



FGR2-P PLUS Radios

FGR2-P
FGR2-PE
FGR2-PE-U

Covering Software v3.14

User & Reference Manual



Safety Information

The products described in this manual can fail in a variety of modes due to misuse, age, or malfunction and is not designed or intended for used in systems requiring fail-safe performance, including life safety systems. Systems with the products must be designed to prevent personal injury and property damage during product operation and in the event of product failure.



Warning! Do not remove or insert the Ethernet or diagnostics cable while circuit is live unless the area is known to be free of ignition concentrations of flammable gasses or vapors.

Warranty

FreeWave Technologies, Inc. warrants the FreeWave® FGR2-P, -PE, & -PE-U PLUS Radios (Product) that you have purchased against defects in materials and manufacturing for a period of three years from the date of shipment, depending on model number. In the event of a Product failure due to materials or workmanship, FreeWave will, at its discretion, repair or replace the Product. For evaluation of Warranty coverage, return the Product to FreeWave upon receiving a Return Material Authorization (RMA). The replacement product will remain under warranty for 90 days or the remainder of the original product warranty period, whichever is longer.

IN NO EVENT WILL FREEWAVE TECHNOLOGIES, INC., ITS SUPPLIERS, OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT. THIS INCLUDES BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, INABILITY TO ACCESS OR SEND COMMUNICATION OR DATA, PERSONAL INJURY OR DAMAGE, OR OTHER LOSS WHICH MAY ARISE FROM THE USE OF THIS PRODUCT. THE WARRANTY IS EXCLUSIVE AND ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE ARE EXPRESSLY DISCLAIMED.

FreeWave's Warranty does **not apply** in the following circumstances:

1. If Product repair, adjustments, or parts replacements are required due to accident, neglect, or undue physical, electrical, or electromagnetic stress.
2. If Product is used outside of FreeWave specifications as stated in the Product's data sheet.
3. If Product has been modified, repaired, or altered by Customer unless FreeWave specifically authorized such alterations in each instance in writing.

FreeWave Technologies, Inc.
5395 Pearl Parkway, Suite 100
Boulder, CO 80301
303.381.9200
Toll Free: 1.866.923.6168
Fax: 303.786.9948

Copyright © 2018 by FreeWave Technologies, Inc.
All rights reserved.

www.freewave.com

Table Of Contents

Preface	11
1. Introduction	14
1.1. Components of the FGR2-P, -PE, & -PE-U PLUS Radios	15
1.2. LED Designations	16
1.2.1. Authentication LEDs	16
1.2.2. Boot-Up LED Sequence	17
1.2.3. COM Port LED Conditions	17
1.2.4. Error LED Conditions	17
1.2.5. Ethernet Port LED Conditions	17
1.3. Choose a Radio Location	18
1.4. Choose Point-to-Point (PTP) or Point-to-MultiPoint (PTMP) Operation	18
PTP Network	18
PTMP Network	18
1.4.1. Differences between PTP and PTMP Networks	19
PTP Network	19
PTMP Network	19
1.5. Point-to-Point (PTP) Operation LEDs	20
1.6. Point-to-MultiPoint (PTMP) Operation LEDs	20
2. Set Up and Program Radios	22
2.1. Basic Steps to Programming the FGR2-P, -PE, & -PE-U PLUS Radios	23
2.1.1. PTMP Network Considerations	24
2.2. Powering the FGR2-P, -PE, & -PE-U PLUS Radio	24
2.3. Identify and Change the FGR2-P, -PE, & -PE-U PLUS Radio's IP Address	24
2.4. Configuration Tool Options	25
2.5. Accessing the Configuration Windows	27
Administrator Login and Password	27
Guest Login and Password	27
2.6. Navigating the Configuration Windows	29
2.6.1. Menu bar	29
2.6.2. Save and Apply	30
2.6.3. Reboot	31
2.7. Providing Site Information	32
2.8. Use the MultiPoint Gateway to Change All Connected Radios	33
2.9. Creating User Logins	36
2.9.1. Defining User Groups	36
2.9.2. Editing User Group Rights	37

2.9.3. Add and Delete Users	38
Adding a User	38
Deleting a User	39
2.9.4. Changing User Passwords	40
2.10. Upgrading the FGR2-P, -PE, & -PE-U PLUS Radio Software Using a TFTP Server	41
2.10.1. Downgrading Software	41
2.10.2. Configuring the TFTP Server	42
Before Upgrading Software Using the TFTP Server	42
2.10.3. Upgrading Software Using the Configuration Windows	43
2.10.4. Upgrade FGR2-P, -PE, & -PE-U PLUS Software Globally	46
2.10.5. Verifying Software Upgrades	48
2.10.6. Common Software Upgrade Issues and Solutions	49
"File Not Found" in either the Configuration Windows or the FreeWave TFTP Server	49
Software Upgrade Times Out	49
Software Upgrading is Taking a Long Time to Complete	49
2.11. Resetting Radios to the Factory Default Settings	49
3. IP and Network Communication Settings	51
3.1. IP Setup Parameter Reference	52
3.1.1. Default Gateway	52
3.1.2. IP Address	53
3.1.3. MTU	54
3.1.4. NTP Client Enable	55
3.1.5. NTP IP Address	55
3.1.6. Push to (Syslog) Server	56
3.1.7. Spanning Tree	56
3.1.8. Subnet Mask	57
3.1.9. Syslog Server 1	58
3.1.10. Syslog Server 2	58
3.1.11. Data VLAN ID	59
3.1.12. VLAN Default Gateway	59
3.1.13. VLAN IP Address	60
3.1.14. Management VLAN ID	60
3.1.15. VLAN Mode	61
3.1.16. VLAN Subnet Mask	61
3.1.17. VLAN Trunk ID 1 to VLAN Trunk ID 5	62
3.1.18. Web Page Port (http)	62
4. Serial Port Settings	64
4.1. Set the Serial Port Mode	64

4.2. Disabling Serial Ports	66
4.3. Viewing the Serial Port Status	67
4.3.1. Ethernet (Rx and Tx)	68
4.3.2. Serial (Rx and Tx)	68
4.3.3. Status	68
4.4. Serial Port Parameter Reference	69
4.4.1. Multicast Enable	69
4.4.2. Multicast IP Address	69
4.4.3. Multicast Port	70
4.4.4. Pre-Packet and Post-Packet Timeouts	70
4.4.5. Runtime Serial Setup "U"	72
4.4.6. Baud Rate	72
4.4.7. CD Mode	73
4.4.8. Data Bits	74
4.4.9. Flow Control	74
4.4.10. Interface	74
4.4.11. Modbus RTU	75
4.4.12. Parity	76
4.4.13. Stop Bits	76
4.4.14. TCP Client Enable	76
4.4.15. TCP Client IP Address	77
4.4.16. TCP Client Port	77
4.4.17. TCP Server Enable	78
4.4.18. TCP Server Inactivity Timeout	79
4.4.19. TCP Server Keep Alive	79
4.4.20. TCP Server Port	80
4.4.21. UDP Enable	80
4.4.22. UDP IP Address	80
4.4.23. UDP IP Port	81
5. Radio Settings	82
5.1. Radio Setup Parameter Reference	83
5.1.1. Addressed Repeat	83
5.1.2. Broadcast Repeat	84
5.1.3. Broadcast Repeat in MultiPoint Networks with Repeaters	85
5.1.4. Frequency Key	85
5.1.5. Frequency Zones	86
5.1.6. Master Tx Beacon	87
5.1.7. Max Packet Size and Min Packet Size	88

5.1.8. Modem Mode	90
Modem Mode Options	91
5.1.9. Network ID	93
5.1.10. Network Type	94
5.1.11. Repeaters	94
5.1.12. Retry Timeout	95
5.1.13. RF Data Rate	96
5.1.14. Slave Attempts	97
5.1.15. Slave Connect Odds	98
5.1.16. Subnet ID	99
5.1.17. Transmit Power	100
5.1.18. Transmit Rate	101
6. Security Settings	102
6.1. Viewing the System Log	103
6.2. Specify a Reboot Interval Schedule	105
6.3. Security Parameter Reference	109
6.3.1. AES Encryption Key	109
6.3.2. AES Version	110
6.3.3. Detach Local Ethernet	110
6.3.4. Force SSL (https)	111
6.3.5. MAC Filter	111
6.3.6. Peer To Peer	112
6.3.7. RADIUS Enable	113
6.3.8. RADIUS IP Address	114
6.3.9. RADIUS Port	115
6.3.10. Reboot Interval	115
6.3.11. Shared Secret	115
6.3.12. User Password	116
7. SNMP Settings	117
7.1. SNMP Parameter Reference	118
7.1.1. Authentication Method	118
7.1.2. Authentication Password (v3)	118
7.1.3. Min Fault Time	119
7.1.4. Privacy Method	119
7.1.5. Privacy Password (v3)	119
7.1.6. Read Community	120
7.1.7. SNMP Version	120
7.1.8. Trap Community	121

7.1.9. Trap Manager IP	121
7.1.10. Trap Version	122
7.1.11. Write Community	122
7.2. SNMP Trap Limits Parameter Reference	123
7.2.1. Delta Alarm Enable	123
7.2.2. Delta Alarm Below	123
7.2.3. Noise Alarm Above	124
7.2.4. Noise Alarm Enable	124
7.2.5. Reflected Alarm Above	124
7.2.6. Reflected Alarm Enable	125
7.2.7. Rx Rate Alarm Below	125
7.2.8. Rx Rate Alarm Enable	126
7.2.9. Signal Alarm Below	126
7.2.10. Signal Alarm Enable	126
7.2.11. Tx Rate Alarm Below	127
7.2.12. Tx Rate Alarm Enable	127
7.2.13. Voltage Alarm Above	128
7.2.14. Voltage Alarm Below	128
7.2.15. Voltage Alarm Enable	128
8. Viewing Radio Status and Statistics	129
8.1. Refreshing and Resetting Statistics	130
8.2. Available Statistics	130
8.2.1. admin From	130
8.2.2. Bad Packets	130
8.2.3. Broadcast Packets	130
8.2.4. Connected To	130
8.2.5. Disconnect Count	131
8.2.6. Distance	131
8.2.7. Firmware Version	131
8.2.8. Hardware Version	131
8.2.9. Noise	131
8.2.10. Notes	131
8.2.11. Packets Dropped	132
8.2.12. Packets Sent	132
8.2.13. Peer to Peer Packets	132
8.2.14. Radio Addressed Packets	132
8.2.15. Radio Parse Error	132
8.2.16. Received	132

8.2.17. Reflected Power	132
8.2.18. RX Success Rate	133
8.2.19. RX Throughput	133
8.2.20. Signal	133
8.2.21. Site Contact	133
8.2.22. Site Name	133
8.2.23. Software Boot Version	133
8.2.24. System Name	133
8.2.25. Temperature	134
8.2.26. TX Success Rate	134
8.2.27. TX Throughput	134
8.2.28. Un-Acked Packets	134
8.2.29. Upstream Noise	134
8.2.30. Upstream Signal	135
8.2.31. Uptime	135
8.2.32. Voltage	135
8.2.33. Wireless Version	135
9. Data Communication Link Examples	136
9.1. Example 1: Gateway to Endpoint	137
9.2. Example 2: Gateway, Repeater, and Endpoint	137
9.3. Example 3: Gateway, Two Repeaters, and Endpoint	138
9.4. Example 4: Gateway, Repeater, and Multiple Endpoints	139
9.5. Example 5: Standard Point-to-MultiPoint Network	140
9.6. Example 6: Point-to-MultiPoint Network with an Endpoint/Repeater Site	141
9.7. Assigning Subnet Values	142
9.7.1. Subnet Example 1	142
9.7.2. Subnet Example 2	143
9.7.3. Subnet Example 3	144
10. Additional Radio Information	145
10.1. Operational RS422 and RS485 Information	145
10.1.1. RS422	145
10.1.2. RS485	145
10.2. RS422 and RS485 Full Duplex Pinouts	146
10.3. RS485 Half Duplex Pinouts	146
10.4. RJ45 to DB9 Cable	147
10.4.1. RS232 - COM1 and COM2 RJ45 Pin Assignments	147
10.4.2. RS232 - DB9 Connector Pin Assignments	148
11. Approved Antennas	149

11.1. 900MHz Directional Antennas	149
11.2. 900MHz Omni-directional Antennas	149
12. Configuration Windows	151
12.1. Diagnostics window	152
12.2. IP Setup window	153
12.3. Radio Setup window	156
12.4. Call Book window	158
12.4.1. Programming Point-To-Point Extended Call Book to Use Three or Four Repeaters	160
12.4.2. Programming Point-to-MultiPoint Call Book	161
12.4.3. MultiPoint Master Call Book (Unit Serial Number 884-1111)	161
12.4.4. MultiPoint Repeater Call Book (Unit Serial Number 884-2222)	161
12.4.5. MultiPoint Slave Call Book (Unit Serial Number 884-3333)	162
12.4.6. Programming Point-to-MultiPoint Extended Call Book	162
12.5. Security window	163
12.5.1. Memory Information window	166
12.5.2. View Log window	167
12.6. Serial Setup window	168
12.6.1. Serial Port Status window	171
12.7. SNMP window	173
12.8. Status window	175
12.9. Tools window	178
12.10. Users window	180
12.10.1. Add User window	181
12.10.2. Change Password window	182
13. Release Notes: FGR2-P, -PE, & -PE-U PLUS Radios	183
13.1. Version 3.14	183
13.2. Version 3.13	183
13.3. Version 3.11	184
13.4. Version 3.06	184
13.5. Version 3.01	185
13.5.1. Warning: Extreme Set-Up Parameters	186
IP Setup	186
Serial Setup	186
Security Setup	186
SNMP Setup	187
13.5.2. ERRATA Information	187
13.5.3. Specific Upgrade Notes for the Serial Setup window	187
Upgrading from v2.22 to v3.01	187

Upgrading from v2.34 to v3.01	188
13.6. Version 2.34	188
13.7. Version 2.22	190
Appendix A: Factory Default Settings	191
Appendix B: FGR2-P, -PE, & -PE-U Technical Specifications	196
Appendix C: FGR2-P Mechanical Drawing	199
Appendix D: FGR2-PE and PE-U Mechanical Drawing	200
Appendix E: Object List for FREEWAVE-TECHNOLOGIES-MIB	201
Appendix F: FreeWave Legal Information	209

Preface

This document includes this information about the FreeWave FGR2-P, -PE, & -PE-U Radios:

- An introduction to the radio, its ports and LEDs, and how to determine the mode to run it in.
- Basic programming information including the interfaces used to program the radio, determining a radio's IP address, setting permissions to access the radio setup information, and how to perform software upgrades.
- Descriptions of each parameter available when defining IP information, serial port setup, general radio setup, SNMP information, and security.
- Descriptions of each statistic that is available about the radio's state and performance.
- Examples of how FreeWave radios can exist in a network with other radios.
- Pinouts, specifications, and other mechanical information.
- Information about additional tools when working with the FGR2-P, -PE, & -PE-U Radios.

Additional Information

For more information about creating Ethernet networks, see:

- Application Note #5474: Connecting a Plus Radio to a Data Radio T-96SR
- Application Note #5495: Not All Wireless Ethernet/IP Applications are Created Equal
- Application Note #5500: Design Considerations for Plus IP/Ethernet Radios

For information about installing PLUS Radios, see:

- Enterprise Gateway Installation Guide

Contact FreeWave Technical Support

For up-to-date troubleshooting information, check the **Support** page at www.freewave.com.

FreeWave provides technical support Monday through Friday, 8:00 AM to 5:00 PM Mountain Time (GMT -7).

- Call toll-free at 1.866.923.6168.
- In Colorado, call 303.381.9200.
- Contact us through e-mail at moreinfo@freewave.com.

Document Styles

This document uses these styles:

- FreeWave applications appear as: **FreeWave**.
- Parameter setting text appears as: **[Page=radioSettings]**
- File names appear as: **configuration.cfg**.
- File paths appear as: **C:\Program Files (x86)\FreeWave Technologies**.
- User-entered text appears as: **xxxxxxxxxx**.



Caution: Indicates a situation that **may** cause damage to personnel, the radio, data, or network.

Example: Provides example information of the related text.

FREEWAVE Recommends: Identifies FreeWave recommendation information.

Important!: Provides semi-cautionary information relevant to the text or procedure.

Note: Emphasis of specific information relevant to the text or procedure.



Tip Provides time saving or informative suggestions about using the product.



Warning! Indicates a situation that **will** cause damage to personnel, the radio, data, or network.

Parameter Preference

The **Parameter Preference** tables describe the available parameters / controls using the:

- [Configuration Windows \(on page 151\)](#).
- Terminal Interface.

The **Parameter Preference** tables have this layout:

<Parameter Name>	
Setting	Description
Web Parameter:	The name of the field as it appears in the Configuration Windows .
Terminal Menu:	The menu path and field name to access the parameter using the terminal menus available through the serial port.
Network Type:	Point-to-Point, Point-to-MultiPoint, or Both
Default Setting:	The factory default setting for the parameter.
Options:	The options the parameter can be set to.
Description:	A description of what the parameter is and how it applies to the radio in the network.

1. Introduction

Thank you for purchasing the FreeWave Technologies, Inc. FGR2-P, -PE, & -PE-U device. The FGR2-P, -PE, & -PE-U offer industrial serial and Ethernet wireless connectivity using the license-free spread spectrum for data communication over long distances. The Radios are compatible with other FreeWave FGR plus family Radios and have two Ethernet ports and two serial ports, providing the ability to transition from serial to Ethernet data communications without having to replace your wireless communications infrastructure.



Figure 1: FGR2-P, -PE, & -PE-U Product Image

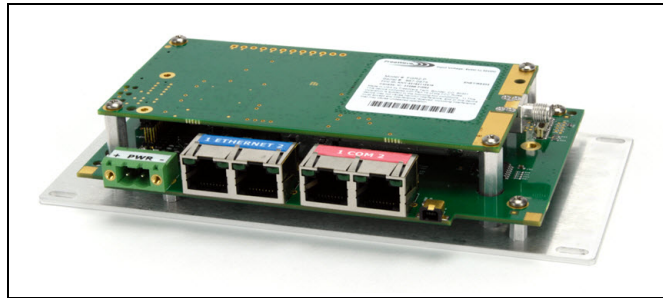


Figure 2: FGR2-P, -PE, & -PE-U Board

Important! The FGR2-P, -PE, & -PE-U are compatible over the air with the FGRplusRE and the MM2-P-T Radios. They are NOT compatible over the air with any other FreeWave products.

1.1. Components of the FGR2-P, -PE, & -PE-U PLUS Radios

The FGR2-P, -PE, & -PE-U PLUS Radios have these components:

- A power connector.
- LEDs to help determine when data is being received or sent from the radio and to provide additional information about the radio's state.
- Two Ethernet ports (items 4 to 7, outlined in blue on the radio).
- Two COM ports (items 8 to 11, outlined in red on the radio).
- An antenna port.
- A diagnostic port (may be present on some units).
- The FGR2-P Radio has the same configuration as the FGR2-PE-U, without the enclosure.

Note: As of May-2018, the diagnostic port is active under certain configurations:
The diagnostic port does NOT function using MultiPoint Gateways and Point to Point Repeaters.
The diagnostic port does function using MultiPoint Repeaters and Endpoints.
The diagnostic port functions with restrictions using Point to Point Gateways and Point to Point Endpoints.



Radios running software v2.26 or later can be configured using a terminal emulator connected to COM1.

