page header includes the Teledyne Paradise Datacom, LLC logo and name. The main content area displays "Current Firmware: RCP2DigiCore5 Ver.601". Below this, there are two steps: "STEP 1. Select *.bin File" with a "Choose File" button and "No file chosen" text, and "STEP 2. Upload to Device" with an "Upload" button. At the bottom, a red warning message reads: "IMPORTANT: DO NOT INTERRUPT POWER DURING UPLOAD. WAIT FOR CONFIRMATION OF EITHER SUCCESS OR FAILURE".

Figure 5-17: Firmware Upload Form

-
- Click the “Upload” button. A warning message will appear; click the “OK” button (See **Figure 5-18**).

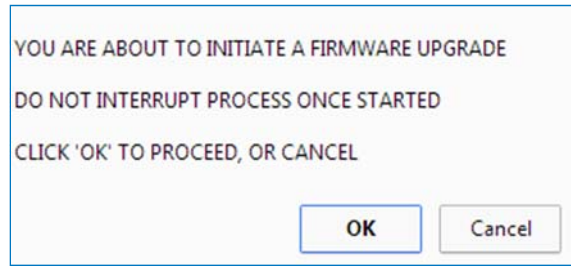


Figure 5-18: Proceed With Upgrade Prompt

- The upload process will begin and the form will be informing about loading process (See **Figure 5-19**). Do not interrupt this process and wait until its completion with positive or negative result. The process may take up to 15 minutes. When completed, the form will notify about end of process. See **Figure 5-20**.

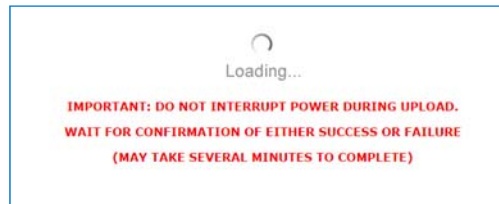


Figure 5-19: Upload Process Message

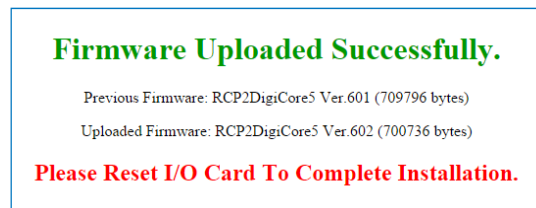


Figure 5-20: Upload Completed Message

- During the upgrade process, the unit remains fully functional. The new firmware will stay dormant until the next reboot of the control card. Reboot the controller card by selecting the relevant front panel menu or by cycling power to the unit. Browse to the front panel menu firmware information page and verify the installed version.
- If the load process was interrupted, for any reason, the unit may not operate properly after a reboot. It is still possible to recover from the problem by applying firmware upload over USB port. See **Section 5.6.4** for details.

5.6.4 USB Port Upgrade Procedure

1. Contact Teledyne Paradise Datacom support to obtain the latest firmware image and field programming utility. The programming utility package includes an RFU upload utility, a script file and FTDI USB drivers. Use the USB upgrade method only if the web upgrade has failed!
2. Install FTDI VCP driver on the target PC;
3. Connect the USB mini port J1 at the back of unit to an available PC USB port. Warning! Connecting J1 to a PC USB will interrupt normal operation of the unit.
4. After connecting the unit, the target PC should recognize the newly connected hardware and connect to it using the previously installed VCP FTDI drivers. Wait until this process is complete. Check the Windows device manager Ports section and note the newly added USB Serial Port (See **Figure 5-21**). You will need a COM port designator in the next step.



Figure 5-21: Windows Device Manager > Ports

5. Locate and run Upgrade.bat script file which was provided in firmware upgrade package. File will open command prompt window and request programming serial port designator. Enter port designator located in previous step and then press "Enter". The script file will start downloading a new image file to the unit. The resulting window is shown in **Figure 5-22**;

```
C:\_Projects_UB6\Firmware write>clrfu c:\_code\~code.bin -v -s 10:230400 -usb+
Rabbit Field Utility v4.62
Installing RCP2DigiCore5 v6.0.1

Sending Coldloader
363 of 704623 bytes sent
Sending Pilot BIOS
3887 of 704623 bytes sent
Erasing flash

Sending Program
704623 of 704623 bytes sent
Elapsed Time: 62.977 seconds

C:\_Projects_UB6\Firmware write>pause
Press any key to continue . . .
```

Figure 5-22: Command Window Showing Program Prompts

6. Unplug the USB cable from the control card. The unit should restart with the new firmware image.

This section describes the procedure for setting up the RCP2-1000 Ethernet IP interface through the front panel interface. It also describes basic network setup of a Windows based host PC for a peer-to-peer network connection with the RCP2-1000.