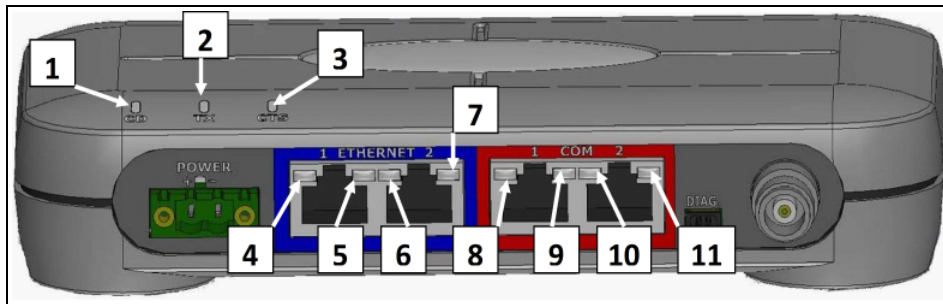


Figure 3: Components of the FGR2-P, -PE, & -PE-U PLUS Radios

Components of the FGR2-P, -PE, & -PE-U PLUS Radios	
Label #	Description
1	CD
2	TX
3	CTS
4	Ethernet 1 10 BaseT Link/Activity
5	Ethernet 1 100 BaseT Link
6	Ethernet 2 10 BaseT Link/Activity
7	Ethernet 2 100 BaseT Link
8	COM 1 Data (C1)
9	Error 1 (E1)
10	COM 2 Data (C2)
11	Error 2 (E2)




1.2. LED Designations

1.2.1. Authentication LEDs



Authentication LEDs	
Condition	LED Pattern
Endpoint cannot contact RADIUS server	Solid green ■ E1 LED
Endpoint was denied authentication from the RADIUS server	Alternating green ■ E1 and E2 LED
Endpoint AES encryption key does not match Gateway encryption key	Alternating green ■ E1 and E2 LED

1.2.2. Boot-Up LED Sequence



The LEDs on the FGR2-P, -PE, & -PE-U PLUS Radio follows this sequence when the radio powers up:

1. C1 lights solid green .
2. C2 lights solid green , C1 remains lit.
3. E2 lights solid green , C1 and C2 remain lit.
4. C1 turns off.
5. C2 turns off.
6. E2 turns off.









1.2.3. COM Port LED Conditions

COM Port LED Conditions	
Condition	Communications Port 1 (C1) or 2 (C2)
Data streaming into RX	Solid red bright 
Data streaming out TX	Solid red bright 

1.2.4. Error LED Conditions

Error LED Conditions	
Condition	Error Light (E1/E2)
Buffer overflow locally	E1 LED is solid green 
Buffer overflow in network	E2 LED is solid green 

1.2.5. Ethernet Port LED Conditions

Ethernet Port LED Conditions		
Status	10 Base T Link / Activity	100 Base T Link LED
Linked, data activity	Blinking / Flickering green 	Solid green (100 BaseT  /Off (10 BaseT )
Linked, no data activity	Solid green 	Solid green (100 BaseT  /Off (10 BaseT )
Not linked. Verify cable is in good condition and plugged in.	Off 	Off 

1.3. Choose a Radio Location

Placement of the FreeWave radio may have a significant impact on its performance. The key to the overall robustness of the radio link is the height of the antenna.

When using an external antenna, placement of that antenna is critical to a solid data link. Other antennas in close proximity are a potential source of interference.

Use the **Radio Statistics** on the [Status window \(on page 175\)](#) to help identify potential problems. In general, FreeWave units with a higher antenna placement will have a better communication link.

In practice, the radio should be placed away from computers, telephones, answering machines, and other similar devices. The cable included with the radio provides ample distance for placement away from other equipment.

Note: FreeWave offers directional and Omni-directional antennas with cable lengths ranging from 3 to 200 feet.



An adjustment as little as 2 feet in antenna placement may resolve noise issues. In extreme cases, (e.g., Cellular Telephone tower interference) the band pass filters that FreeWave offers may reduce this out-of-band noise.

1.4. Choose Point-to-Point (PTP) or Point-to-MultiPoint (PTMP) Operation

PTP Network

- A PTP network functions best when the network consists of one Gateway and one Endpoint radio.
- A maximum of four Repeaters can be added to extend the reach of the network.

Important! Adding a Repeater to a network cuts the network throughput by 50%.

In a Point-to-Point network, the Gateway determines all settings in an Endpoint or Repeater, except for the **Transmit Power** and **Retry Timeout**. All other settings in a Point-to-Point network are determined by the Gateway's settings.

PTMP Network

In a PTMP network, the Gateway radio is able to simultaneously communicate with numerous Endpoint radios.

- In its simplest form, a PTMP network functions with the Gateway broadcasting its messages to all Endpoint radios.
- If requested by the Gateway, the Endpoint radios respond to the Gateway when given data by the device connected to the data port.
 - This response depends on the setup.

- The network can be extended with as many Repeaters as is required.

Important!: Adding a Repeater to a network cuts the network throughput by 50%.

1.4.1. Differences between PTP and PTMP Networks

PTP Network

In a PTP network all packets are acknowledged, whether sent from the Gateway to the Endpoint or from the Endpoint to the Gateway.

PTMP Network

In a PTMP network, the user determines the number of times outbound packets from the Gateway or Repeater to the Endpoint or other Repeaters are sent.


























































- The receiving radio, Endpoint or Repeater, accepts the first packet received that passes the 32 bit CRC.
 - However, the packet is not acknowledged.
- On the return to the Gateway, all packets sent are acknowledged or retransmitted until they are acknowledged.
 - Therefore, the return link in a PTMP network is generally very robust.

Traditionally, a PTMP network is used in applications where data is collected from many instruments and reported back to one central site. The architecture of such a network is different from PTP applications. These parameters influence the number of radios that can exist in a PTMP network:










- **Baud Rate.** The data rate between the radio and the device it is connected to could limit the amount of data and the number of radios that can exist in a network.
- **Contention:** The amount of contention between Endpoint radios. Polled Endpoint radios versus vs. timed Endpoint radios.
- **Data Block Size.** The longer the data blocks, the fewer number of deployed Endpoint radios can exist in the network.
- **Repeater Use.** Using the **Repeater** setting in a PTP or PTMP network decreases the overall network capacity by at least 50%.






































Example: If the network polls once a day to retrieve sparse data, several hundred Endpoint radios could be configured to a single Gateway. However, if each Endpoint transmits larger amounts of data or data more frequently, fewer Endpoint radios can link to the Gateway while receiving the same network performance. When larger amounts of data are sent more frequently, the overall network bandwidth is closer to capacity with fewer Endpoint radios.



1.5. Point-to-Point (PTP) Operation LEDs

Condition	Gateway			Endpoint			Repeater		
	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)
Powered, no link	Solid red bright 	Solid red bright 	Solid red bright 	Solid red bright 	Off 	Blinking red 	Solid red bright 	Off 	Blinking red 
Linked, no Repeater, sending sparse data	Solid green 	Intermittent flash red 	Intermittent flash red 	Solid green 	Intermittent flash red 	Intermittent flash red 	n/a	n/a	n/a
Gateway calling Endpoint through Repeater	Solid red bright 	Solid red dim 	Solid red bright 	Solid red bright 	Off 	Blinking red 	Solid red bright 	Off 	Blinking red 
Gateway linked to Repeater, not to Endpoint	Flashing orange 	Solid red dim 	Solid red bright 	Solid red bright 	Off 	Blinking red 	Solid Red bright 	Solid red dim 	Solid red bright 
Repeater linked to Endpoint	Solid green 	Intermittent flash red 	Intermittent flash red 	Solid green 	Intermittent flash red 	Intermittent flash red 	Solid green 	Intermittent flash red 	Intermittent flash red 
Mode 6 - waiting for ATD command	Solid red bright 	Off 	Blinking red 	Solid red bright 	Off 	Blinking red 	n/a	n/a	n/a
Setup Mode	Solid green 	Solid green 	Solid green 	Solid green 	Solid green 	Solid green 	Solid green 	Solid green 	Solid green 

1.6. Point-to-MultiPoint (PTMP) Operation LEDs

Condition	Gateway			Endpoint			Repeater		
	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)
Powered, not linked	Solid red bright 	Solid red dim 	Off 	Solid red bright 	Off 	Blinking red 	Solid red bright 	Off 	Blinking red 

Condition	Gateway			Endpoint			Repeater		
	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)	Carrier Detect (CD)	Transmit (Tx)	Clear to Send (CTS)
Repeater and Endpoint linked to Gateway, no data	Solid red bright 	Solid red dim 	Off 	Solid green 	Off 	Solid red bright 	Solid green 	Solid red dim 	Solid red bright 
Repeater and Endpoint linked to Gateway, Gateway sending data to Endpoint	Solid red bright 	Solid red dim 	Off 	Solid green 	Off 	Solid red bright 	Solid green 	Solid red dim 	Solid red bright 
Repeater and Endpoint linked to Gateway, Endpoint sending data to Gateway	Solid green  RCV data or Solid red bright 	Solid red dim 	Intermittent flash red 	Solid green 	Intermittent flash red 	Solid red bright 	Solid green 	Solid red bright 	Solid red bright 
Gateway with diagnostics program running	Solid red bright 	Solid red dim 	Intermittent flash red 	Solid green 	Intermittent flash red 	Solid red bright 	Solid green 	Solid red bright 	Solid red bright 

* in an idle condition, the CTS LED is solid red  with a solid link, as the link weakens the CTS LED on the Repeater and Endpoint begins to blink 

2. Set Up and Program Radios

This section provides details about setup, programming, and defining who has access to the FGR2-P, -PE, & -PE-U PLUS Radios using the available setup tools. This information is included:

- [Basic Steps to Programming the FGR2-P, -PE, & -PE-U PLUS Radios \(on page 23\)](#)
- [Powering the FGR2-P, -PE, & -PE-U PLUS Radio \(on page 24\)](#)
- [Identify and Change the FGR2-P, -PE, & -PE-U PLUS Radio's IP Address \(on page 24\)](#)
- [Configuration Tool Options \(on page 25\)](#)
- [Accessing the Configuration Windows \(on page 27\)](#)
- [Navigating the Configuration Windows \(on page 29\)](#)
- [Providing Site Information \(on page 32\)](#)
- [Use the MultiPoint Gateway to Change All Connected Radios \(on page 33\)](#)
- [Creating User Logins \(on page 36\)](#)
- [Upgrading the FGR2-P, -PE, & -PE-U PLUS Radio Software Using a TFTP Server \(on page 41\)](#)
- [Resetting Radios to the Factory Default Settings \(on page 49\)](#)

2.1. Basic Steps to Programming the FGR2-P, -PE, & -PE-U PLUS Radios

This basic procedure programs any FreeWave PLUS Radio.

1. Determine or set the radio's IP address.

Note: The PLUS radio can be programmed using the terminal menu available through the radio's serial port without having to know the radio's IP address.

2. Be familiar with the network and know if it is a Point-to-Point (PTP) or Point-to-MultiPoint (PTMP) configuration.

Note: Most FreeWave networks are PTMP.

3. Open the radio's [Configuration Windows](#).
4. Set the radio's operation mode (e.g., Gateway, Repeater, or Endpoint).
5. Set the radio's network type (PTP or PTMP).
6. Program the radio, verifying all devices in a PTMP network have the same settings for these parameters:
 - Frequency Key
 - Max Packet Size
 - Min Packet Size
 - Network ID
 - RF Data Rate
7. Setup the Call Book if the radio is in a network NOT using **Network IDs**. See the [Call Book window \(on page 158\)](#).

FREEWAVE Recommends: While the Call Book is an option in Point-to-MultiPoint networks, FreeWave strongly recommends using the **Network ID** feature in most applications. If a large MultiPoint network is implemented using the Call Book and a radio needs to be added or replaced in the network, each radio **MUST** be physically reprogrammed in the network and the new serial number entered in the radio's Call Book. This can be a time consuming process and can cause a delay in getting the network back up and running.

Note: If using a **Network ID**, see the **Network ID** and **Subnet ID** parameters described in the [Radio Settings \(on page 82\)](#).

2.1.1. PTMP Network Considerations

Planning is important when installing PTMP networks. A PTMP network requires that several parameters are set consistently on ALL radios in the network. This includes:

- Frequency Key.
- Min and Max Packet Size.
- Network ID.
- RF Data Rate.

Important! If several independent, PTMP networks are located in close proximity, it is very important to include as much frequency and time diversity as possible using different **Frequency Key** and **Min and Max Packet Sizes**.

2.2. Powering the FGR2-P, -PE, & -PE-U PLUS Radio

Connect the FGR2-P, -PE, & -PE-U PLUS Radio to a positive DC power supply with +6.0 to +30.0 VDC (typically, +12 VDC).

The power supply used MUST provide **more** current than the amount of current drain listed on the [FGR2-P, -PE, & -PE-U Technical Specifications \(on page 196\)](#) for the voltage used.

Example: When using +12 VDC, the power supply must provide current capability greater than the drain that is required for transmit or greater than 550 mA.

Note: For any application where the radio is used in a UL-controlled environment, the power supply MUST be a Class 2 power source. Using a dedicated power supply line is preferred.



Warning! If the power supply is above approximately +18 to +20 VDC, use a 1 ohm resistor in line with B+ input to the radio.



Warning! If the power supply line runs outside the enclosure, use electrostatic discharge (ESD) protectors to protect the radio from electric shock and transient voltage suppressors (TVS) to protect from an over-voltage situation. Using both helps to ensure long-term, reliable operation.

2.3. Identify and Change the FGR2-P, -PE, & -PE-U PLUS Radio's IP Address

Note: In software versions 2.26 and later, the FGR2-P, -PE, & -PE-U PLUS radio can be programmed through the radio's COM1 port without having to know the radio's IP address.



It is good practice to identify the IP addresses of all the devices in the network and verify each is unique.

- The FGR2-P, -PE, & -PE-U PLUS Radio's default IP address is 192.168.111.100.
- The default user name is **admin**.
- The default password is **admin**.



Caution: Each radio in the network MUST have its own unique IP address. Putting multiple devices with the same IP address on the same network can cause network problems.

2.4. Configuration Tool Options

After the Ethernet address is identified and changed on the FGR2-P, -PE, & -PE-U PLUS radio, use the [Configuration Windows](#) setup tools to configure the radio.

A Web browser must be installed on the computer to access the [Configuration Windows](#).

Note: See [Accessing the Configuration Windows](#) on page 27.

Example: To setup a serial port, access all the parameters for the first serial port in the **Serial Setup 1** window.

Window	Used To
Status window	View all device status information. Note: See Viewing Radio Status and Statistics on page 129.
IP Setup window	Use to identify and configure the IP address, Subnet Mask, and Default Gateway. Important! Consult with the Network Administrator before changing these settings. Note: See IP and Network Communication Settings on page 51.

Window	Used To
Serial Setup window (Serial Setup 2)	Use to identify and configure the port numbers and data settings for each serial port. <div data-bbox="545 359 1365 464" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Important! These settings MUST match the device to which each port is connected.</p> </div> <div data-bbox="545 485 1365 552" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See Serial Port Settings on page 64.</p> </div>
Radio Setup window	Use to identify and configure the radio's: <ul style="list-style-type: none"> • Operation Mode. • Transmission Characteristics. • MultiPoint Parameters. • Call Book. <div data-bbox="545 789 1365 856" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See Radio Settings on page 82.</p> </div>
Security window	Use to identify and configure the: <ul style="list-style-type: none"> • RADIUS server authentication. • MAC filtering. • AES Encryption information. <div data-bbox="545 1052 1365 1119" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See Security Settings on page 102.</p> </div>
SNMP window	Use to identify and configure the SNMP management features of the radio. <ul style="list-style-type: none"> • The radio supports SNMP versions 1, 2, and 3. • All of the SNMP-manageable objects for FreeWave's radios are contained in a single MIB file. • See Object List for FREEWAVE-TECHNOLOGIES-MIB on page 201. <div data-bbox="545 1381 1365 1486" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: This file is available from FreeWave upon request. See SNMP Settings on page 117.</p> </div>
Diagnostics window	Use to view this information: <ul style="list-style-type: none"> • Signal level • Noise level • Signal-to-noise delta • Receive rate for each frequency available to the radio. <div data-bbox="545 1724 1365 1791" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: See Viewing Radio Status and Statistics on page 129.</p> </div>

Window	Used To
Users window	Use to add or change logins for the radio. <ul style="list-style-type: none"> • A maximum of nine (9) custom users can be created for each radio. • The admin user is the permanent 10th user. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: See Creating User Logins on page 36.</p> </div>
Tools window	Use to edit the site information and upgrade the radio's Software. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: In a MultiPoint Gateway, use to enable the Global Change functionality.</p> </div>

2.5. Accessing the Configuration Windows

Each FGR2-P, -PE, & -PE-U PLUS Radio includes [Configuration Windows](#) to identify, change, and program its settings.

Note: See [Configuration Windows](#) for detailed information.

- A Web browser must be installed on the computer to access the [Configuration Windows](#).
- The router / switch and/or the computer accessing the radio must be on the same subnet.

If the Subnet Mask for the network is 255.255.255.0, the first three octets, or sections, of the IP address on the radio and the IP address on the computer **MUST** match. The last octet is unique.

Example: If the subnet mask is 255.255.255.0 and the radio's IP address is 198.168.111.100, then the computer must have an IP address that begins with 198.168.111. The last section of the IP address is unique to identify the device.

Administrator Login and Password


- The default **User Name** for the administrator login is **admin**.
- The default **Password** is **admin**.

Note: The administrator login has full permission to change all settings on the radio, including upgrading software.

Guest Login and Password

- The default **User Name** for the guest login is **guest**.
- The default **Password** is **guest**.
- The guest login can view the settings but **CANNOT**:
 - save any changes.
 - view the [Security window \(on page 163\)](#).

- view the [Tools window](#) (on page 178).
- reboot the radio.

Note: The  button is not available to **Guest** users.

Procedure

1. Connect the FGR2-P, -PE, & -PE-U radio's Ethernet port to either a computer or a router / switch.
2. Apply power to the radio.
3. Open a web browser.
4. Enter the IP address of the radio into the address bar.

Note: The default IP address is 192.168.111.100.

Example: Enter **192.168.111.100** in the address bar of the web browser to access a radio with that IP address.

5. Refresh the browser window.
The **Authentication Required** dialog box opens.
6. Enter the **User Name** and **Password** to access the radio.

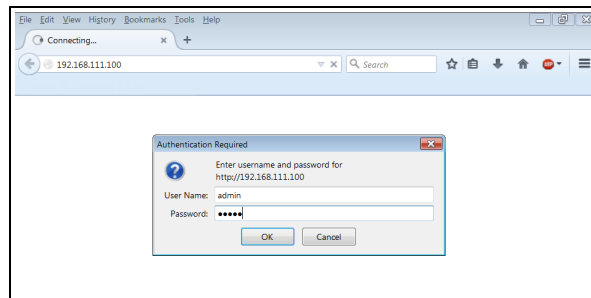


Figure 4: Authentication Required dialog box

7. Click **OK**.
The [Status window](#) opens.

FREEWAVE		D2+	
		192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525	
		'admin' From 192.168.111.1	
Status	Hardware Information		
IP Setup	Firmware Version	3.01.15 Dec 2 2014	
Serial Setup 1	Wireless Version	+8.80a	
Serial Setup 2	Software Boot Version	3	
Radio Setup	Hardware Version	1	
Security	Country Code	FFFF	
SNMP	Uptime	0 days 0 hours 13 minutes 41 seconds	
Diagnostics	RF Stats		
Users	Connected To	0	
Tools	Signal	0	
	Noise	0	
	Upstream signal	0	
	Upstream Noise	0	
	Voltage	10.92v	
	RX Success Rate	0.00%	
	TX Success Rate	0.00%	
	Reflected Power	0	
	Disconnect Count	0	
	Temperature	~31°C ~ 88°F	
	Distance	~0 meters or 0.0 miles	
	Packet Stats		
	Received	0 packets - 0 Bytes	
	Packets Sent	45 packets - 8140 Bytes	
	Packets Dropped	353	
	RF Packets Skipped	0	
	RF Buffer Overflow Skip	0	
	Bad Packets	0	
	Un-Ackd Packets	0 (0.00%)	
	Broadcast Packets	0 (0.00%)	
	Radio Addressed Packets	3 (6.67%)	
	Radio Parse Error	0	
	RX Throughput	0.00 kbps - 0.00 avg/min	

Figure 5: FGR2-P, -PE, & -PE-U Status window

2.6. Navigating the Configuration Windows

2.6.1. Menu bar

The [Configuration Windows](#) group the parameters into the **Menu** bar on the left side of all windows.

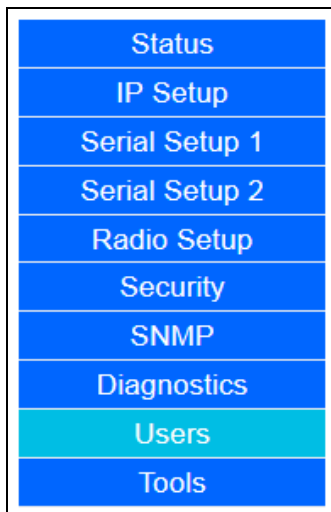
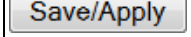


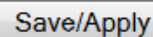
Figure 6: Menu bar

- Click any item in the **Menu** bar to open that **Configuration** window.
- The currently selected window is highlighted in the **Menu** bar.

2.6.2. Save and Apply

When making changes to the radio settings, click the  button before navigating away from a window or rebooting the radio to save the changes.

Important!: No changes take effect until you click



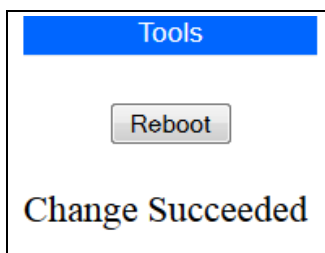






Figure 7: Change Succeeded message

- When the changes have been successfully saved and applied, the **Change Succeeded** message appears under the  button.

Serial Settings	
Baud Rate	1200
Data Bits	8
Parity	None

Figure 8: Changed Baud Rate before  is clicked.

- Any change made in the [Configuration Windows](#) that is not yet saved is highlighted in yellow.
- This highlight indicates that you need to click  before navigating away from the page, or the changes will be lost.
- Some setting changes (e.g., changes to the IP Setup) require a reboot to complete the changes.
- When such a change is made, the **Change Succeeded** message below the  button changes to include a link labeled **Reboot Required**.

2.6.3. Reboot


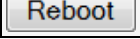
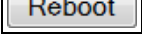
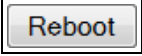
Tools

Change Succeeded Reboot Required

Figure 9: Reboot Required message

Note: The  button is not available to **Guest** users.

- Below the **Menu** bar is the  button. Click this button to force the radio to reboot.
- Click either the **Reboot Required** link or the  button to reboot the radio and apply the requested changes.

Important! The requested changes are NOT made until the radio is rebooted.

Note: A **Reboot Required** link appears at the top of every page until the radio is rebooted.

2.7. Providing Site Information

For each radio in the network, information to help identify that FGR2-P, -PE, & -PE-U PLUS radio (i.e., name and contact information) can be provided. The site information appears on the [Status window on page 175](#).

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu** bar, click **Tools**.
The [Tools window](#) opens.

Figure 10: FGR2-P, -PE, & -PE-U Tools window

Important! On the FGR2-P, -PE, & -PE-U radios, the **Modem Mode** list box on the [Radio Setup window on page 156](#) must be set to Gateway for the

ENABLE Global Change Functionality

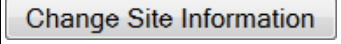
button to be visible.

3. In the **Change Site Information** area:

Important! Free form text fields CANNOT use any of these characters: % & + = < >

- a. In the **Site Name** text box, enter a maximum of 25 characters to help identify the radio.
- b. In the **Site Contact** text box, enter a maximum of 25 characters about who to contact about the site's status.
- c. In the **System Name** text box, enter a maximum of 32 characters to identify the system the radio operates in.
- d. In the **Notes** text box, enter a maximum of 50 characters to describe the radio or the

site.

4. Click  to save the changes.

2.8. Use the MultiPoint Gateway to Change All Connected Radios

Important! The **Global Change** function can ONLY be enabled or disabled using the [Configuration Windows](#).

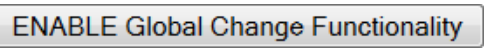
Often, the settings on radios in the network should be the same as the settings in the MultiPoint Gateway. Instead of changing each radio individually, use the **Global Change** function to push the **IP Setup**, **Radio Setup**, **Security**, **SNMP**, and **User** settings to all connected radios in the network.

Important! The **Global Change** can only be successfully performed if the Endpoint or Repeater radio is linked wirelessly to the Gateway.

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click **Tools**.
The [Tools window](#) opens.

Figure 11: FGR2-P, -PE, & -PE-U Tools window

Important! On the FGR2-P, -PE, & -PE-U radios, the **Modem Mode** list box on the [Radio Setup window on page 156](#) must be set to Gateway for the

 button to be visible.

3. Click 

The button changes to 

Note: Click that button to turn off global changing.

When enabled, the **All Changes to All Radios** message appears.

WARNING!!! Changes Will Be Applied To all RF Connected Radios From Their Point-Of-View!


Figure 12: All Changes to All Radios message

- On the Gateway, the **Push Globally** button replaces the **Save/Apply** button on the windows that allow global changes.
- Click **Push Globally** to send any changes made to the parameters on that window are sent to all the connected radios.
- Every connected radio that receives the changes reboots after the changes are applied.
- The [Configuration Windows](#) on the remote radios are not accessible until the reboot completes.

Note: The settings on the MultiPoint Gateway are NOT changed during a global change.

When the Global Change functionality is enabled, these changes occur in these windows:

Global Functionality Changes	
Window	Description
IP Setup window	<ul style="list-style-type: none"> • The IP Address text box is hidden. • It cannot be part of a global change.
Radio Setup window	<ul style="list-style-type: none"> • The Network Type and Modem Mode list boxes are hidden. • They do NOT change as part of a global change. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important!: Changes made to the settings on the Radio Setup window can cause the radios to lose communication with the Gateway and/or MultiPoint Repeaters. Use caution when making global changes.</p> </div>

Global Functionality Changes	
Window	Description
Security window	<ul style="list-style-type: none"> All settings on the Security window can be part of a global change. <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;">  <p>Caution: When changing the AES Encryption Key globally, make the first change on the MultiPoint Gateway. After the Gateway has been changed, push the new key to the other radios in the network. If this is not done in this order, changing the encryption key can cause radios to lose connectivity with the Gateway for an extended period of time.</p> </div>
SNMP window	<ul style="list-style-type: none"> All settings on the SNMP window can be part of a global change.
Users window	<ul style="list-style-type: none"> The Edit Group Level Rights area and the User Accounts Level can be adjusted using global changes. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important!: User accounts and User passwords CANNOT be created or deleted using global changes.</p> </div>

2.9. Creating User Logins

To limit who can access the FGR2-P, -PE, & -PE-U PLUS Radios in the network and edit configuration settings, a maximum of nine (9) custom users with login access can be created.

Note: The permanent **admin** login is the 10th login.

Procedure

1. [Defining User Groups on page 36.](#)
2. [Editing User Group Rights on page 37.](#)
3. [Add and Delete Users on page 38.](#)
4. [Changing User Passwords on page 40.](#)

2.9.1. Defining User Groups

User groups set the access rights for the [Configuration Windows](#) for a radio. Users are assigned to one of three Groups and inherit the access rights that are set for that Group.

There are three pre-defined Groups (Groups 1, 2, and 3).

Note: Additional Groups cannot be added.

In each group, assign one access level to each page or tab:

- **No Access** - Users cannot see the settings in the tab or page.
 - Any attempt to navigate to the tab or page shows an **Access Denied** message.
- **Read Only** - Users can see the settings in the tab or page, but cannot save or apply any changes.
- **Full Access** - Users are able to see the settings in the tab or page and can save and apply changes.

When a user is created it is assigned to a group. The group number corresponds to the user group and the user inherits the permissions assigned to that group.

Example: If Group 1 has **Read Only** access to the IP Setup parameters and **No Access** to the **Security** parameters, any user assigned to Group 1 can view IP Setup parameters but not make changes, and receives an Access Denied message if they try to access the [Security window on page 163](#).

Note: The group assigned to the admin user cannot be changed.
The admin user always has **Full Access** to all pages.

2.9.2. Editing User Group Rights


1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click **Users**.
The [Users window](#) opens.

D2+
192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
'admin' From 192.168.111.1

User Accounts			
	Level		
admin	0		
guest	3		
Add User			
Edit Group Level Rights			
Level	1	2	3
IP Setup	Read Only	Read Only	Read Only
Serial Setup	Read Only	Read Only	Read Only
Radio Setup	Read Only	Read Only	Read Only
Security	No Access	No Access	No Access
SNMP	Read Only	Read Only	Read Only
RMS	Read Only	Read Only	Read Only
Tools	No Access	No Access	No Access

©2006-2014 FreeWave Technologies, Inc.

Figure 13: FGR2-P, -PE, & -PE-U Users window

3. In the **Edit Group Level Rights** area, click the list box arrow for each group and select the access rights for each window.
4. Click  to save the changes and apply them to the radio.

2.9.3. Add and Delete Users

A maximum of nine (9) custom users with login access can be created to limit who can access the FGR2-P, -PE, & -PE-U PLUS Radios in the network and edit configuration settings.

Important! Users can only be created and edited using the [Configuration Windows](#).

Note: The permanent **admin** login is the 10th login.

Adding a User

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click **Users**.
The [Users window](#) opens.

The screenshot shows the FreeWave web interface. At the top, it displays the device information: D2+, IP 192.168.111.100, MAC=00:07:E7:82:B6:FD, and Serial#=8566525. Below this is a navigation menu on the left with options like Status, IP Setup, Serial Setup 1, Serial Setup 2, Radio Setup, Security, SNMP, Diagnostics, Users, and Tools. The main content area is titled 'User Accounts' and shows a table with columns for Level, and a list of users: 'admin' with level 0 and 'guest' with level 3. There is an 'Add User' link and a green plus button. Below the user list is an 'Edit Group Level Rights' table with columns for Level (1, 2, 3) and rows for various settings like IP Setup, Serial Setup, Radio Setup, Security, SNMP, RMS, and Tools. A 'Reboot' button is visible on the left, and a 'Save/Apply' button is at the bottom of the main content area. The footer indicates copyright from 2006-2014 FreeWave Technologies, Inc.

Figure 14: FGR2-P, -PE, & -PE-U Users window

3. In the **User Accounts** area, click the **Add User** link or click the green plus  button.
The [Add User window](#) opens.

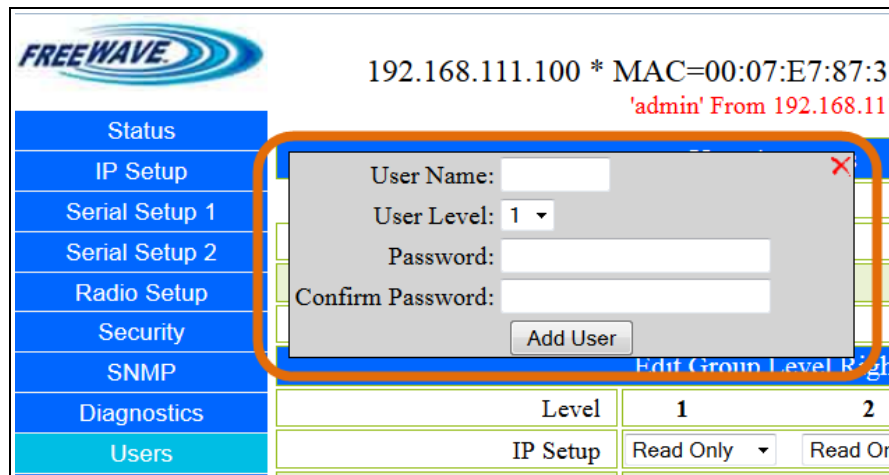


Figure 15: Add User window

4. In the **User Name** text box, enter a name that identifies the user.


Example: Enter **guest** or a user's first initial and last name.

5. Click the **User Level** list box arrow and select 1, 2, or 3 to assign the user to a group.

Note: See [Defining User Groups \(on page 36\)](#) for more information.

6. In the **Password** and **Confirm Password** text boxes, enter the user password to enter when accessing restricted windows.
7. Click **Add User** to close the **Add User** window and immediately create the new user.

Deleting a User

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu** bar, click Users.
The [Users window](#) opens.
3. In the **User Accounts** area, click the red  button next to the user to delete.



Caution: There is no confirmation message to delete the User.
The selected User is deleted immediately.

2.9.4. Changing User Passwords

Important! User Passwords can ONLY be changed in the [Configuration Windows](#).

When a user is created, they are assigned a password. This password can be changed at any time.

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click **Users**.
The [Users window](#) opens.

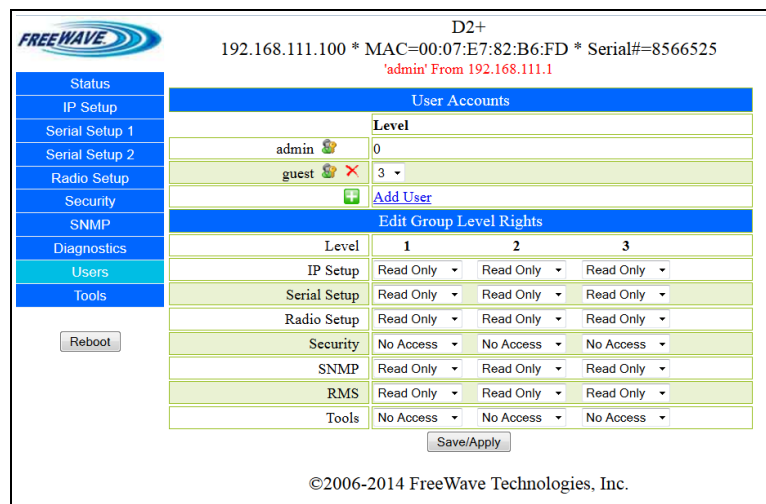



Figure 16: FGR2-P, -PE, & -PE-U Users window

2. Click the key  button next to the user to change the password.
The [Change Password window](#) opens.

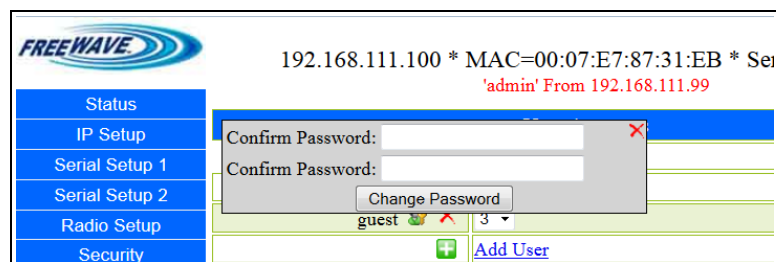
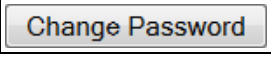


Figure 17: Change Password window

3. In the first **Confirm Password** text box, enter the new password.
4. Re-type the password in the second **Confirm Password** text box.
5. Click .
The **Change Password** window closes and the new password is saved.

2.10. Upgrading the FGR2-P, -PE, & -PE-U PLUS Radio Software Using a TFTP Server

The PLUS Radios share a common software upgrade platform and process using the FreeWave TFTP Server and a FreeWave-supplied software upgrade file. This section details the step-by-step process of upgrading software either locally (directly connected to the radio via an Ethernet cable) or over-the-air (OTA).

Upgrading software:

- does NOT change any radio settings.
- locally is much faster than if done OTA.



Caution: Only attempt an OTA software upgrade if the link is stable and of good quality. If the link is unstable or poor, the software upgrade is likely to fail.

Assumption

These instructions assume the IP address is known for the radio to upgrade and the radio's [Configuration Windows](#) are accessible. If needed, contact FreeWave Technical Support for assistance.

Note: See [Contact FreeWave Technical Support on page 12](#) for contact information.

Complete these steps to upgrade a FGR2-P, -PE, & -PE-U PLUS radio:

1. Confirm access with a TFTP server with the Network Administrator.
2. [Configuring the TFTP Server on page 42](#).
3. [Upgrading Software Using the Configuration Windows on page 43](#).
4. [Verifying Software Upgrades on page 48](#).

2.10.1. Downgrading Software



Warning! Downgrading a FGR2-P, -PE, & -PE-U PLUS Radio from the current software version to a previous software version may result in the radio settings becoming invalid.

FREEWAVE Recommends: FreeWave recommends resetting any downgraded radio to the factory defaults using the steps provided in [Resetting Radios to the Factory Default Settings on page 49](#) BEFORE attempting to use or configure the radio.

If downgrading the software version, contact FreeWave Technical Support for information. See [Contact FreeWave Technical Support on page 12](#).

2.10.2. Configuring the TFTP Server

Before Upgrading Software Using the TFTP Server

Important! Before upgrading a FGR2-P, -PE, & -PE-U PLUS Radio's software, download the specific software file and install the FreeWave TFTP Server from www.freewave.com. Contact FreeWave Technical Support for assistance. See [Contact FreeWave Technical Support \(on page 12\)](#) for contact information.

FREEWAVE Recommends: Create a folder on the computer desktop called Root and save the software file in that folder.

The FreeWave TFTP Server enables the transfer of the software file from the computer to the radio. After the FreeWave TFTP Server program is downloaded, run the installer to access the executable program, **fwTFTP.exe**.


When installation is completed, the TFTP Server can be configured.

Procedure

1. On the Windows® **Start** menu, click **All Programs > FreeWave Technologies > fwTFTP > fwTFTP.exe**.

Note: If the TFTP server is installed in another location, follow that directory path and open the **fwTFTP.exe** file.

2. When the application appears, click **Configure**.
The **Server Configuration** dialog box opens.

3. In the **Root Folder** field, click  next to the text box.

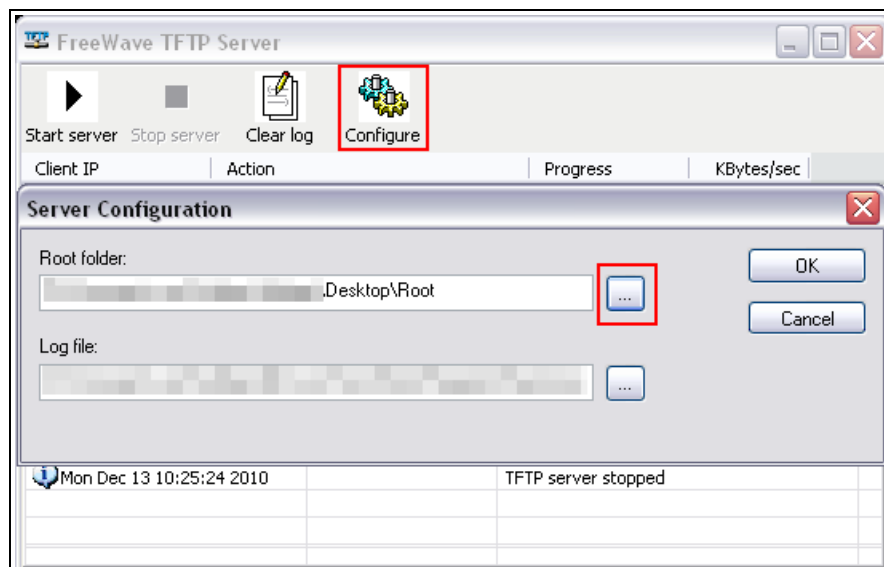


Figure 18: Server Configuration dialog box

The **Browse for Folder** dialog box opens.

4. Search for and locate the folder the software upgrade file was saved in.
5. Click **OK** and verify that the folder is listed in the **Root Folder** text box.
6. Click **OK** to return to the main **TFTP Server** window.



7. Click **Start server**.

Note: If the button and text are gray, the server is started.

8. Minimize (**do not close**) the FreeWave **TFTP Server** window and continue with [Upgrading Software Using the Configuration Windows on page 43](#).

2.10.3. Upgrading Software Using the Configuration Windows

After the FreeWave **TFTP Server** is configured, complete the software upgrade using the radio's [Configuration Windows](#).

Important! This procedure requires Windows® Explorer file extension to be visible. See the Microsoft® topic [Show or Hide File Name Extensions](#) to view the extensions.