Important! Do not use a crossover cable to connect to the network hub, use crossover only for direct PC-to-RCP2-1000 connection!

1. Connect J6 Ethernet Port of the RCP2-1000 controller to a host PC through a cross-over null-modem network cable (see **Appendix B**) for wiring details.
2. If the PC NIC card has not previously been set, do so now using the following procedure, otherwise skip to Step 3.

2.1 From Windows Control Panel select Network icon;

2.2 Select TCP/IP properties of your LAN card. The window shown in **Figure B-1** will appear:



Figure A-1: TCP/IP Properties Window

2.3 Select "Specify an IP Address". And enter the following parameters in the IP address and Subnet fields:

IP Address.....:192.168.0.3
Subnet Mask.....:255.255.255.0

After you press "OK", depending on the operating system, you may need to reboot the workstation.

2.4 After optional reboot, open the Command Prompt console window and enter:

```
C:\>IPCONFIG
```

This will display the IP settings:

```
0 Ethernet Adapter:
IP Address:        192.168.0.3
Subnet Mask:       255.255.255.0
Default Gateway:
```

2.5 You can now try to Ping your PC:

In Command Prompt window enter the following:

```
C:\>ping 192.168.0.3
```

This will display:

```
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<10ms TTL=128
Reply from 192.168.0.3: bytes=32 time<10ms TTL=128
Reply from 192.168.0.3: bytes=32 time<10ms TTL=128
Reply from 192.168.0.3: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.0.3:
    Packets: Sent=4, Received=4, Lost=0 (0%loss),
    Approximate round trip times I milli-seconds:
    Minimum=0ms, Maximum=0ms, Average=0ms
```

Your network LAN card is now set up.

3. On the RCP2-1000 unit front panel, select sequentially:

Main Menu → 2.Com.Setup → 5.IPSetup → 2.LocalIP and then select address 192.168.0.0 by using the navigation (▲▼▶◀) keys. Then press the **Enter** key. Follow the same menu route to select the Subnet, Gateway, IPPort and IPLock items, and set those parameters to:

```
Subnet:255.255.255.0;
Gateway:0.0.0.0;
IPLock: 255.255.255.255;
IPPort:1038.
```

Verify the selected parameters by selecting item **1.IPInfo** and pressing the **Enter** key.

4. On the RCP2-1000 unit front panel select sequentially:

Main Menu → 2.Com.Setup → 4.Interface → 3.IPNet, then press Enter. The RCP2-1000 is now set up to work with Ethernet Interface. You may now ping the unit from host PC:

```
C:\>ping 192.168.0.0
```

This will display:

```
Pinging 192.168.0.0 with 32 bytes of data:
Reply from 192.168.0.0: bytes=32 time<10ms TTL=128
Reply from 192.168.0.0: bytes=32 time<10ms TTL=128
Reply from 192.168.0.0: bytes=32 time<10ms TTL=128
Reply from 192.168.0.0: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.0.3:
    Packets: Sent=4, Received=4, Lost=0 (0%loss),
    Approximate round trip times I milli-seconds:
    Minimum=0ms, Maximum=0ms, Average=0ms
```

5. Run the Paradise Datacom Universal M&C package on the host PC to check all M&C functions. Refer to Appendix C for details. When prompted, select an Internet connection to the unit using IP Address 192.168.0.0, local port address to 1039 and remote port address to 1038. The unit is now connected to your host workstation for remote M&C.

THIS PAGE LEFT INTENTIONALLY BLANK

This section briefly describes the basic theory related to the physical layer of 10/100Bas-T networking, as well as proper wiring techniques.

There are several classifications of cable used for twisted-pair networks. Recommended cable for all new installations is Category 5 (or CAT 5). CAT 5 cable has four twisted pairs of wire for a total of eight individually insulated wires. Each pair is color coded with one wire having a solid color (blue, orange, green, or brown) twisted around a second wire with a white background and a stripe of the same color. The solid colors may have a white stripe in some cables. Cable colors are commonly described using the background color followed by the color of the stripe; e.g., white-orange is a cable with a white background and an orange stripe.