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#). The [Status window](#) opens.
2. On the **Menu bar**, click **Tools**. The [Tools window](#) opens.

 The screenshot shows the FreeWave web interface. At the top, it displays the IP address 192.168.111.100, MAC address 00:07:E7:87:31:EB, and Serial number 8860139. A left-hand menu lists various configuration options, with 'Tools' highlighted in red. The 'Tools' section is expanded to show 'TFTP Firmware Upgrade'. This section includes a warning to 'Consult Errata Before Downgrading', a text box for 'Address of TFTP Server' containing '192.168.111.200', and a text box for 'File Name' containing 'Name Here'. A red arrow points to the 'File Name' field. Below these fields are buttons for 'Upgrade Firmware' and 'Global Firmware Upgrade'. A 'Reboot' button is also visible in the 'Tools' section. The footer of the window reads '©2006-2014 FreeWave Technologies, Inc.'

Figure 19: FGR2-P, -PE, & -PE-U Tools window

- In the **TFTP Software Upgrade** area of the window, in the **Address of TFTP Server** text box, enter the IP address of the computer the TFTP Server is installed on.

Important!: Do **NOT** enter the radio's IP address.

- In the **File Name** text box, enter the exact name of the software upgrade file saved in the **Root** directory on the computer in [Configuring the TFTP Server on page 42](#).

Example: **http3_01**

- Click .

The radio retrieves the software file from the TFTP Server.

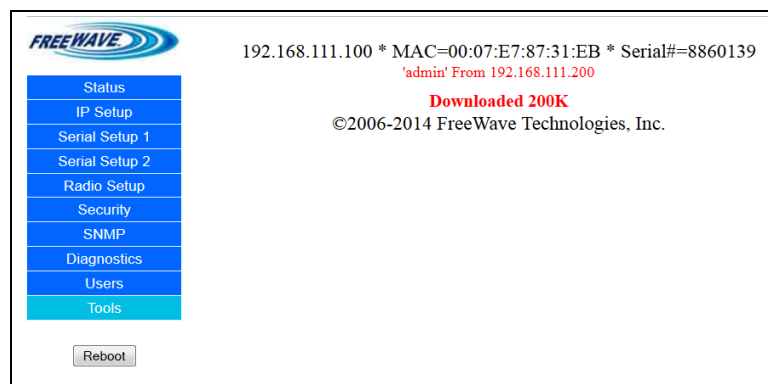


Figure 20: Downloading the upgrade

The upgrade message identifies the FLASH device when it is programming.

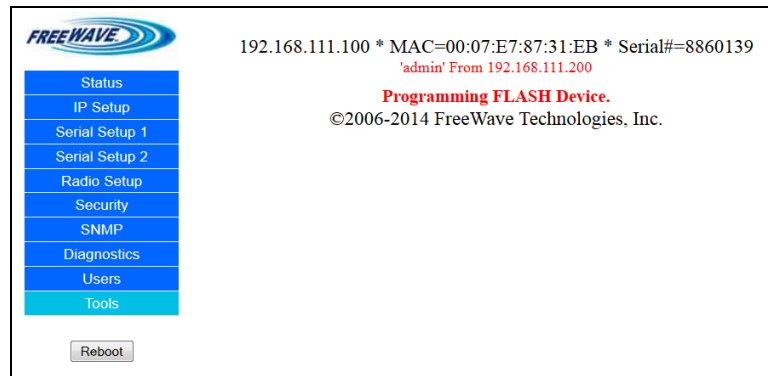


Figure 21: Programming FLASH Device

The **Reboot** message appears.

- Click to manually reboot the FGR2-P, -PE, & -PE-U PLUS Radios.

Important!: Wait for the reboot to complete.

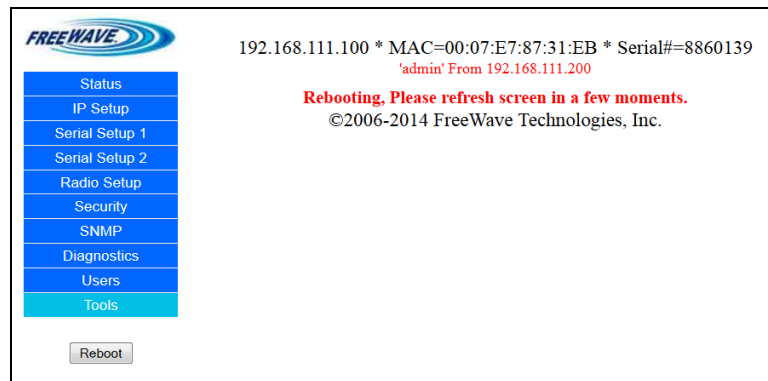


Figure 22: Reboot message

After the radio has the software upgrade and is rebooted to its previously programmed state, verify the software upgrade was successful.

7. Refresh the radio's browser window.
If applicable, re-enter the IP address of the radio into the address bar.
The **Authentication Required** dialog box opens.



If there are problems viewing the Web pages, it may be necessary to clear the Web browser cache and cookies.
This process varies depending on the Web browser.

Note: By default, this window should load when logged in.

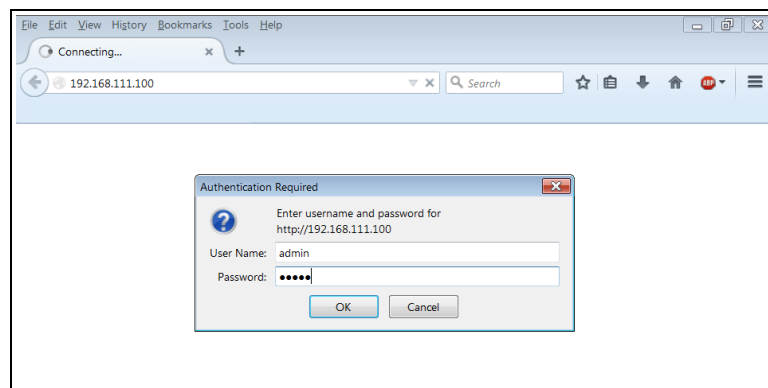


Figure 23: Authentication Required dialog box

8. Enter the **User Name** and **Password**.
9. Click **OK**.

The [Status window](#) opens.

The **Firmware Version** text box in the **Hardware Information** area of the window shows the current software version installed.

Verify this matches the upgrade software version.

FREEWAVE		192.168.111.100 * MAC=00:07:E7:87:31:EB * Serial#=8860139 'admin' From 192.168.111.200	
Status			
IP Setup	Hardware Information		
Serial Setup 1	Firmware Version	3.01.15 Dec 2 2014	
Serial Setup 2	Wireless Version	+7.71i	
Radio Setup	Software Boot Version	3	
Security	Hardware Version	1	
SNMP	Country Code	FFFF	
Diagnostics	Uptime	0 days 0 hours 2 minutes 9 seconds	
Users	RF Stats		
Tools	Last Connected To	0	
	Noise	-100	

Figure 24: FGR2-P, -PE, & -PE-U Status window with software upgrade

Verify the Radio Connection

10. Open a CLI window.
11. Type **Ping** and the **IP address** of the radio.
12. Press <Enter>.

When successful, the radio ping responds similar to:

```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

U:\>ping 192.168.111.100

Pinging 192.168.111.100 with 32 bytes of data:
Reply from 192.168.111.100: bytes=32 time=5ms TTL=64
Reply from 192.168.111.100: bytes=32 time=2ms TTL=64
Reply from 192.168.111.100: bytes=32 time=2ms TTL=64
Reply from 192.168.111.100: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.111.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms

U:\>

```

Figure 25: Ping CLI window

2.10.4. Upgrade FGR2-P, -PE, & -PE-U PLUS Software Globally

Important! If a beta version of the v2.23 software is running, you must use the TFTP upgrade process for any Slave in the network to upgrade it to the v2.23 general release. Do **NOT** use the Global Software Update functionality. Using the Global Update can pin the software version to the radio, requiring an RMA for the affected device. After the radio has been updated to the general release using the TFTP upgrade method, it is safe to use the Global Update functionality for future upgrades.

Upgrade the software to all connected FGR2-P, -PE, & -PE-U PLUS Radios of the same type using the **GLOBAL Software Upgrade** option. The Gateway sends a copy of the software update in 1 KB sections to all connected Endpoints and MultiPoint Repeaters.

- Each radio must successfully receive every section, or it will not upgrade its software.
- Increasing the **Broadcast Repeat** setting increases the probability of success, but slows down the overall process.
- The Gateway itself is NOT upgraded during a Global Upgrade.

Note: If the **GLOBAL Software Upgrade** button is selected on an Endpoint or a MultiPoint Repeater, that individual radio is NOT upgraded. It sends the upgrade file to its Gateway, which will be upgraded. No other radios will receive the file.

Important!: This procedure requires Windows® Explorer file extension to be visible. See the Microsoft® topic [Show or Hide File Name Extensions](#) to view the extensions.

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#). The **Status** window opens.
2. On the **Menu** bar, click **Tools**. The **Tools** window opens.

Figure 26: FGR2-P, -PE, & -PE-U Tools window

3. In the **TFTP Software Upgrade** area of the window, in the **Address of TFTP Server** text box, enter the IP address of the computer the TFTP Server is installed on.

Important!: Do **not** enter the radio's IP address.

4. In the **File Name** text box, enter the exact name of the software upgrade file saved in the **Root** directory on the computer in [Configuring the TFTP Server \(on page 42\)](#).

Example: [http3_01](#)

5. Click **Global Firmware Upgrade**.

- Radios that successfully receive the software upgrade load the file to memory, and then reboot.
- The reboot times are randomized within a short window, to keep every radio from restarting at the same time.

Note: If a remote radio's configuration page is accessed while it is rebooting, an error appears.

6. See [Verifying Software Upgrades \(on page 48\)](#).

2.10.5. Verifying Software Upgrades

After the radio has taken a software upgrade and rebooted to its previously programmed state, verify the software upgrade was successful.

1. Refresh the radio's browser window or opening a new session.



If there are problems viewing the Web pages, it may be necessary to clear the Web browser cache and cookies.
This process varies depending on the Web browser.

2. On the **Menu** bar, click **Status**.
The [Status window](#) opens.

FREEWAVE		192.168.111.100 * MAC=00:07:E7:87:31:EB * Serial#=8860139 'admin' From 192.168.111.200	
Status	Hardware Information		
IP Setup	Firmware Version	3.01.15 Dec 2 2014	
Serial Setup 1	Wireless Version	+7.71i	
Serial Setup 2	Software Boot Version	3	
Radio Setup	Hardware Version	1	
Security	Country Code	FFFF	
SNMP	Uptime	0 days 0 hours 2 minutes 9 seconds	
Diagnostics	RF Stats		
Users	Last Connected To	0	
Tools	Noise	-100	

Figure 27: FGR2-P, -PE, & -PE-U Status window with software upgrade

The **Firmware Version** text box in the **Hardware Information** area of the window shows the current software version installed.

Verify this matches the upgrade software version.

Note: By default, this window should load when logged in.

2.10.6. Common Software Upgrade Issues and Solutions

"File Not Found" in either the Configuration Windows or the FreeWave TFTP Server

- Verify the file name of the software upgrade file is **exactly** as the file is named.
- If still unsuccessful, check the extension of the file.

Note: If the computer does not show file name extensions, see the [Microsoft®](#) topic [Show or Hide File Name Extensions](#) to view the extensions.

Software Upgrade Times Out

- Verify:
 - the connection is to the proper IP address.
 - the radio is powered on.
- If you are able to access the [Configuration Windows](#), but the software upgrade times out, verify the FreeWave TFTP Server is configured properly and is started.

Software Upgrading is Taking a Long Time to Complete

- If the software upgrade is being done over-the-air, it can take a significant amount of time to complete the file transfer.
- This time can be extended if the quality of the link is poor.

FREEWAVE Recommends: Only attempt an over-the-air software upgrade with links that are stable and of high quality.

2.11. Resetting Radios to the Factory Default Settings

Note: For a list of factory defaults, see [Factory Default Settings \(on page 191\)](#).

1. Access the terminal menu.

Note: For more information, see [Identify and Change the FGR2-P, -PE, & -PE-U PLUS Radio's IP Address \(on page 24\)](#).

2. With the terminal session open, connect power to the radio.
3. Type **Y** to access the IP setup of the radio.
After entering a **Y**, the radio's serial number, software and wireless versions, and login prompt appear.

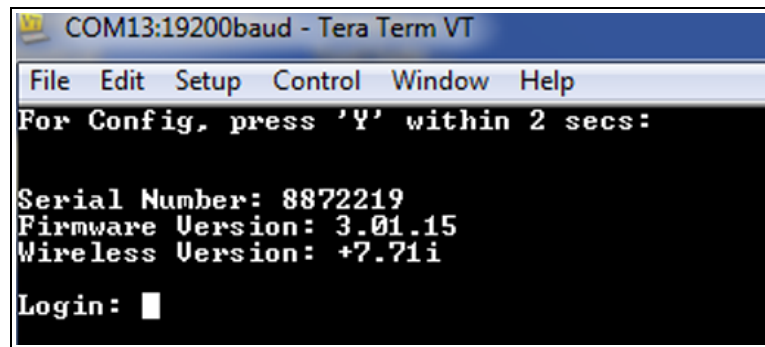


Figure 28: Example: Tera Term VT window

4. Enter **default** at the prompt and press <Enter>.
The radio reboots, and all of the radio settings are reset to the factory defaults.

3. IP and Network Communication Settings

The parameters on the **IP Setup** tab or the [IP Setup window](#) are typically changed by a Network Administrator. These are the parameters that set the Ethernet address and other communications for the radio.

Note: Use the [IP Address \(on page 53\)](#) to change the IP and network communication settings using the Terminal Menu.

In the **IP Setup** window, these are the available parameters:

- **LAN Network Interface Configuration (Management)** - The local area network (LAN) settings.
- **VLAN Configuration (Data)** - The virtual local area network (VLAN) settings.
 - A VLAN is a group of devices with a common set of requirements that communicate as if they were attached to the same domain, regardless of their network location.

Note: Not every network needs or uses VLAN IDs.
The **VLAN Mode** setting is typically set to **Disabled**.
Changes to VLAN settings should be approved by a network administrator.

- **NTP Client** - The Network Time Protocol (NTP) settings.
 - The device with the IP address entered here is the device that the radios in the network use to synchronize their internal clocks.
- **Syslog Server** - The system logging settings.
 - Enabling and setting IP addresses in the system server settings instructs the radio to send all its log entries to a system server.

Note: For more information, see [Viewing the System Log \(on page 103\)](#).

3.1. IP Setup Parameter Reference

This section contains the IP setup parameters.


Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.

3.1.1. Default Gateway

Default Gateway	
Setting	Description
Web Parameter:	Default Gateway text box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (2) Default Gateway
Network Type:	Both
Default Setting:	192.168.111.1
Options:	Any valid IP address.
Description:	<p>The IP address for the appropriate default Gateway. A network administrator typically sets this parameter.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Putting multiple devices on the network with the same IP address can cause network problems.</p> </div>

3.1.2. IP Address

Important! If using the configuration Web pages, the system does not validate that the entered IP address is in the correct 0.0.0.0 format.
Verify the entered IP address before sending the setting to the radio.

IP Address	
Setting	Description
Web Parameter:	IP Address text box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (0) IP Address
Network Type:	Both
Default Setting:	192.168.111.100
Options:	Any valid IP address.
Description:	<p>This is the IP address assigned to the radio.</p> <ul style="list-style-type: none"> Each radio in the network is assigned a unique IP address. The IP address for each radio must in the proper subnet. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: It is possible to have a transparent bridge with an IP address of 255.255.255.255, but serial port functionality, the Security features, and access to the configuration Web pages is lost.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p> Caution: Putting multiple devices with the same IP address on the same network can cause network problems.</p> </div> <ul style="list-style-type: none"> When the VLAN Mode (on page 61) parameter is set to Tagged or Untagged, this IP information is assigned to the Management portion of the radio (Setup pages, SNMP, and Discovery Server). Any communication with the radio's Web pages, SNMP, or changes made using the Discovery Server need to be: <ul style="list-style-type: none"> addressed to this IP address and tagged with the address in the Management VLAN ID (on page 60) parameter. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: This parameter is hidden in the Configuration Windows when Global Changes are enabled. For more information about making global changes, see Use the MultiPoint Gateway to Change All Connected Radios (on page 33).</p> </div>

3.1.3. MTU

FREEWAVE Recommends: Leave this setting at its default of 1500 bytes unless networks are run back-to-back using VLAN tagging (802.1Q trunking, specifically).

MTU	
Setting	Description
Web Parameter:	MTU text box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153) ..
Terminal Menu:	(1) IP Setup > (5) MTU
Network Type:	Both
Default Setting:	1500 bytes
Options:	0 to 1500 bytes
Description:	<p>The Maximum Transmission Unit (MTU) is the largest data unit that the radio can pass via the Ethernet port.</p> <ul style="list-style-type: none"> For TCP, the MTU is the size at which the radio fragments the request into multiple TCP packets which must be assembled on the remote side for receipt. TCP guarantees complete in-order delivery of traffic where possible. The radio attempts to retry sending the packet, with a timeout for each try. The radio tries to send portions of the packet or the whole packet if the packet's size is within the MTU size for each packet sent. If pings go through the network but data traffic does not reliably go through, verify this setting is one to three times the size of what the Maximum Packet Size parameter setting is for the radio. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>FREEWAVE Recommends: With VLANs and some other specific configurations, TCP/IP traffic can periodically time out over links unless the MTU parameter is adjusted to be lower than the 1500 byte default value, with the networks also adjusted accordingly. FreeWave recommends starting with 1400 bytes in this scenario.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Important! If the MTU setting is changed, the setting must be changed to match on all devices within the network.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px; background-color: #ffffcc;"> <p>Caution: Changing this parameter may lead to network instability. Contact FreeWave Technical Support for guidance about changing this parameter from the default 1500 bytes. See Contact FreeWave Technical Support on page 12.</p> </div>

3.1.4. NTP Client Enable

NTP Client Enable	
Setting	Description
Web Parameter:	Enable check box in the NTP Client area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (D) NTP Client
Network Type:	Both
Default Setting:	Disabled
Options:	Disabled, Enabled
Description:	<p>Enables the Network Time Protocol (NTP) client on the radio.</p> <ul style="list-style-type: none"> The radio checks with the NTP Server specified in the NTP IP Address (on page 55) parameter and sets its internal clock to the time and date specified by the NTP server. The radio checks with the NTP server on its initial startup, and then periodically checks the server to ensure its internal clock is still in sync. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>FREEWAVE Recommends: Test the connectivity to the NTP server and its response to NTP requests. If the radio is unsuccessful connecting to the NTP server upon booting, it makes a new request to the server before every log file entry, which can cause unnecessary network traffic.</p> </div>

3.1.5. NTP IP Address

NTP IP Address	
Setting	Description
Web Parameter:	IP Address text box in the NTP Client area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (E) NTP IP Address
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid IP address.
Description:	<p>This is the IP address of the NTP server.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: If the NTP Client parameter is enabled, the radio checks with this IP address upon startup to set its internal clock.</p> </div>

3.1.6. Push to (Syslog) Server

FREEWAVE Recommends: This setting is best setup using the [Configuration Windows \(on page 151\)](#).

Push to (Syslog) Server	
Setting	Description
Web Parameter:	Push to Server check box in the Syslog Server area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (F) Syslog Server
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enabling this option instructs the radio to send its log entries to the system logging server identified in the Syslog Server 1 (on page 58) and Syslog Server 2 (on page 58) text boxes.