The straight through and crossover patch cables are terminated with CAT 5 RJ-45 modular plugs. RJ-45 plugs are similar to those you'll see on the end of your telephone cable except they have eight versus four or six contacts on the end of the plug and they are about twice as big. Make sure they are rated for CAT 5 wiring. (RJ means "Registered Jack"). A special Modular Plug Crimping Tool (such as that shown in **Figure B-1**) is needed for proper wiring.



Figure B-1: Modular Plug Crimping Tool

The 10BASE-T and 100BASE-TX Ethernets consist of two transmission lines. Each transmission line is a pair of twisted wires. One pair receives data signals and the other pair transmits data signals. A balanced line driver or transmitter is at one end of one of these lines and a line receiver is at the other end. A simplified schematic for one of these lines and its transmitter and receiver is shown in **Figure B-2**.

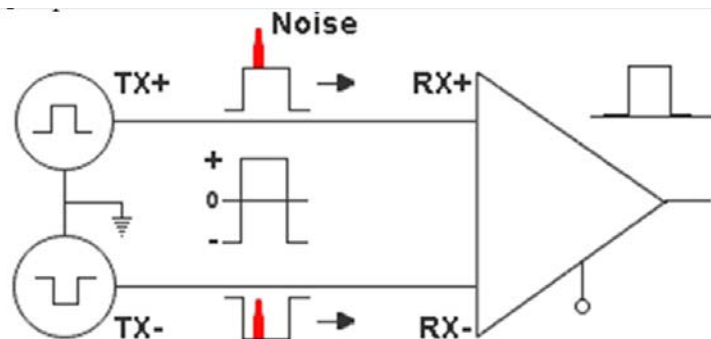


Figure B-2: Transmission Line

The main concern is the transient magnetic fields which surrounds the wires and the magnetic fields generated externally by the other transmission lines in the cable, other network cables, electric motors, fluorescent lights, telephone and electric lines, lightning, etc. This is known as noise. Magnetic fields induce their own pulses in a transmission line, which may literally bury the Ethernet pulses.

The twisted-pair Ethernet employs two principle means for combating noise. The first is the use of balanced transmitters and receivers. A signal pulse actually consists of two simultaneous pulses relative to ground: a negative pulse on one line and a positive pulse on the other. The receiver detects the total difference between these two pulses. Since a pulse of noise (shown in red in the diagram) usually produces pulses of the same polarity on both lines one pulse is essentially canceled by out the other at the receiver. In addition, the magnetic field surrounding one wire from a signal pulse is a mirror of the one on the other wire. At a very short distance from the two wires, the magnetic fields are opposite and have a tendency to cancel the effect of each other. This reduces the line's impact on the other pair of wires and the rest of the world.

The second and the primary means of reducing cross-talk between the pairs in the cable, is the double helix configuration produced by twisting the wires together. This configuration produces symmetrical (identical) noise signals in each wire. Ideally, their difference, as detected at the receiver, is zero. In actuality, it is much reduced.

Pin-out diagrams of the two types of UTP Ethernet cables are shown in **Figure B-3**.

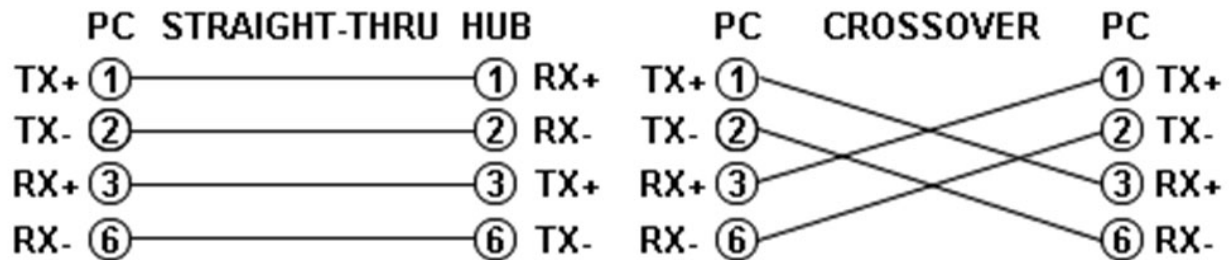


Figure B-3: Ethernet Cable Pin-Outs

Note that the TX (transmitter) pins are connected to corresponding RX (receiver) pins, plus to plus and minus to minus. Use a crossover cable to connect units with identical interfaces. If you use a straight-through cable, one of the two units must, in effect, perform the crossover function.

Two wire color-code standards apply: EIA/TIA 568A and EIA/TIA 568B. The codes are commonly depicted with RJ-45 jacks as shown in **Figure B-4**. If we apply the 568A color code and show all eight wires, our pin-out looks like **Figure B-5**.