3.1.7. Spanning Tree

Spanning Tree	
Setting	Description
Web Parameter:	Spanning Tree Enable check box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (4) Spanning Tree
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled

Spanning Tree	
Setting	Description
Description:	<p>Enabling this parameter causes a Gateway to use the Spanning Tree Protocol (IEEE 802.1D).</p> <ul style="list-style-type: none"> This protocol eliminates the possibility of the radios creating a network loop, which can cause network-wide problems. Spanning Tree Protocol uses radio bandwidth, as any Spanning Tree radios are constantly communicating their network location. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Some network devices (e.g., switches and routers), disable a connection to a device that uses the Spanning Tree Protocol. Prior to enabling this setting, verify that all network devices work with the Spanning Tree Protocol.</p> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>FREEWAVE Recommends: Leave Spanning Tree disabled, unless the Spanning Tree Protocol is required.</p> </div>

3.1.8. Subnet Mask

Subnet Mask	
Setting	Description
Web Parameter:	Subnet Mask text box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (1) Subnet Mask
Network Type:	Both
Default Setting:	255.255.255.0
Options:	Any valid net mask address in the network.
Description:	<p>Used to route data in a sub-network.</p> <ul style="list-style-type: none"> Devices in the same sub network must have addresses in the same subnet to successfully communicate. A Network Administrator typically sets this parameter. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: If the default Subnet setting of 255.255.255.0 is used, all devices within the network MUST have addresses where the first three sections of the address match, but the last section is unique.</p> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px; background-color: #e6f2ff;"> <p>Example: Addresses 10.0.1.201 and 10.0.1.202 are in the same subnet, but 10.0.2.201 is not included in the subnet. If the subnet mask is set to 255.255.0.0, then only the first two sections must be unique.</p> </div>

3.1.9. Syslog Server 1

Syslog Server 1	
Setting	Description
Web Parameter:	Syslog Server 1 text box in the Syslog Server area of the IP Setup window on page 153 .
Terminal Menu:	(1) IP Setup > (G) Syslog Server 1 IP
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid IP address.
Description:	<p>This is the primary IP address of the system log server.</p> <ul style="list-style-type: none"> • If system logging is enabled, the radio sends all log entries to the IP address entered in this text box. • The radio sends logs to both server entries, Syslog Server 1 and Syslog Server 2, concurrently.

3.1.10. Syslog Server 2

Syslog Server 2	
Setting	Description
Web Parameter:	Syslog Server 2 text box in the Syslog Server area of the IP Setup window on page 153 .
Terminal Menu:	(1) IP Setup > (H) Syslog Server 2 IP
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid IP address.
Description:	<p>This is the IP address of a second system log server.</p> <ul style="list-style-type: none"> • If system logging is enabled, the radio sends all log entries to the IP address entered in this text box. • The radio sends logs to both server entries, Syslog Server 1 and Syslog Server 2, concurrently. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important! If a second server does not exist, enter 0.0.0.0.</p> </div>

3.1.11. Data VLAN ID



Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance. Incorrect settings can cause devices in the network to lose communication. See [Contact FreeWave Technical Support \(on page 12\)](#).

Data VLAN ID	
Setting	Description
Web Parameter:	Data VLAN ID text box in the VLAN Configuration (Data) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (B) Data VLAN ID
Network Type:	Both
Default Setting:	0
Options:	Any valid VLAN ID between 1 and 4095.
Description:	<ul style="list-style-type: none"> Data using this VLAN ID is allowed to: <ul style="list-style-type: none"> come into or be sent out of the radio's local Ethernet port. access the serial ports via the terminal server.

3.1.12. VLAN Default Gateway



Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance. Incorrect settings can cause devices in the network to lose communication. See [Contact FreeWave Technical Support \(on page 12\)](#).

VLAN Default Gateway	
Setting	Description
Web Parameter:	Default Gateway text box in the VLAN Configuration (Data) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (9) Data Default Gateway
Network Type:	Both
Default Setting:	192.168.111.1
Options:	Any valid IP address.
Description:	<p>The IP address for the appropriate default Gateway for the Data VLAN IP address.</p> <p>A network administrator typically sets this parameter.</p>

3.1.13. VLAN IP Address



Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance. Incorrect settings can cause devices in the network to lose communication. See [Contact FreeWave Technical Support \(on page 12\)](#).

VLAN IP Address	
Setting	Description
Web Parameter:	IP Address text box in the VLAN Configuration (Data) area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (7) Data IP Address
Network Type:	Both
Default Setting:	192.168.111.100
Options:	Any valid IP Address.
Description:	When the VLAN Mode is set to Tagged or Untagged , the IP address entered in this text box is assigned to the Data portion of the radio (Ethernet port traffic and terminal server communication). Any data destined for one of the radio's serial ports or its Ethernet port needs to be addressed to this IP address and tagged with the Data VLAN ID .

3.1.14. Management VLAN ID



Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance. Incorrect settings can cause devices in the network to lose communication. See [Contact FreeWave Technical Support \(on page 12\)](#).

Management VLAN ID	
Setting	Description
Web Parameter:	Management VLAN ID text box in the VLAN Configuration (Data) area of the IP Setup window (on page 153).
Terminal Menu:	(1) IP Setup > (A) Management VLAN ID
Network Type:	Both
Default Setting:	0
Options:	Any valid VLAN ID between 1 and 4095.
Description:	Computers and devices using the VLAN ID entered here are able to: <ul style="list-style-type: none"> • access the radio's Setup pages, • receive SNMP information, • send SNMP commands, and • view the radio in the FreeWave Discovery Server.

3.1.15. VLAN Mode

Warning! Not every network needs or uses VLAN IDs.

The **Mode** parameter is typically set to **Disabled**.



The Network Administrator should approve any changes.

Configuring the VLAN information incorrectly can cause loss of communication between devices in the network.

VLAN Mode	
Setting	Description
Web Parameter:	Mode list box in the VLAN Configuration (Data) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (6) VLAN
Network Type:	Both
Default Setting:	Disabled
Options:	<p>Select the applicable option:</p> <ul style="list-style-type: none"> • Disabled - VLAN is not used. • Tagged - If the data coming into the radio's local Ethernet port is tagged with a VLAN ID. <ul style="list-style-type: none"> • The radio bridges the data, leaving the VLAN ID as-is. • Untagged - If the data coming into the radio's local Ethernet port is NOT tagged with a VLAN ID. <ul style="list-style-type: none"> • The radio accepts the data, tags it with the VLAN ID entered in the Data VLAN ID text box, and sends it across the radio link. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Data arriving at this radio and being sent out of the local Ethernet port has any VLAN tag removed before being sent out of the port.</p> </div>
Description:	Determines whether VLAN is active and in which mode it is used.

3.1.16. VLAN Subnet Mask

Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance.



Incorrect settings can cause devices in the network to lose communication.

See [Contact FreeWave Technical Support \(on page 12\)](#).

VLAN Subnet Mask	
Setting	Description
Web Parameter:	Subnet Mask text box in the VLAN Configuration (Data) area of the IP Setup window (on page 153) .

VLAN Subnet Mask	
Setting	Description
Terminal Menu:	(1) IP Setup > (8) Data Subnet Mask
Network Type:	Both
Default Setting:	255.255.255.0
Options:	Any IPV4 net mask address.
Description:	This is the Subnet mask for the Data VLAN IP address. <div style="border: 1px solid gray; padding: 5px; background-color: #e0e0e0; display: inline-block;"> Example: 255.255.255.0. </div>

3.1.17. VLAN Trunk ID 1 to VLAN Trunk ID 5



Warning! If this parameter needs to be set, contact FreeWave Technical Support for guidance. Incorrect settings can cause devices in the network to lose communication. See [Contact FreeWave Technical Support \(on page 12\)](#).

VLAN Trunk ID 1 to VLAN Trunk ID 5	
Setting	Description
Web Parameter:	VLAN Trunk ID 1 to VLAN Trunk ID 5 text boxes in the VLAN Configuration (Data) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (C) VLAN Trunk
Network Type:	Both
Default Setting:	0
Options:	Any number between 1 and 4095.
Description:	Use VLAN Trunk IDs to propagate the definition of VLANs on the whole local area network. On each device, enter the VLAN IDs of the devices that radios will be a participant. <div style="border: 1px solid gray; padding: 5px; background-color: #e0e0e0; display: inline-block;"> Note: Most networks do not use VLAN trunk IDs. </div>

3.1.18. Web Page Port (http)

Web Page Port (http)	
Setting	Description
Web Parameter:	Web Page Port (http) text box in the LAN Network Interface Configuration (Management) area of the IP Setup window (on page 153) .
Terminal Menu:	(1) IP Setup > (3) Web Page Port (http)

Web Page Port (http)	
Setting	Description
Network Type:	Both
Default Setting:	80
Options:	Any valid TCP port from 1 to 65535.
Description:	<p>Use this to change the assigned port for the configuration Web pages. The default setting is port 80, the standard Web page port.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: If this setting is changed from port 80, the proper port number MUST be included when accessing the Setup pages.</p> </div> <div style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p>Example: <code>http://<IP address>:<Port></code>, where: <IP address> is the IP address of the radio and <Port> is the port number assigned in this parameter.</p> </div> <p>If an invalid TCP port is entered, the radio defaults the Web Page Port setting to 80.</p>

4. Serial Port Settings

Use the settings on the **Serial Setup** tab or the [Serial Setup window](#) to set the serial ports on the radio. The ports are labeled 1 and 2 on the physical radio. See the radio illustration in [Components of the FGR2-P, -PE, & -PE-U PLUS Radios on page 15](#).

These parameters are available in **Serial Setup**:

- **Serial Port Mode** - This setting defines whether the port acts as a TCP terminal server, TCP client, UDP client, or Multicast.
- **Serial Settings** - This setting defines data transmission settings (e.g., **Baud Rate** and **Flow Control**).
 - Set these parameters to match the device the port is connected to.

Each serial port is setup independently and configured on its own tab or [Configuration Windows](#). The ports can have different baud rates, parity, protocol, and so on, but must match the device to which it is connected. To access either port, a client needs to call the IP address of the radio plus its assigned port number.

Note: See [Viewing the Serial Port Status on page 67](#) to view the status of each serial port.

4.1. Set the Serial Port Mode

The first parameter is to define the serial port using the:

- MULTICAST Settings.
- TCP Client Settings.
- TCP Server Settings.
- UDP Settings.

Procedure


1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click the serial port to configure (i.e., **Serial Port 1** or **Serial Port 2**).
The applicable [Serial Setup window](#) opens.

FREEWAVE
D2+
192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
'admin' From 192.168.111.1

Status	TCP Server Settings	
IP Setup	Enable	<input checked="" type="checkbox"/>
Serial Setup 1	Port	7000
Serial Setup 2	Enable Keepalive	<input type="checkbox"/>
Radio Setup	Inactivity Timeout (Seconds)	0
Security	TCP Client Settings	
SNMP	Enable	<input type="checkbox"/>
Diagnostics	IP Address & Port	0.0.0.0 : 9000
Users	UDP Settings	
Tools	Enable	<input type="checkbox"/>
Reboot	UDP IP & Port	0.0.0.0 : 6000
	MULTICAST Settings	
	Enable	<input type="checkbox"/>
	Multicast IP & Port	225.0.0.38 : 11111
	Serial Settings	
	Baud Rate	19200
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None
	CD Mode	Normal
	Interface	RS232
	Runtime Serial Setup 'U'	<input checked="" type="checkbox"/> Enable
	RTU Mode Timing Settings	
	Modbus RTU	<input checked="" type="checkbox"/> Enable
	Pre-Packet Timeout (ms)	0
	Post-Packet Timeout (ms)	20
	Save/Apply	

[Serial Port Status](#)
©2006-2014 FreeWave Technologies, Inc.

Figure 29: FGR2-P, -PE, & -PE-U Serial Setup window

3. In one of these areas, click the **Enable** check box to designate the port as that type:
 - **TCP Server Settings** - Designate the port as a TCP terminal server.
 - **TCP Client Settings** - Designate the port as a TCP client to the IP address and port entered in the [TCP Client IP Address](#) and [TCP Client Port](#) text boxes.
 - **UDP Settings** - Designate the radio as a UDP terminal server to the IP address and port entered in the [UDP IP Address](#) and [UDP IP Port](#) text boxes.
 - **MULTICAST Settings** - Designate a one-to-many connection from the MultiPoint Gateway's serial port to the MultiPoint Repeater's and/or Endpoint's serial ports using the IP address and port entered in the [Multicast IP Address](#) and [Multicast Port](#) text boxes.
4. Click  to save the changes.

4.2. Disabling Serial Ports

If a serial port on the radio is not used, it can be disabled.

Note: If both ports are disabled, the Basic IP Setup for the radio still works through Port 1.

Procedure


1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu** bar, click the serial port to configure (i.e., **Serial Port 1** or **Serial Port 2**).
The applicable [Serial Setup window](#) opens.

The screenshot shows the 'Serial Setup 1' configuration window. The interface includes a sidebar with navigation options: Status, IP Setup, Serial Setup 1 (selected), Serial Setup 2, Radio Setup, Security, SNMP, Diagnostics, Users, and Tools. A 'Reboot' button is located below the sidebar. The main content area is divided into several sections:

- TCP Server Settings:** Includes 'Enable' (checked), 'Port' (7000), 'Enable Keepalive' (unchecked), and 'Inactivity Timeout (Seconds)' (0).
- TCP Client Settings:** Includes 'Enable' (unchecked) and 'IP Address & Port' (0.0.0.0 : 9000).
- UDP Settings:** Includes 'Enable' (unchecked) and 'UDP IP & Port' (0.0.0.0 : 6000).
- MULTICAST Settings:** Includes 'Enable' (unchecked) and 'Multicast IP & Port' (225.0.0.38 : 11111).
- Serial Settings:** Includes 'Baud Rate' (19200), 'Data Bits' (8), 'Parity' (None), 'Stop Bits' (1), 'Flow Control' (None), 'CD Mode' (Normal), 'Interface' (RS232), and 'Runtime Serial Setup 'U'' (unchecked).
- RTU Mode Timing Settings:** Includes 'Modbus RTU' (checked), 'Pre-Packet Timeout (ms)' (0), and 'Post-Packet Timeout (ms)' (20).

A 'Save/Apply' button is located at the bottom right of the configuration area. Below the configuration area, there is a link for 'Serial Port Status' and a copyright notice: '©2006-2014 FreeWave Technologies, Inc.'

Figure 30: FGR2-P, -PE, & -PE-U Serial Setup window

3. Clear all the **Enable** check boxes in the window.
4. Click  to save the changes.

4.3. Viewing the Serial Port Status

Note: The serial port's status is ONLY visible through the [Configuration Windows](#).

This status information is available for each serial port:

- [Ethernet \(Rx and Tx\) \(on page 68\)](#)
- [Serial \(Rx and Tx\) \(on page 68\)](#)
- [Status \(on page 68\)](#)

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu** bar, click the serial port to configure (i.e., **Serial Port 1** or **Serial Port 2**).
The applicable [Serial Setup window](#) opens.

FREEWAVE D2+
192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
'admin' From 192.168.111.1

Status	TCP Server Settings	
IP Setup	Enable	<input checked="" type="checkbox"/>
Serial Setup 1	Port	7000
Serial Setup 2	Enable Keepalive	<input type="checkbox"/>
Radio Setup	Inactivity Timeout (Seconds)	0
Security	TCP Client Settings	
SNMP	Enable	<input type="checkbox"/>
Diagnostics	IP Address & Port	0.0.0.0 : 9000
Users	UDP Settings	
Tools	Enable	<input type="checkbox"/>
Reboot	UDP IP & Port	0.0.0.0 : 6000
	MULTICAST Settings	
	Enable	<input type="checkbox"/>
	Multicast IP & Port	225.0.0.38 : 11111
	Serial Settings	
	Baud Rate	19200
	Data Bits	8
	Parity	None
	Stop Bits	1
	Flow Control	None
	CD Mode	Normal
	Interface	RS232
	Runtime Serial Setup 'U'	<input checked="" type="checkbox"/> Enable
	RTU Mode Timing Settings	
	Modbus RTU	<input checked="" type="checkbox"/> Enable
	Pre-Packet Timeout (ms)	0
	Post-Packet Timeout (ms)	20
	Save/Apply	

[Serial Port Status](#)
©2006-2014 FreeWave Technologies, Inc.

Figure 31: FGR2-P, -PE, & -PE-U Serial Setup window

3. Click the **Serial Port Status** link.
The [Serial Port Status window](#) opens.

Note: This window is read-only and cannot be changed.

Serial Port 1	
Socket 1 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 2 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 3 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 4 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 5 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Serial Port 2	
Socket 1 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 2 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 3 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 4 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 5 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0

Figure 32: FGR2-P, -PE, & -PE-U Serial Port Status window

By default, this window updates every 5 seconds.

4. Click the **Refresh** link to manually refresh the page.

4.3.1. Ethernet (Rx and Tx)

This is the amount of data received (Rx) and transmitted (Tx) from the terminal server to the port.

- Received data indicates data received on the radio via the Ethernet port.
- Transmitted data indicates data sent from the radio out the port.
- The amount is listed in bytes.

4.3.2. Serial (Rx and Tx)

This is the amount of data received (Rx) and transmitted (Tx) from the serial port.

- Received data indicates data coming from the connected device into the serial port.
- Transmitted data indicates data sent out the serial port to the connected device.
- This amount is listed in bytes.

4.3.3. Status

This is the current status of the Terminal Server.

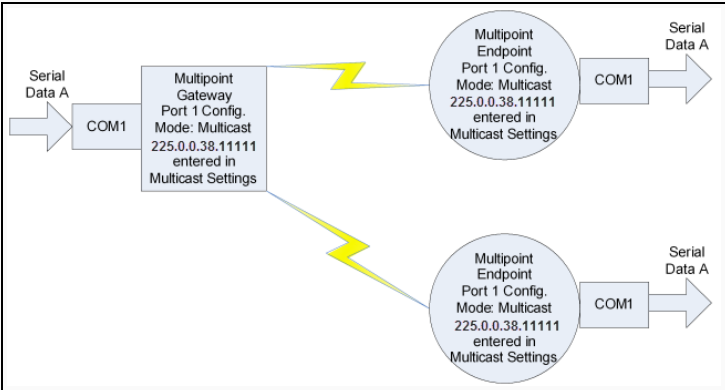
Example: Waiting or Connected.

4.4. Serial Port Parameter Reference

This section contains the serial port parameters.

Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.

4.4.1. Multicast Enable

Multicast Enable	
Setting	Description
Web Parameter:	Enable check box in the MULTICAST Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (C) Multicast
Network Type:	Both
Default Setting:	Disabled
Options:	Disabled, Enabled
Description:	<p>This setting enables the radio to use Multicast mode when enabled.</p> <ul style="list-style-type: none"> • A Multicast is a one-to-many connection from the MultiPoint Gateway's serial port to the interested MultiPoint Repeaters and/or Endpoints serial ports. • In a MultiPoint Gateway, selecting Multicast causes the radio to act as an IP Multicast Sender on the Multicast address and port. 

4.4.2. Multicast IP Address

Multicast IP Address	
Setting	Description
Web Parameter:	Multicast IP text box in the MULTICAST Settings area of the Serial Setup window (on page 168) .

Multicast IP Address	
Setting	Description
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (D) Multicast IP
Network Type:	Both
Default Setting:	225.0.0.38
Options:	Any valid multicast address from 224.0.0.0 to 239.255.255.255.
Description:	<p>This is the IP address used for Multicast if the serial port is set to Multicast mode.</p> <ul style="list-style-type: none"> In a MultiPoint Gateway, this is the sending address. In MultiPoint Endpoints and MultiPoint Repeaters, this is the address they register interest in. <p>In the Configuration Web pages:</p> <ul style="list-style-type: none"> Enter the IP address in the field to the left of the colon. Enter the port number in the field to the right of the colon.

4.4.3. Multicast Port


Multicast Port	
Setting	Description
Web Parameter:	The Multicast Port text box in the MULTICAST Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (E) Multicast Port
Network Type:	Both
Default Setting:	Setup 1: 11111 Setup 2: 22222
Options:	Any valid port number between 0 and 65535.
Description:	<p>The port used if the serial port is set to Multicast mode.</p> <p>In the Serial Setup window (on page 168), in the MULTICAST Settings area:</p> <ul style="list-style-type: none"> In the Multicast IP text box on the left of the colon, enter the IP address. In the Port text box on the right of the colon, enter the port number.