Note that pins 4, 5, 7, and 8 and the blue and brown pairs are not used in either standard. Quite contrary to what you may read elsewhere, these pins and wires are not used or required to implement 100BASE-TX duplexing.

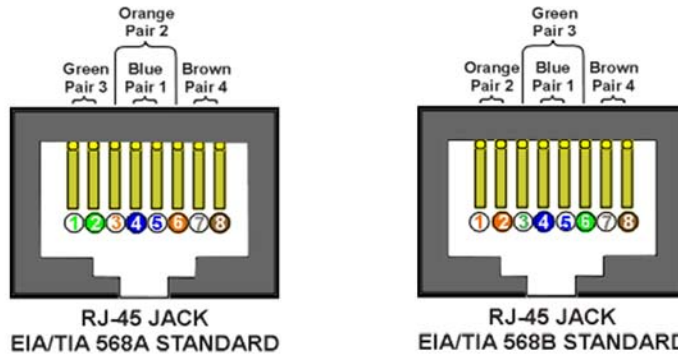


Figure B-4: Ethernet Wire Color Code Standards

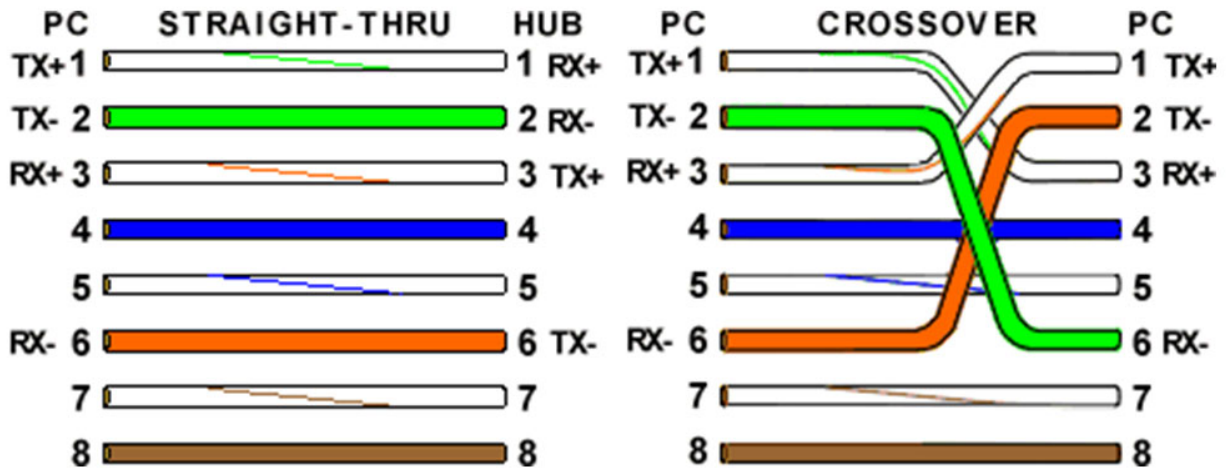
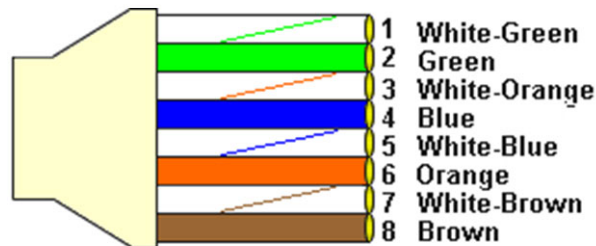
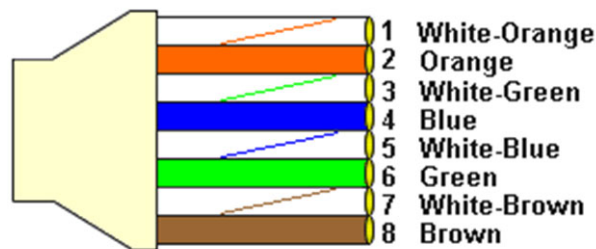


Figure B-5: Wiring Using 568A Color Codes

There are only two unique cable ends in the preceding diagrams, they correspond to the 568A and 568B RJ-45 jacks and are shown in **Figure B-6**.



568A CABLE



568B CABLE

Figure B-6: Wiring Using 568A and 568B Color Codes

Again, the wires with colored backgrounds may have white stripes and may be denoted that way in diagrams found elsewhere. For example, the green wire may be labeled Green-White. The background color is always specified first.

Now, all you need to remember, to properly configure the cables, are the diagrams for the two cable ends and the following rules:

- A straight-thru cable has identical ends.
- A crossover cable has different ends.

It makes no functional difference which standard you use for a straight-thru cable. You can start a crossover cable with either standard as long as the other end is the other standard. It makes no functional difference which end is which. 568A patch cable will work in a network with 568B wiring and 568B patch cable will work in a 568A network

Here are some essential cabling rules:

1. Try to avoid running cables parallel to power cables.
2. Do not bend cables to less than four times the diameter of the cable.
3. If you bundle a group of cables together with cable ties (zip ties), do not over-cinch them. It's okay to snug them together firmly; but don't tighten them so much that you deform the cables.
4. Keep cables away from devices which can introduce noise into them. Here's a short list: copy machines, electric heaters, speakers, printers, TV sets, fluorescent lights, copiers, welding machines, microwave ovens, telephones, fans, elevators, motors, electric ovens, dryers, washing machines, and shop equipment.
5. Avoid stretching UTP cables (tension when pulling cables should not exceed 25 LBS).
6. Do not run UTP cable outside of a building. It presents a very dangerous lightning hazard!
7. Do not use a stapler to secure UTP cables. Use telephone wire/RG-6 coaxial wire hangers, which are available at most hardware stores.

C.1 Adding a New Compact Outdoor SSPA to the Universal M&C

Download the Teledyne Paradise Universal Monitor & Control application and install it onto a personal computer. Launch the application.

The operator may connect the PC to the RCP2-1000-CO and communicate with a connected Compact Outdoor SSPA.

To add a new unit to the Universal M&C application, choose “Action > Add Unit” from the Main Menu. Then choose “Compact Outdoor SSPA”. A new dialog window will open, as shown in **Figure C-1**.

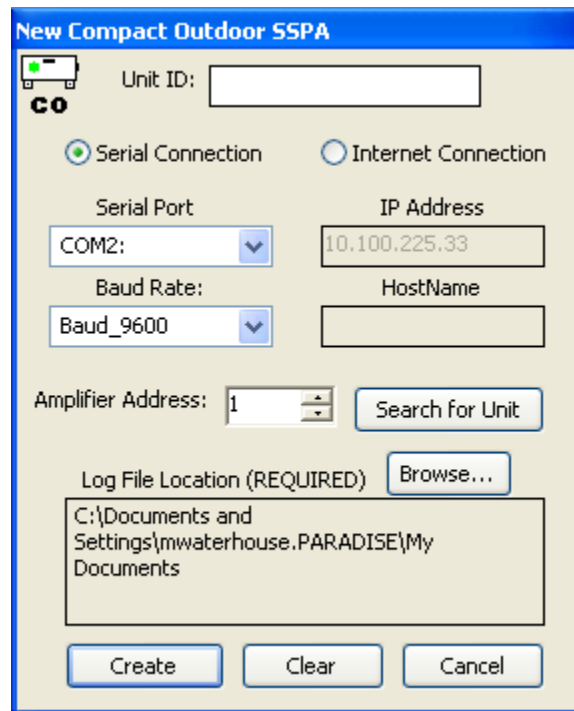


Figure C-1: New Compact Outdoor SSPA Dialog Window

To add a single SSPA to the M&C Utility, fill in the appropriate boxes in the “New Compact Outdoor SSPA” dialog window.

A Unit ID is not required, although it is recommended. If a Unit ID isn’t entered the Unit ID will be assigned by the M&C.

To add a unit connected to a serial port you must supply a Port and a Baud Rate.

To add a unit connected via UDP (TCP/IP) you must supply either a Hostname or an IP Address

Specify the Unit's Unique Address in the "Amplifier Address" box. If you don't know the address of the unit, you may search for it. Be aware that this search feature is only useful when you have only one unit connected to your PC at a time.

Choose a log file location by clicking the "Browse..." button. The default is the "My Documents" folder. The log file name will be the UnitID and the extension ".log" appended to the file name; i.e., "Unit1.log".

C.2 Remote Control of Compact Outdoor SSPA via Universal M&C

The Universal M&C application opens on the "Status" screen, shown in **Figure C-2**. The status screen reflects the current conditions (or state) of the SSPA. In addition, the status screen allows the operator to Mute or Unmute the carrier and adjust the unit's attenuation for gain control. It also shows the unit's fault status.