4.4.4. Pre-Packet and Post-Packet Timeouts

Pre-Packet and Post-Packet Timeouts	
Setting	Description
Web Parameter:	Pre-Packet Timeout (ms) and Post-Packet Timeout (ms) in the RTU Mode Timing Settings area of the Serial Setup window (on page 168) .


Pre-Packet and Post-Packet Timeouts																							
Setting	Description																						
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (F) Pre Packet Timeout (2) Serial Setup 1 or (3) Serial Setup 2 > (G) Post Packet Timeout																						
Network Type:	Both																						
Default Setting:	<p>Defaults are based on the data rate selected in the Serial Baud Rate field:</p> <table border="1"> <thead> <tr> <th>Serial Baud Rate (bps)</th> <th>Timeout (ms)</th> </tr> </thead> <tbody> <tr><td>300</td><td>133</td></tr> <tr><td>600</td><td>67</td></tr> <tr><td>1200</td><td>34</td></tr> <tr><td>2400</td><td>17</td></tr> <tr><td>4800</td><td>10</td></tr> <tr><td>9600</td><td>6</td></tr> <tr><td>19200</td><td>4</td></tr> <tr><td>38400</td><td>2</td></tr> <tr><td>57600</td><td>2</td></tr> <tr><td>115200</td><td>1</td></tr> </tbody> </table>	Serial Baud Rate (bps)	Timeout (ms)	300	133	600	67	1200	34	2400	17	4800	10	9600	6	19200	4	38400	2	57600	2	115200	1
Serial Baud Rate (bps)	Timeout (ms)																						
300	133																						
600	67																						
1200	34																						
2400	17																						
4800	10																						
9600	6																						
19200	4																						
38400	2																						
57600	2																						
115200	1																						
Options:	<p>Any number of milliseconds.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>FREEWAVE Recommends: Accept the defaults based on the selected Serial Baud Rate.</p> </div>																						
Description:	<p>The timeout values are pre-populated when the Modbus RTU parameter is enabled and are based on the Modbus RTU specification.</p> <p>Modify the timeout values to account for higher performing Modbus RTU devices.</p> <ul style="list-style-type: none"> • If using a non-Modbus device, clear the Modbus RTU Enable check box. • Both Timeout parameters set to 0, regardless of the selected Baud Rate (on page 72). • Set the timeout settings to what the non-Modbus device requires. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: As of May-2018, FreeWave only supports Modbus RTU/ASCII.</p> </div> <p>If a silence-delimited RTU protocol (e.g., the DNP3 protocol) is not used, set both the Timeout parameters to 0. Any other setting adds additional latencies during polling.</p>																						

4.4.5. Runtime Serial Setup "U"

Runtime Serial Setup "U"	
Setting	Description
Web Parameter:	Runtime Serial Setup "U" check box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (O) Runtime Serial Setup
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<div style="border: 1px solid black; padding: 5px;">  <p>If Runtime Serial Setup "U" check box is selected, AND the computer is connected to the radio using the serial port, press <Shift+U> to access the Setup Mode without having the radio reboot.</p> </div>

4.4.6. Baud Rate

Baud Rate	
Setting	Description
Web Parameter:	Baud Rate list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (H) Baud Rate
Network Type:	Both
Default Setting:	19200
Options:	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200

Baud Rate	
Setting	Description
Description:	<p>This is the actual baud rate for the radio's data port.</p> <p>This setting is the communication rate between the radio and the instrument to which it is connected, and is independent of the baud rate for the other radios in the network. It is also independent of the other serial port on the radio.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Set the baud rate to the highest level supported by the device to which it is connected. With a poor radio link, however, this may actually result in slower data communications.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0; background-color: #e0e0e0;"> <p>Example: A pair of radios may be used in an application to send data from remote process instrumentation to the engineer's computer. In this application, the baud rate for the radio on the instrumentation might be set to 9600, and the radio on the engineer's computer might be set to 57,600.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: The serial ports do not support RFC 2217 level flow control. To avoid congestion-related data loss, use a link data rate that is at least 2 times higher than the actual data flow rate.</p> </div>

4.4.7. CD Mode

CD Mode	
Setting	Description
Web Parameter:	CD Mode list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (M) CD Mode
Network Type:	Both
Default Setting:	Normal
Options:	<ul style="list-style-type: none"> • Normal - CD is asserted when a TCP connection to the associated port is made, and de-asserted when the TCP connection is closed. Most serial devices use this option. • Keyed - CD asserts 500 μs before transmit, and de-asserts 1 ms after the transmission of the first bit of the last byte of data. This option should be used with serial devices that require the CD line to be asserted prior to the transmission of data.
Description:	Controls the function of the CD line on the serial port.

4.4.8. Data Bits

Data Bits	
Setting	Description
Web Parameter:	Data Bits list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (I) Data Bits
Network Type:	Both
Default Setting:	8
Options:	5, 6, 7, 8
Description:	The number of data bits the serial port sends. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: The setting in this parameter should match the number of data bits the connected device requires or is set to.</p> </div>

4.4.9. Flow Control

Flow Control	
Setting	Description
Web Parameter:	Flow Control list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (L) Flow Control
Network Type:	Both
Default Setting:	None
Options:	<ul style="list-style-type: none"> • None - Uses software flow control (XON / XOFF). • Hardware - Uses hardware flow control (RTS / CTS).
Description:	Indicates whether hardware flow control is used on the serial port. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>FREEWAVE Recommends: Use Flow Control if using a Baud Rate (on page 72) higher than 19200.</p> </div>

4.4.10. Interface

Interface	
Setting	Description
Web Parameter:	Interface list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (N) Interface

Interface	
Setting	Description
Network Type:	Both
Default Setting:	RS232
Options:	<ul style="list-style-type: none"> • RS232 • RS485 • RS422
Description:	<p>This is the serial protocol the serial port uses. This protocol should match the protocol the connected device requires.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: For pinout information, see RS422 and RS485 Full Duplex Pinouts (on page 146).</p> </div>

4.4.11. Modbus RTU

Modbus RTU	
Setting	Description
Web Parameter:	Modbus RTU Enable check box in the RTU Mode Timing Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	Not available
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<p>When enabled, the radio gathers data on the serial port until there is a break (3.5 characters) in the data due to Modbus RTU timing.</p> <ul style="list-style-type: none"> • The data is sent as one TCP packet. • Based on the data rate selected in the Baud Rate (on page 72) parameter, the system populates the Pre-Packet and Post-Packet Timeouts (on page 70) parameters with the default number of milliseconds (ms) according to the Modbus RTU specifications. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important! If a silence-delimited RTU protocol (e.g., the DNP3 protocol) is NOT used, set both the timeout fields to 0. Any other setting adds additional latencies during polling.</p> </div>

4.4.12. Parity

Parity	
Setting	Description
Web Parameter:	Parity list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (J) Parity
Network Type:	Both
Default Setting:	None
Options:	<ul style="list-style-type: none"> • Even • None • Odd
Description:	<p>This is the parity type the serial port uses.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This type should match the parity the connected device requires.</p> </div>

4.4.13. Stop Bits

Stop Bits	
Setting	Description
Web Parameter:	Stop Bits list box in the Serial Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (K) Stop Bits
Network Type:	Both
Default Setting:	1
Options:	1, 2
Description:	<p>This is the number of stop bits the serial port sends.</p> <p>This number should match the number of stop bits the connected device requires.</p>

4.4.14. TCP Client Enable

TCP Client Enable	
Setting	Description
Web Parameter:	Enable check box in the TCP Client Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (0) TCP Client
Network Type:	Both

TCP Client Enable	
Setting	Description
Default Setting:	Disabled
Options:	Disabled, Enabled
Description:	<p>Enabling this parameter sets the operating mode of the radio's terminal server to TCP Client.</p> <p>Your selection determines which other parameters are available for the serial port. After booting up, the radio creates a persistent outgoing TCP connection to the TCP Client IP Address on page 77 and TCP Client Port on page 77.</p> <p>Any data sent to the associated serial port on the radio is automatically directed to the entered IP address and port number.</p>

4.4.15. TCP Client IP Address

TCP Client IP Address	
Setting	Description
Web Parameter:	IP Address text box in the TCP Client Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (4) Client IP
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid IP address.
Description:	<p>This is the IP address the radio creates a connection to on boot-up, when the radio is set to TCP Client mode.</p> <p>In the Configuration Web page:</p> <ul style="list-style-type: none"> • Enter the IP address to the left of the colon. • Enter the TCP port number in the box to the right of the colon.

4.4.16. TCP Client Port

TCP Client Port	
Setting	Description
Web Parameter:	Port text box in the TCP Client Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (5) Client Port
Network Type:	Both
Default Setting:	Setup 1: 9000 Setup 2: 9001

TCP Client Port	
Setting	Description
Options:	Any valid port number between 0 and 65335.
Description:	<p>This is the port number the radio creates a connection to on boot-up, when the radio is set to TCP Client mode.</p> <p>In the Configuration Web page:</p> <ul style="list-style-type: none"> • Enter the IP address to the left of the colon. • Enter the TCP port number in the box to the right of the colon.

4.4.17. TCP Server Enable

TCP Server Enable	
Setting	Description
Web Parameter:	Enable check box in the TCP Server Settings area of the Serial Setup window (on page 168).
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (0) TCP Server
Network Type:	Both
Default Setting:	Enabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<p>Enabling this parameter sets the operating mode of the radio's terminal server to TCP Server.</p> <ul style="list-style-type: none"> • The selection determines which other parameters are available for the serial port. <ul style="list-style-type: none"> • TCP establishes a connection at both ends of the communication between two machines before any data can be transmitted. • The TCP Server waits for calls from a TCP client. • If there are multiple TCP Clients set up to communicate with the TCP Server, after a request comes into the TCP Server port, the radio sends any incoming serial data to the IP address of the requesting device. • The radio continues doing so until a new device makes a request on that port. • The radio always sends the serial data to the address of the last successful requesting device.

4.4.18. TCP Server Inactivity Timeout

TCP Server Inactivity Timeout	
Setting	Description
Web Parameter:	Inactivity Timeout (Seconds) text box in the TCP Server Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (2) Inactivity Timeout
Network Type:	Both
Default Setting:	0
Options:	Any number of seconds.
Description:	<p>This setting controls how long, in seconds, an incoming TCP connection must be idle (that is, no data being transferred) before the radio drops the connection.</p> <p>A setting of 0 means that the radio never disconnects an idle connection—all disconnects need to come from the client.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>FREEWAVE Recommends: In some RTUs, after the RTU is connected to the radio as a client, the RTU does not properly disconnect the TCP session. To help overcome this potential behavior of some RTUs, FreeWave recommends setting the Inactivity Timeout parameter to 10.</p> </div>

4.4.19. TCP Server Keep Alive

TCP Server Keep Alive	
Setting	Description
Web Parameter:	TCP Server Keep Alive check box in the TCP Server Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	Not available
Network Type:	Both
Default Setting:	Disabled
Options:	Disabled, Enabled
Description:	<p>If enabled, the radio sends a packet at a regular interval to ensure the route used for an Ethernet session is kept for the entire session.</p> <p>If there is no data or keep alive packets, routers can lose their current session and the packets can travel a different route through the TCP network.</p>

4.4.20. TCP Server Port

TCP Server Port	
Setting	Description
Web Parameter:	Port text box in the TCP Server Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (1) TCP Server Port
Network Type:	Both
Default Setting:	Setup 1: 7000 Setup 2: 7001
Options:	Any valid TCP port between 0 and 65535.
Description:	The TCP port the radio listens to for incoming TCP connections.

4.4.21. UDP Enable

UDP Enable	
Setting	Description
Web Parameter:	Enable check box in the UDP Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (9) UDP
Network Type:	Both
Default Setting:	Disabled
Options:	Disabled, Enabled
Description:	This setting enables the radio as a UDP terminal server using the port number entered in the destination port. If using as a UDP terminal server, the port number entered in the destination port is the UDP port that the radio listens to for requests.

4.4.22. UDP IP Address

UDP IP Address	
Setting	Description
Web Parameter:	IP Address text box in the UDP Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (A) UDP IP
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid Multicast address from 224.0.0.0 to 239.255.255.255.

UDP IP Address	
Setting	Description
Description:	<p>When the serial port is set to UDP mode, enter the IP address where the radio sends any serial data coming into its serial port.</p> <ol style="list-style-type: none"> 1. Enter the IP address to the left of the colon. 2. Enter the port number in the box to the right of the colon.

4.4.23. UDP IP Port

UDP IP Port	
Setting	Description
Web Parameter:	Port text box in the UDP Settings area of the Serial Setup window (on page 168) .
Terminal Menu:	(2) Serial Setup 1 or (3) Serial Setup 2 > (B) UDP Port
Network Type:	Both
Default Setting:	Setup 1: 6000 Setup 2: 6001
Options:	Any valid IP port number between 0 and 65535.
Description:	This is the destination port that the radio listens to for requests.

5. Radio Settings

Use the settings on the [Radio Setup window \(on page 156\)](#) to set the general functioning of the radio.

The available parameters are:

- **Operation Mode** - Designates the mode the radio uses to communicate and the network type.
- **Transmission Characteristics** - Transmission characteristics (e.g., **Frequency Key** and the packet size parameters) are for advanced users **only**.

Important! It is critical to understand the principles of RF data transmission to change these parameters.

- **Point-to-Point** - The **Transmit Rate** and the Call Book are mainly for use in a Point-to-Point network.

Note: See the [Call Book window on page 158](#).

- **Multipoint Parameters** - A Point-to-MultiPoint network requires that several parameters are set consistently on all radios in the network. This includes **RF Data Rate**, **Min and Max Packet Size**, and **Frequency Key**.

Important! If several independent, PTMP networks are located in close proximity, it is very important to include as much frequency and time diversity as possible using different **Frequency Key** and **Min and Max Packet Sizes**.

In a Point-to-Point network, the Gateway determines all settings in an Endpoint or Repeater, except for the **Transmit Power** and **Retry Timeout**. All other settings in a Point-to-Point network are determined by the Gateway's settings.



Caution: Changes made to the radio settings can cause the radios to lose communication with the Gateway and Multipoint Repeaters.

Use caution when making global changes using the **Global Change** function.

For more information about making global changes, see [Use the MultiPoint Gateway to Change All Connected Radios \(on page 33\)](#).

5.1. Radio Setup Parameter Reference

This section contains the radio setup parameters.

Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.


5.1.1. Addressed Repeat

Note: This setting MUST match between the Gateway and all Repeaters.

Addressed Repeat	
Setting	Description
Web Parameter:	Addressed Repeat list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (A) Addressed Repeat
Network Type:	MultiPoint
Default Setting:	3
Options:	Any number between 0 and 9.
Description:	<p>In a MultiPoint network where the Repeaters parameter is set to Disabled, most packets from the Gateway are addressed to a specific MAC address. This addressing allows the destination device to send an acknowledgment back to the Gateway that the packet was received successfully.</p> <p>The Addressed Repeat parameter determines the maximum number of times the Gateway repeats its data packet if it does not receive an acknowledgment from the destination device.</p> <ul style="list-style-type: none"> This repeat is a smart repeat - the Gateway only repeats its data if it does not receive an acknowledgment. Changing this setting to a higher number can increase the reliability of weaker radio links while keeping the maximum possible throughput for that link. <p>In Endpoints, this setting determines how many times the Endpoint retries a packet of addressed data before taking the action set in the Slave Connect Odds parameter.</p>

5.1.2. Broadcast Repeat

Note: This setting MUST match between the Gateway and all Repeaters.

Broadcast Repeat	
Setting	Description
Web Parameter:	Broadcast Repeat list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (B) Broadcast Repeat
Network Type:	MultiPoint
Default Setting:	3
Options:	Any number between 0 and 9.
Description:	<p>In Endpoints, this setting determines how many times the Endpoint retries a packet of broadcast data before taking the action set in the Slave Connect Odds (on page 98) parameter.</p> <p>The Broadcast Repeat parameter may be set to 0 in the Gateway if the software is capable of or requires acknowledgment. In this case, if the Gateway sends a packet that the Endpoint does not receive, the software controls the retries, as needed.</p> <ul style="list-style-type: none"> • For networks with solid RF links, this parameter should be set to a low value such as 1 or 2. • If a network has some weak or marginal links, this parameter should be set to higher values. • If an Endpoint receives a good packet from a Gateway more than once, it discards the repeated packets. • Similarly, after a MultiPoint Repeater receives a good packet from the Gateway more than once, it discards any further repeated packets. • In turn, the Repeater sends the packet out to the next Repeater or Endpoint (s) the number of times corresponding to its own Broadcast Repeat parameter setting. <p>In a network that contains radios set as a Repeater, all packets from the Gateway are considered broadcast MAC address packets.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Increasing the Broadcast Repeat parameter setting in this type of network increases the probability of a packet getting through. It also increases latency and decreases Gateway-to-Repeater and Gateway-to-Endpoint throughput in the network because each packet from the Gateway or Repeater is being sent multiple times.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Important!: Find the optimal mix between network robustness, throughput, and latency. In general, a setting of 2 to 3 works well for most well designed networks.</p> </div>

5.1.3. Broadcast Repeat in MultiPoint Networks with Repeaters

The **Broadcast Repeat** parameter must also be set in MultiPoint Repeaters because a Repeater appears as a Gateway to an Endpoint.

Therefore, the Repeater sends the packet out the number of times corresponding to its own **Broadcast Repeat** parameter setting. If this parameter is set improperly, the reliability of the overall network may be diminished.


Example: If a Gateway's **Broadcast Repeat** parameter is set to **3**, the link between the Gateway and Repeater should be robust.
If the Repeater's **Broadcast Repeat** parameter is set to **0**, this could cause marginal communication between the Repeater and the Endpoints.
The Endpoints communicating through this Repeater only receives the initial packet from the Gateway with no repeats.
Therefore, if the packet is not received on the first try, the Endpoint does not respond as expected.

Important!: This parameter should NEVER be set higher on a Repeater than on its Gateway.

5.1.4. Frequency Key

Note: If subnet IDs are not used to route network traffic, the **Frequency Key** must match on all radios in the network.

Frequency Key	
Setting	Description
Web Parameter:	Frequency Key list box in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (2) Frequency Key
Network Type:	Both
Default Setting:	5
Options:	Any number between 0 to 9, or any letter between A to E.

Frequency Key	
Setting	Description
Description:	<p>This setting changes the hopping patterns of the radio.</p> <ul style="list-style-type: none"> There are 15 choices available for the Frequency Key parameter representing 15 different pseudo-random hop patterns. These hopping patterns minimize the interference with other FreeWave radios operating in the area. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Example: If there were 10 pairs of FreeWave radios operating on different networks in close proximity, setting a different Frequency Key value for each pair reduces the chance that radios hop to the same frequency at the same time.</p> <p>If two networks were to hop to the same frequency by chance, the next hop would be to a different frequency for both networks.</p> <p>To use a different Frequency Key, subnet IDs MUST be used.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: See Subnet ID on page 99.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> Additional network separation can be gained by adjusting the Max and Min Packet Size settings.</p> </div>

5.1.5. Frequency Zones

Important! When trying to inter-operate and there are radios with different **Country Codes** on the [Status window \(on page 175\)](#), contact FreeWave Customer Support for assistance. See [Contact FreeWave Technical Support on page 12](#).

Note: In MultiPoint networks, this setting only needs to be set on the Gateway. In a Point-to-Point network, the Gateway and the Endpoint must have matching **Frequency Zone** settings.

Frequency Zones	
Setting	Description
Web Parameter:	Zones check boxes in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (3) Zones
Network Type:	Both
Default Setting:	All selected

Note: HTP-900RE-SR004 and HTP-900SEO-SR004 models are configured to limit frequencies to 915 MHz to 927 MHz.