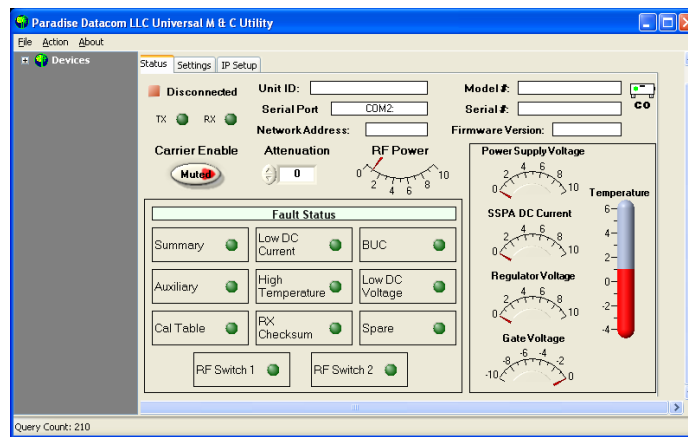


Figure C-2: SSPA Status Window

The second tab is the "Settings" screen, shown in **Figure C-3**.

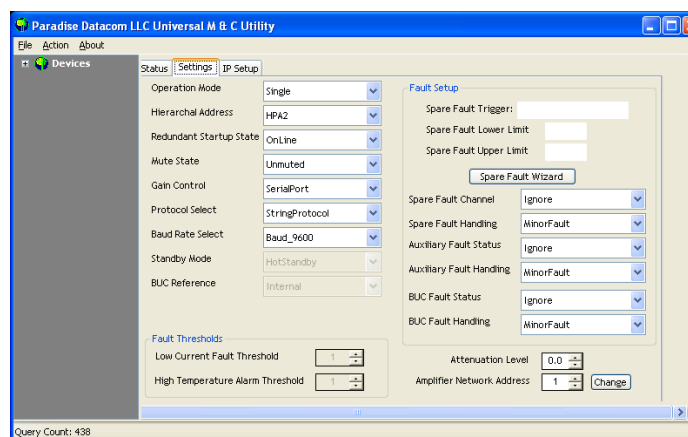


Figure C-3: SSPA Settings Window

This window shows the user all available settings on the connected Compact Outdoor SSPA unit. All user-adjustable settings may be modified to suit the specific needs of the customer. If modification of any settings is necessary please refer to your Compact Outdoor SSPA Manual.

The third tab is the “IP Setup” screen, shown in **Figure C-4**.

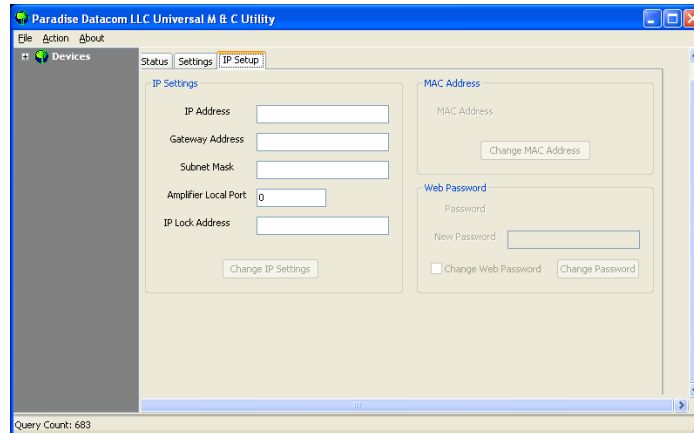


Figure C-4: IP Setup Window

This window displays the TCP/IP settings for the RCP unit, including the IP Address, Gateway Address, Subnet Mask, Local Port and IP Lock Address. The “Amplifier Local Port” is the port that the RCP listens to for UDP requests. The RCP also answers requests using the same port. The Gateway Address and Subnet Mask are standard settings for TCP/IP communications.

If any of the above settings are modified, the RCP unit must be reset before the new values may be used.

The IP Lock Address is used for security. If it is set to something besides 0.0.0.0 or 255.255.255.255 it will only answer the address it is set to. For example, if the IP Lock Address is 192.168.0.50 then a request from 192.168.0.100 will not be accepted. The IP Lock Address may be changed without resetting the SSPA.

THIS PAGE LEFT INTENTIONALLY BLANK

The following pages comprise the specification sheet (209728) for the RCP2-1000 Remote Control Panel for Compact Outdoor and High Power Outdoor SSPAs. Please refer to the Paradise Datacom web site (www.paradisedata.com) for the latest revision of this document.

THIS PAGE LEFT INTENTIONALLY BLANK