Frequency Zones	
Setting	Description
Options:	See Description.
Description:	<p>In the Radio Setup window, the zones are listed as check boxes in the Zones box in the Transmission Characteristics area.</p> <p>Select the check box next to the zone to enable it.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Important! A cleared check box indicates the radio does NOT use that frequency.</p> </div> <p>This setting divides the available band into smaller bands (i.e., 16 smaller bands each consisting of 2 or 3 frequency channels):</p> <ul style="list-style-type: none"> • 902 MHz to 928 MHz • The zones listed are in MHz. • The radio requires at least one zone active to operate.

5.1.6. Master Tx Beacon

Note: This setting MUST to be the same in every Gateway, Repeater, and Endpoint.

Master Tx Beacon	
Setting	Description
Web Parameter:	Master Tx Beacon list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (E) Master Tx Beacon
Network Type:	MultiPoint
Default Setting:	1
Options:	Any number between 1 and 9.
Description:	<p>This setting controls the Gateway's duty-cycle during idle times.</p> <ul style="list-style-type: none"> • By default, the Gateway transmits every frame, whether there is payload data or not. • Selecting a number larger than 1 in this parameter causes the Gateway to skip that number of transmit frames when it has no other data to send. <ul style="list-style-type: none"> • This skip can reduce the power usage from the Gateway during idle times. • If data does come into the Gateway, the Gateway transmits that data regardless of this setting. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: In a network that has the Repeaters parameter set to Enabled, this parameter must be set to 1.</p> </div>

5.1.7. Max Packet Size and Min Packet Size

Note: In MultiPoint networks, the **Max Packet Size** and **Min Packet Size** must be identical in all radios.

In Point-to-Point networks the Gateway's settings take precedence over the Endpoint.

Max Packet Size and Min Packet Size	
Setting	Description
Web Parameter:	Max Packet Size and Min Packet Size list boxes in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (4) Max Packet Size (4) Radio Setup > (5) Min Packet Size
Network Type:	Both
Default Setting:	<ul style="list-style-type: none"> Max Packet Size = 9 Min Packet Size = 1 Use these settings for the overall best throughput.
Options:	Any number between 0 and 9.
Description:	The Max and Min Packet Size settings and the RF Data Rate determine the number of bytes in the packets. <ul style="list-style-type: none"> Throughput can be enhanced when packet sizes are optimized. In Point-to-Point mode, the Max and Min Packet Size parameter settings do not have material impact on throughput unless a data rate of 92 kbps is applicable. This may have an impact on latency. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Example: If small amounts of data are sent and large packet sizes are selected, there would be a certain amount of time “wasted” between each packet.</p> </div>

This table defines the minimum packet size (in bytes) of the **Min Packet Size** setting versus the **RF Data Rate** setting.

Note: Using the default settings, the actual minimum packet size for the radios, in bytes, is 21.

Minimum Packet Size Definition		
Minimum Setting	Min Packet Size (bytes) RF Data rate = 154 kbps	Min Packet Size (bytes) RF Data Rate = 115 kbps
0	15	8

Minimum Packet Size Definition		
Minimum Setting	Min Packet Size (bytes) RF Data rate = 154 kbps	Min Packet Size (bytes) RF Data Rate = 115 kbps
1	21	12
2	26	16
3	31	20
4	37	24
5	42	28
6	47	32
7	53	36
8	58	40
9	63	44

This table defines the maximum packet size (in bytes) of the **Min Packet Size** setting versus the **Max Packet Size** setting where the **RF Data Rate** is set to **154 kbps**.

Note: Using the default settings, the actual maximum packet size, in bytes, is 213.

Maximum Packet Size Definition with RF Data Rate of 154 kbps (in bytes)										
Minimum Setting	Max Setting (blank area = not recommended)									
	0	1	2	3	4	5	6	7	8	9
0								165	186	207
1								170	191	213
2							154	175	197	218
3							159	181	202	223
4							165	186	207	229
5							170	191	213	234
6						154	175	197	218	239
7						159	181	202	223	245
8						165	186	207	229	250
9						170	191	213	234	255

Referencing the default settings, the Gateway transmits a maximum of 213 bytes on every hop. If fewer than 213 bytes are transmitted by the Gateway, the balance is allocated to the Endpoint's transmission, plus the quantity in the **Min Packet Size** setting.

Example: If a Gateway transmits 100 bytes, the Endpoint then has a total of 134 bytes available [113 (leftover bytes) + 21 (Min Packet Size)].

This table defines the maximum packet size (in bytes) of the **Min Packet Size** setting versus the **Max Packet Size** setting where the **RF Data Rate** is set to **115 kbps**.

Maximum Packet Size Definition with RF Data Rate of 115 kbps (in bytes)										
	Max Setting (blank area = not recommended)									
Minimum Setting	0	1	2	3	4	5	6	7	8	9
0						88	104	120	136	152
1						92	108	124	140	156
2					80	96	112	128	144	160
3					84	100	116	132	148	164
4					88	104	120	136	152	168
5					92	108	124	140	156	172
6				80	96	112	128	144	160	176
7				84	100	116	132	148	164	180
8				88	104	120	136	152	168	184
9				92	108	124	140	156	172	188


5.1.8. Modem Mode

Modem Mode	
Setting	Description
Web Parameter:	Modem Mode list box in the Operation Mode are of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (1) Modem Mode
Network Type:	Both
Default Setting:	Gateway in software earlier than 2.30 MultiPoint Endpoint in software 2.30 and later
Options:	See Modem Mode Options (on page 91) .

Modem Mode	
Setting	Description
Description:	<p>The Network Type and Modem Mode options designate the method FreeWave radios use to communicate with each other. FreeWave Ethernet radios operate in a Gateway-to-Endpoint configuration. Before the radios can operate together, they must be set up to properly communicate.</p> <ul style="list-style-type: none"> In a standard configuration, the Gateway mode should be used on the end which will be connected to the LAN. When setting up the radio, remember that a number of parameters are controlled by the settings in the Gateway. Therefore, deploying the Gateway on the communications end where it is easier to access is strongly advised. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This parameter is hidden in the Configuration Windows when Global Changes are enabled. For more information about making global changes, see Use the MultiPoint Gateway to Change All Connected Radios (on page 33).</p> </div>



Modem Mode Options

Repeaters are commonly used in serial networks to connect long distances, but not in Ethernet networks. If the network topology requires a Repeater to connect radios over greater distances, use a back-to-back Repeater where data is repeated over a wire instead of over the air. This preserves throughput.

Modem Mode Options	
Operation Mode	Description
Point-to-Point Gateway	<p>Designates the radio as the Gateway in Point-to-Point mode.</p> <ul style="list-style-type: none"> The Gateway may call any or all Endpoints designated in its Call Book. A quick method of identifying a Gateway is to power the radio. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Prior to establishing a communication link with an Endpoint or Repeater, all three of the Gateway's lower LEDs (CD, TX, CTS) are solid red ().</p> </div>
Point-to-Point Endpoint	<p>Designates the radio as an Endpoint in Point-to-Point mode.</p> <p>The Endpoint communicates with any Gateway in its Call Book, either directly or through up to four Repeaters.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: When functioning as an Endpoint, the Entry to Call feature in the radio's Call Book is not operational.</p> </div>

Modem Mode Options	
Operation Mode	Description
MultiPoint Gateway	<p>Designates the radio as a Gateway in MultiPoint mode.</p> <ul style="list-style-type: none"> This mode allows one Gateway radio to simultaneously be in communication with numerous Endpoints and Repeaters. A MultiPoint Gateway communicates only with other radios designated as MultiPoint Endpoints or MultiPoint Repeaters.
MultiPoint Endpoint	<p>Designates the radio as an Endpoint in MultiPoint mode.</p> <ul style="list-style-type: none"> This mode allows the Endpoint to communicate with a MultiPoint Gateway. The Endpoint may communicate with its Gateway through one or more Repeaters.
Point-to-Point Repeater (Single Radio Repeater)	<p>FreeWave allows the use of a maximum four (4) Repeaters in a Point-to-Point communications link, significantly extending the operating range.</p> <ul style="list-style-type: none"> When designated as a Point-to-Point Repeater, a radio behaves as a pass-through link. All settings for the baud rates and RF transmission characteristics are disabled. A Repeater connects with any Gateway that calls it. The Repeater must be set up properly in the Gateway's Call Book. In Point-to-Point mode, the Repeater is NOT an Endpoint/Repeater. <ul style="list-style-type: none"> The Call Book MUST be set in Point-to-Point mode. <p>Note: This operation mode should be used when operating the radio as a terminal server only (no RF connectivity).</p> <p>Important! Adding a Repeater to a network cuts the network throughput by 50%.</p> <p>Note: For more information, see the Call Book window (on page 158).</p>
MultiPoint Repeater (Single Radio Repeater)	<p>Allows the radio to operate as an Endpoint/Repeater in a MultiPoint network.</p> <p>Important! Some advanced features of the radio do NOT operate in networks containing Repeaters. FreeWave does not recommend the use of single-radio Repeaters.</p> <p>Important! Adding a Repeater to a network cuts the network throughput by 50%.</p> <p>Any Repeater in a Point-to-MultiPoint network is an Endpoint/Repeater.</p>

5.1.9. Network ID

Network ID	
Setting	Description
Web Parameter:	Network ID text box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (F) Network ID
Network Type:	MultiPoint
Default Setting:	<ul style="list-style-type: none"> • 255 in software earlier than 2.30. • 1 in software 2.30 and later.
Options:	Any number between 0 and 4095.
Description:	<p>Use the Network ID to establish MultiPoint networks without using the Call Book.</p> <ul style="list-style-type: none"> • To enable the Network ID, the value must be set between 0 and 4095 (excluding 255, which disables the Network ID and enables the Call Book). • Because the Network ID does not use serial numbers, MultiPoint Gateways and Repeaters may be replaced without reconfiguring all of the Endpoints in the network. • An Endpoint links with the first Gateway or Repeater that it hears that has a matching Network ID. • The Network ID should be used in conjunction with the Subnet ID feature (if necessary) to route data through the radio network. • Without having the serial numbers in the Call Book, Endpoints may establish communications with different Masters, though not at the same time. <ul style="list-style-type: none"> • This is very useful in mobile MultiPoint applications. <p>FREEWAVE Recommends: A Network ID of four characters.</p> <p>Example: The last four digits of the Gateway's serial number.</p> <p> Tip: Using the last four digits of the Gateway's serial number, if it is below 4095, helps to ensure the Network ID is unique and does not overlap with other nearby FreeWave networks.</p> <p> Caution: Avoid using numbers that coincide with nearby landmarks or highways.</p>

5.1.10. Network Type

Network Type	
Setting	Description
Web Parameter:	Network Type list box in the Operation Mode are of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (0) Network Type
Network Type:	Both
Default Setting:	<ul style="list-style-type: none"> Point-to-Point in software earlier than 2.30. Point-to-MultiPoint in software 2.30 and later.
Options:	MultiPoint, Point-to-Point
Description:	<p>This setting indicates the type of network the radio resides in. This selection and the selection in the Modem Mode parameter determine the operation mode of the radio (e.g., a Point-to-Point Gateway).</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: For descriptions of each network type and modem mode combination, see Modem Mode on page 90.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Important! The network type MUST match for all radios in a network.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0; background-color: #e6f2ff;"> <p>Example: If configuring a Point-to-MultiPoint network, verify the Network Type selection for each radio in the network is MultiPoint.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: This parameter is hidden in the Configuration Windows when Global Changes are enabled. For more information about making global changes, see Use the MultiPoint Gateway to Change All Connected Radios (on page 33).</p> </div>

5.1.11. Repeaters


Repeaters	
Setting	Description
Web Parameter:	Repeaters list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (G) Repeaters
Network Type:	MultiPoint
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> Disabled Enabled

Repeaters	
Setting	Description
Description:	<p>Important! In a MultiPoint network, it is critical to transmission timing to configure this parameter correctly.</p> <ul style="list-style-type: none"> Set to Disabled if there are no Repeaters in the network. Set to Enabled if any number of Repeaters exist in the network. <p>Important! Many advanced features of the FGR2-P, -PE, & -PE-U PLUS Radio are restricted in networks where the Repeaters parameter is set to Enabled.</p> <p>Note: For best operation, FreeWave does NOT recommend the use of single-radio Repeaters.</p>

5.1.12. Retry Timeout

Important! While intended primarily for MultiPoint networks, the **Retry Time Out** parameter may also be modified in Point-to-Point networks. However, the value in Point-to-Point mode should not be set to less than **151**.

Retry Timeout	
Setting	Description
Web Parameter:	Retry Timeout list box in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (7) Retry Timeout
Network Type:	Both
Default Setting:	255
Options:	Any number between 8 and 255 in MultiPoint networks. Any number between 151 and 255 in Point-to-Point networks.

Retry Timeout	
Setting	Description
Description:	<p>The Retry Time Out parameter in an Endpoint or Repeater sets the delay the unit waits before dropping the connection to a Gateway or Repeater in MultiPoint mode.</p> <ul style="list-style-type: none"> The maximum setting means that if 1 packet in 255 is received successfully, the link is maintained. The minimum setting is 8. <ul style="list-style-type: none"> This allows an Endpoint or Repeater to drop a connection if less than 1 in 8 consecutive packets is successfully received from the Gateway. With a setting of 255, the Gateway allows an Endpoint or Repeater to stay connected as long as 1 packet in 255 is successfully received at the Gateway. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>The Retry Time Out parameter is useful when a MultiPoint network has a roving Gateway or Endpoint(s). As the link gets weaker, a lower setting allows a poor link to break in search of a different link.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>FREEWAVE Recommends: Setting the Retry Time Out parameter to 20 in areas where several FreeWave networks exist. This setting allows Endpoints and Repeaters to drop the connection if the link becomes too weak, while preventing errant disconnects due to interference from neighboring networks.</p> </div>

5.1.13. RF Data Rate

Important! In MultiPoint networks, the **RF Data Rate** MUST be set identically in all radios.

- Any radio with an **RF Data Rate** different from the Gateway will not establish a link.
- In Point-to-Point networks, the Gateway's settings take precedence over the Endpoint.

RF Data Rate	
Setting	Description
Web Parameter:	RF Data Rate list box in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (8) RF Data Rate
Network Type:	Both
Default Setting:	154 kbps
Options:	<ul style="list-style-type: none"> 115 kbps 154 kbps

RF Data Rate	
Setting	Description
Description:	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Important! Do NOT confuse the RF Data Rate with the serial port Baud Rate.</p> </div> <ul style="list-style-type: none"> • Use a setting of 154 kbps when: <ul style="list-style-type: none"> • the radios are close together. • data throughput needs to be optimized. • A setting of 154 kbps MUST also be used when: <ul style="list-style-type: none"> • the full throughput of 92 kbps is necessary. • A setting of 115 kbps should be used when: <ul style="list-style-type: none"> • the radios are farther away. • a solid data link is preferred over data throughput. <p>The maximum available throughput is:</p> <ul style="list-style-type: none"> • ≈ 70 kbps at an RF Data Rate of 115 kbps. • ≈ 92 kbps at an RF Data Rate of 154 kbps.

5.1.14. Slave Attempts

Slave Attempts	
Setting	Description
Web Parameter:	Slave Connect Odds list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (C) Slave Connect Odds
Network Type:	MultiPoint
Default Setting:	9
Options:	Any number between 1 and 15.

Slave Attempts	
Setting	Description
Description:	<p>This setting, in conjunction with the Slave Connect Odds (on page 98) parameter, controls how the Endpoint retries sending its data when it fails to receive a connection acknowledgment from the Gateway.</p> <p>At each slot the Gateway is available, the Endpoint retries connecting with the Gateway. If the radio retries and still cannot connect with the Gateway, the cycle starts again.</p> <ul style="list-style-type: none"> • The odds determination can happen an unlimited number of times. • It is important in larger networks to help manage contention over connecting to the Gateway. • The higher the Slave Connect Odds parameter setting, the more persistent that Endpoint is in attempting to acquire the Gateway's connection. • This setting is a chance out of a total of 15. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Example: A setting of 1 means the radio has a 1 in 15 chance (6.66%) and a setting of 9 means a 9 in 15 chance (60%).</p> </div> <ul style="list-style-type: none"> • The maximum number of connection retries are determined by the Endpoint's Addressed Repeat (on page 83) and Broadcast Repeat (on page 84) parameter settings. • After the Endpoint has tried reconnecting with the Gateway for the number of Broadcast Repeats or Addressed Repeats (depending on the specific packet type), the Endpoint then takes the action listed in the Slave Connect Odds parameter.

5.1.15. Slave Connect Odds


Slave Connect Odds	
Setting	Description
Web Parameter:	Slave Connect Odds AND THEN list box in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (D) And Then
Network Type:	MultiPoint
Default Setting:	Drop Data

Slave Connect Odds	
Setting	Description
Options:	<ul style="list-style-type: none"> • Drop Data - The Endpoint throws away the current data it failed to send. <ul style="list-style-type: none"> • The pattern begins again upon receipt of new data. • Drop Link - The Endpoint drops its link with the Gateway or Repeater for a brief amount of time and then re-links. • Try Forever - The Endpoint waits a brief amount of time before starting again with the data retries. <ul style="list-style-type: none"> • It keeps retrying the same packet of data until it succeeds.
Description:	<p>This controls how the Endpoint retries sending its data when it fails to receive a connection acknowledgment from the Gateway.</p> <p>This can happen when multiple Endpoints are in contention for the Gateway's connection at the same time.</p> <ul style="list-style-type: none"> • In the Radio Setup window, the number in the first drop-down box in the Slave Connect Odds parameter indicates the odds that an Endpoint retries the connection on the Gateway's next available slot. • Contact FreeWave Technical Support to change this parameter. See Contact FreeWave Technical Support (on page 12).


5.1.16. Subnet ID

Note: See [Data Communication Link Examples \(on page 136\)](#) for additional subnet information and examples.

Subnet ID	
Setting	Description
Web Parameter:	Subnet ID (RX) and Subnet ID (TX) list boxes in the MultiPoint Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (H) Subnet ID (RX) (4) Radio Setup > (I) Subnet ID (TX)
Network Type:	MultiPoint using the Network ID option
Default Setting:	F, F in software earlier than 2.30 RX=0, TX=F in software 2.30 and later
Options:	<ul style="list-style-type: none"> • Any number between 0 and 9. • Any letter between A and F.

Subnet ID	
Setting	Description
Description:	<p>In a MultiPoint network with a Subnet ID (RX) of F and a Subnet ID (TX) of F, an Endpoint or Repeater connects with the first Repeater or Gateway that it hears with the same Network ID (on page 93).</p> <p>There are scenarios, however, where communication needs to be forced to follow a specific path.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Using Subnet IDs is particularly helpful to force two Repeaters in the same network to operate in series rather than in parallel or to force Endpoints to communicate to a specific Repeater for load balancing purposes.</p> </div>

5.1.17. Transmit Power

Transmit Power	
Setting	Description
Web Parameter:	Transmit Power list box in the Transmission Characteristics area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (6) Transmit Power
Network Type:	Both
Default Setting:	10
Options:	Any number between 0 and 10.
Description:	<p>Sets the output power of the radio.</p> <p>The maximum value may be capped at the factory to comply with regulations or capped at other values to comply with country-specific requirements.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>When testing radios and they are in close proximity to one another, set the Transmit Power parameter to a low number.</p> <p>When radios are deployed into the field, raise the Transmit Power number accordingly.</p> </div>

Transmit Power				
Setting	Power (in mW)		Setting	Power (in mW)
0	5		6	330
1	10		7	480
2	35		8	600
3	80		9	800
4	140		10	1000
5	230			

5.1.18. Transmit Rate

Transmit Rate	
Setting	Description
Web Parameter:	Transmit Rate list box in the Point-to-Point Parameters area of the Radio Setup window (on page 156) .
Terminal Menu:	(4) Radio Setup > (9) Transmit Rate
Network Type:	Point-to-Point
Default Setting:	Normal
Options:	<ul style="list-style-type: none"> • Normal - Use for normal radio operation. • Diagnostic - Use to qualitatively gauge signal strength in Point-to-Point mode. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important! In Point-to-Point operation, a Transmit Rate of Diagnostic should ONLY be used as a diagnostic tool and NOT for normal operation.</p> </div>
Description:	<p>When set to Diagnostic, the radios transmits back and forth continuously, whether or not the radios have received any actual data.</p> <ul style="list-style-type: none"> • The strength of the signal may be gauged by the Clear to Send (CTS) LED. • A solid red (■) CTS LED indicates a strong signal. • A blinking (⊖) CTS LED indicates a weaker signal.

6. Security Settings

Use the settings on the **Security** tab or [Security window](#) to define elements that enhance the security of the network, the data that is passed, and customer support information. Typically, a Network Administrator addresses security parameters.



Set the security settings using the **Security** menu in the terminal interface accessed through a terminal emulator.

Use the **Security** parameters to set these security features:

- **Remote Authentication Dial In Service (RADIUS) server information** - Requires authentication from Endpoints and MultiPoint Repeaters before being able to send or receive Ethernet data.
 - The radios comply with the RADIUS standards set forth in RFC 2138. The authentication method used in PLUS Radios is PAP.
 - RADIUS authentication allows control over which radios are allowed to communicate on the Ethernet network. Without authentication, an Endpoint or MultiPoint Repeater are not allowed to send or receive Ethernet data across its RF link.
- **AES Encryption** - Encodes the data in the network.
- **MAC Filtering** - Limits the addresses that can communicate with the radio through its Ethernet port.
- **System Logging** - The system automatically writes events to a local system log.
- **Miscellaneous Security Options** - Additional security options allow:
 - disabling the Ethernet port on a radio.
 - Force viewing of the configuration Web pages through a secure protocol (https).
 - Enabling a Gateway to transmit over the RF link and not the Ethernet port when data is received from specific radios in the network.

6.1. Viewing the System Log

As activity happens on a PLUS Radio, the system logs the activity.

Example: Each time a user logs into the [Configuration Windows](#) or a system upgrade is initiated, the system makes an entry in the log.

Note: The system log time is pulled from the NTP server, if the **NTP Client** setting in the IP Setup parameters is enabled.

If the **NTP Client** setting is disabled, the log date and time is reset to midnight, November 30, 1999, each time the radio reboots.

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu bar**, click **Security**.
The [Security window](#) opens.
3. In the **Customer Support Information** section, click **View Log**.

FREEWAVE D2+
192.168.111.100 * MAC=00:07:E7:82:B2:EF * Serial#=8565487
'admin' From 192.168.111.120

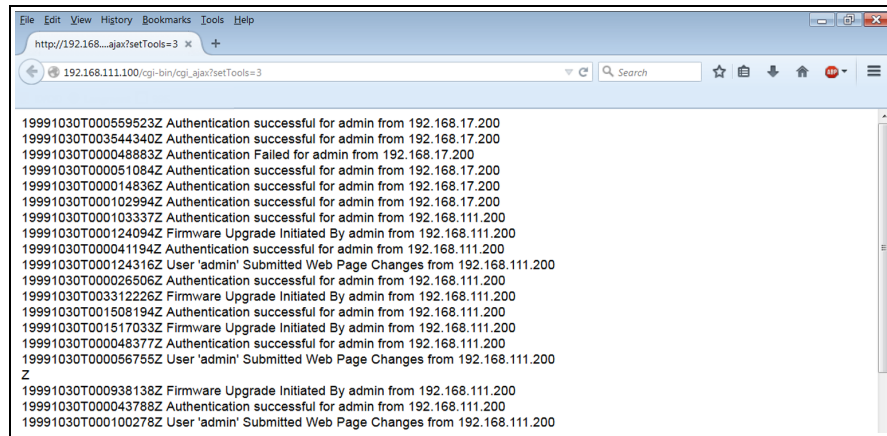
Status	RADIUS Authentication Configuration	
IP Setup	Enable RADIUS	<input type="checkbox"/> Enable
Serial Setup 1	RADIUS IP Address	<input type="text"/>
Serial Setup 2	RADIUS Port Number	1812
Radio Setup	Shared Secret	<input type="text"/>
Security	User-Password	<input type="text"/>
SNMP	Reboot interval	Disabled
	Customer Support Information	
	Syslog Dump	View Log
	System Memory Information	Memory Information

Save/Apply

©2006-2016 FreeWave Technologies, Inc.

Figure 33: FGR2-P, -PE, & -PE-U Security window

The log file opens in a new browser window.

**Figure 34: Example: View Log window**

6.2. Specify a Reboot Interval Schedule

In the [Security window \(on page 163\)](#), in the **Miscellaneous** area, use the **Reboot Interval** list box option to specify a reboot schedule.

- By default, the **Reboot Interval** is **Disabled**.
 - If **Disabled** is selected, the PLUS Radio will operate without automatically rebooting.
 - When an interval (e.g., **1 Hour**, **1 Day**, **30 Days**) is selected, the scheduler automatically reboots the PLUS Radio when the reboot interval expires.

Procedure

1. Follow the procedure for [Accessing the Configuration Windows \(on page 27\)](#).
The [Status window](#) opens.
2. On the **Menu** bar, click **Security**.
The [Security window](#) opens.
3. In the **Misc** section, click the **Reboot Interval** list box arrow and select the amount of time for the interval.

The screenshot shows the 'Security' configuration window for a device. The left sidebar contains navigation options: Status, IP Setup, Serial Setup 1, Serial Setup 2, Radio Setup, Security (highlighted), SNMP, Diagnostics, Users, and Tools. The main content area is titled 'RADIUS Authentication Configuration' and includes fields for 'Enable RADIUS' (checkbox), 'RADIUS IP Address', 'RADIUS Port Number' (1812), 'Shared Secret', and 'User-Password'. Below this is the 'AES Encryption' section with 'Version' (128) and 'Key' fields. The 'MAC Filter' section has 'Force SSL' (checkbox) and 'Peer To Peer' (checkbox). The 'Reboot interval' dropdown menu is circled in red and currently shows 'Disabled'. At the bottom, there are links for 'Syslog Dump' (View Log) and 'System Memory Information' (Memory Information), along with a 'Save/Apply' button. The footer indicates '©2006-2016 FreeWave Technologies, Inc.'

Figure 35: FGR2-P, -PE, & -PE-U Security window

Note: In this example procedure, 4 hours is selected.

D2+
192.168.111.100 * MAC=00:07:E7:82:B2:EF * Serial#=8565487
'admin' From 192.168.111.120

Navigation	Configuration
Status	RADIUS Authentication Configuration
IP Setup	Enable RADIUS <input type="checkbox"/> Enable
Serial Setup 1	RADIUS IP Address
Serial Setup 2	RADIUS Port Number 1812
Radio Setup	Shared Secret
Security	User-Password
SNMP	
	Misc
	Detach Local Eth <input type="checkbox"/> Detach
	Force SSL (https) <input type="checkbox"/> Enable
	Peer To Peer <input checked="" type="checkbox"/> Enable
	Reboot interval 4 Hour
	Customer Support Information
	Syslog Dump View Log
	System Memory Information Memory Information
	<input type="button" value="Save/Apply"/>

©2006-2016 FreeWave Technologies, Inc.

Figure 36: Example: View Log window

- Click the **Save/Apply** button.
The **Security** window refreshes showing the **Change Succeeded** and a **Reboot Required** messages.

D2+
192.168.111.100 * MAC=00:07:E7:82:B2:EF * Serial#=8565487
'admin' From 192.168.111.120

Navigation	Configuration
Status	RADIUS Authentication Configuration
IP Setup	Enable RADIUS <input type="checkbox"/> Enable
Serial Setup 1	RADIUS IP Address
Serial Setup 2	RADIUS Port Number 1812
Radio Setup	Shared Secret
Security	User-Password
	MAC Filter
	MAC Filter
	<input type="button" value="Add"/>
	<input type="button" value="Delete"/> <input type="button" value="Clear"/>
	Misc
	Detach Local Eth <input type="checkbox"/> Detach
	Force SSL (https) <input type="checkbox"/> Enable
	Peer To Peer <input checked="" type="checkbox"/> Enable
	Reboot interval 4 Hour
	Customer Support Information
	Syslog Dump View Log
	System Memory Information Memory Information
	<input type="button" value="Save/Apply"/>

Change Succeeded
Reboot Required

©2006-2016 FreeWave Technologies, Inc.

Figure 37: Security window - Change Succeeded and Reboot Required messages

- Click the **Reboot Required** link.
The **Rebooting** window appears.

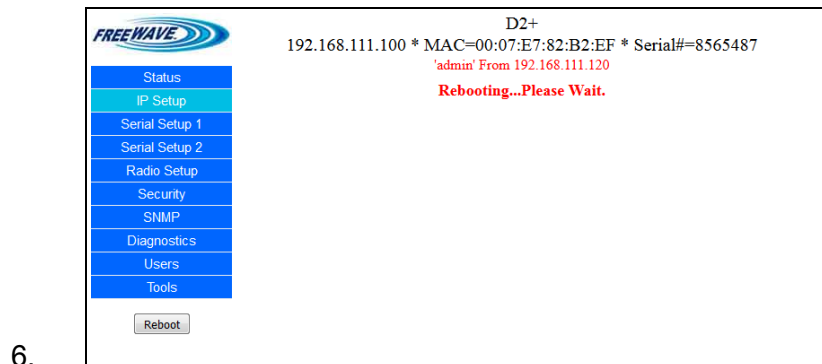


Figure 38: Rebooting message

7. Wait for the reboot to complete.
The **Status** window returns when the reboot is completed.

Hardware Information	
Firmware Version	3.13 Jul 1 2016
Wireless Version	+8.80a
Software Boot Version	3
Hardware Version	1
Country Code	7FFE
Uptime	0 days 0 hours 0 minutes 19 seconds
RF Stats	
Last Connected To	0
Noise	-115
Voltage	11.29v
Reflected Power	3
Disconnect Count	0 (0)

Figure 39: Status window

8. On the **Menu** bar, click **Security**.
The **Security window** opens.
The selected time is shown in the **Reboot Interval** list box.

FREEWAVE		D2+	
		192.168.111.100 * MAC=00:07:E7:82:B2:EF * Serial#=8565487	
		'admin' From 192.168.111.120	
Status	RADIUS Authentication Configuration		
IP Setup	Enable RADIUS	<input type="checkbox"/> Enable	
Serial Setup 1	RADIUS IP Address		
Serial Setup 2	RADIUS Port Number	1812	
Radio Setup	Shared Secret		
Security	User-Password		
SNMP	AES Encryption		
Diagnostics	Version	128	
Users	Key		
Tools	MAC Filter		
	MAC Filter	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Clear"/>	
	Misc		
	Detach Local Eth	<input type="checkbox"/> Detach	
	Force SSL (https)	<input type="checkbox"/> Enable	
	Peer To Peer	<input checked="" type="checkbox"/> Enable	
	Reboot interval	4 Hour	
	Customer Support Information		
	Syslog Dump	View Log	
	System Memory Information	Memory Information	
	<input type="button" value="Save/Apply"/>		
©2006-2016 FreeWave Technologies, Inc.			

Figure 40: Security window - Reboot Interval selected


6.3. Security Parameter Reference

This section contains the Security parameters.

Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.

6.3.1. AES Encryption Key

Important!: The encryption key MUST be the same on every radio in the FreeWave network.

AES Encryption Key	
Setting	Description
Web Parameter:	Key text box in the AES Encryption area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (5) Aes Key
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text using a maximum of 16 characters.
Description:	<p>Protecting the confidentiality, integrity, and authenticity of the data communication is essential to maintaining a robust, reliable, and secure wireless infrastructure.</p> <p>AES Encryption adds a layer of 128-bit or 256-bit encryption strength to the data before it is sent out via RF.</p> <ul style="list-style-type: none"> Enter a user-defined encryption key for the 128-bit AES encryption in this field. AES encryption is always enabled, although the encryption key may be blank. The AES Encryption field is a free form text field. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div> <p>When changing the AES encryption key globally:</p> <ol style="list-style-type: none"> Make the change on the MultiPoint Gateway. Push the new key to the other radios. <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p> Caution: If not done in this order, this change can cause radios to lose connectivity with the Gateway for an extended period of time.</p> </div>

6.3.2. AES Version

AES Version	
Setting	Description
Web Parameter:	AES Version list box in the AES Encryption area of the Security window (on page 163) .
Terminal Menu:	Not available
Network Type:	Both
Default Setting:	128-bit
Options:	128-bit - Enables AES encryption, 128-bit strength. 256-bit - Enables AES encryption, 256-bit strength.
Description:	<p>AES encryption is available in two strengths.</p> <ul style="list-style-type: none"> The network and the data sent determine the encryption strength that should be used. The higher the encryption strength, the stronger the encryption. <ul style="list-style-type: none"> It can also take longer for the encryption and de-encryption to take place. Remember to enter the encryption key. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: For more information, see AES Encryption Key (on page 109).</p> </div>

6.3.3. Detach Local Ethernet

Detach Local Ethernet	
Setting	Description
Web Parameter:	Detach Local Eth check box in the Misc area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (7) Detach Local Eth
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> Disabled Enabled
Description:	<p>If the Enabled check box is selected, the physical Ethernet port on the radio is disabled.</p> <p>With this parameter enabled, the radio can only be contacted via the radio link.</p>

6.3.4. Force SSL (https)




Force SSL (https)	
Setting	Description
Web Parameter:	Force SSL (https) check box in the Misc area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (8) Force SSL (https)
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<p>When the Force SSL (https) check box is selected, any attempt to access the radio's Website via HTTP is redirected to an HTTPS SSL connection.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This will encrypt the data between the radio and the web client, but will make the interface load and run more slowly.</p> </div>

6.3.5. MAC Filter



Warning! Use caution when entering MAC addresses in this list. Incorrect entries can lock the radio.

MAC Filter	
Setting	Description
Web Parameter:	MAC Filter scroll box in the MAC Filter area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (6) MAC Filter
Network Type:	Both
Default Setting:	Blank
Options:	Any valid MAC address.

MAC Filter	
Setting	Description
Description:	<p>Devices with MAC addresses in the MAC Filter parameter are permitted to communicate over the Ethernet port of the radio.</p> <ul style="list-style-type: none"> This list is specific for each radio and is used only in LANs. All other traffic is refused. If the MAC Filter parameter is blank, all traffic is allowed. <p>Add a MAC Address</p> <ol style="list-style-type: none"> Enter a hardware (MAC) address in the MAC Filter text box. MAC addresses contain six hexadecimal segments separated by colons. <p style="text-align: center;">Example: F0:4d:a2:6D:7F:2b.</p> <ol style="list-style-type: none"> Click  to add the MAC address into the MAC Filter list. <p>Delete a MAC Address</p> <ol style="list-style-type: none"> Select a MAC address in the MAC Filter list. Click  to remove that address from the list. <p>Delete all MAC Addresses</p> <p>Click  to remove every entry in the MAC Filter list.</p>

6.3.6. Peer To Peer

Peer To Peer	
Setting	Description
Web Parameter:	Peer To Peer check box in the Misc area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (9) Peer-to-Peer
Network Type:	Both
Default Setting:	Enabled
Options:	<ul style="list-style-type: none"> Disabled Enabled

Peer To Peer	
Setting	Description
Description:	<p>Select this check box to allow the Gateway to build a table of Ethernet devices connected over its radio link.</p> <ul style="list-style-type: none"> • When the Gateway receives a packet over its radio link, it compares the destination of that packet to its address table. • If the destination is found in the table, the Gateway re-transmits that packet over the radio link instead of applying it to the Ethernet port. • If disabled, data the Gateway receives over the radio link is always applied to the Ethernet port only.

6.3.7. RADIUS Enable

Note: This option is controlled from the Gateway only.
It has **no** functionality on Endpoints or MultiPoint Repeaters.

RADIUS Enable	
Setting	Description
Web Parameter:	Enable RADIUS check box in the RADIUS Authentication Configuration area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (0) Radius
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled

RADIUS Enable	
Setting	Description
Description:	<p>Select this check box to enable RADIUS authentication from the Endpoints or MultiPoints through the Gateway.</p> <ul style="list-style-type: none"> Enabling RADIUS authentication on the Gateway requires all of its Endpoints and MultiPoint Repeaters to authenticate to a central RADIUS server. The RADIUS server must be connected to the same LAN segment to which the Gateway is connected. The radios do NOT accept any authentication packets through their own Ethernet port. The ports are part of a hardware Ethernet switch that is integrated into the device. If the radio cannot connect with the RADIUS server, the radio (and its Configuration Windows (on page 151)) can still be reached via its IP address through the over-the-air portion of the network, with the local Ethernet access to the over-the-air portion of the network blocked. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important! For security purposes, if the radio cannot authenticate with the RADIUS server due to a bad password or other authentication credentials, the radio goes into offline mode, blocking all access. It reboots in five minutes.</p> </div>

6.3.8. RADIUS IP Address

Note: This option is controlled from the Gateway only. It has **no** functionality on Endpoints or MultiPoint Repeaters.

RADIUS IP Address	
Setting	Description
Web Parameter:	RADIUS IP Address text box in the RADIUS Authentication Configuration area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (1) Radius IP Address
Network Type:	Both
Default Setting:	Blank
Options:	Any valid IP address.
Description:	<p>This is the IP address of the RADIUS server.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Important! DNS names are NOT accepted.</p> </div>

6.3.9. RADIUS Port

Note: This option is controlled from the Gateway only.
It has **no** functionality on Endpoints or MultiPoint Repeaters.

RADIUS Port	
Setting	Description
Web Parameter:	RADIUS Port Number text box in the RADIUS Authentication Configuration area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (2) Radius Port
Network Type:	Both
Default Setting:	1812
Options:	Any valid port number between 0 and 65535.
Description:	This is the port number of the RADIUS server's authentication port.

6.3.10. Reboot Interval

Reboot Interval	
Setting	Description
Web Parameter:	Reboot Interval list box in the Misc area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (10) Reboot Interval
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • 1, 2, 4, 8, 12 Hour • 1, 2, 4, 7, 14, 30 Days
Description:	Click the list box arrow and select the interval of time between the reboot of the FGR2-P, -PE, & -PE-U.

6.3.11. Shared Secret

Note: This option is used on Endpoints and MultiPoint Repeaters only.
It has **no** functionality on Gateways.

Shared Secret	
Setting	Description
Web Parameter:	Shared Secret text box in the RADIUS Authentication Configuration area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (3) Shared Secret

Shared Secret	
Setting	Description
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text.
Description:	<p>This is the secret for the RADIUS server.</p> <ul style="list-style-type: none"> Enter the IP address of the radio in the RADIUS server's Clients file. Each radio acts as a client when accessing the RADIUS server for authentication. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

6.3.12. User Password

Note: This option is used on Endpoints and MultiPoint Repeaters only. It has **no** functionality on Gateways.

User Password	
Setting	Description
Web Parameter:	User-Password text box in the RADIUS Authentication Configuration area of the Security window (on page 163) .
Terminal Menu:	(5) Security > (4) User-Password
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text.
Description:	<p>The RADIUS password for the radio.</p> <ul style="list-style-type: none"> An entry for the radio should be created in the RADIUS server's Users file. The radio always reports its serial number, minus any hyphens, as its User Name. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7. SNMP Settings

Use the Simple Network Management Protocol (SNMP) settings located in the SNMP tab or [SNMP window](#) to monitor the state of the radio for conditions that may require special attention. The information in this section assumes familiarity with SNMP and its use.

Note: Each of the SNMP-manageable objects is also contained in the FREEWAVE-TECHNOLOGIES-MIB file that can be imported into the system. The basic description of each element available in that file is available in [Object List for FREEWAVE-TECHNOLOGIES-MIB on page 201](#). The file is available from FreeWave upon request.

Defining SNMP management conditions requires:

- **SNMP Agent Information** - SNMP version and passwords.
- **Trap Configuration** - The fault time and the IP address of the location that is gathering the fault conditions.
- **Trap Limits** - The high and low limits after which a fault occurs.

This section includes:

- [SNMP Parameter Reference \(on page 118\)](#)
- [SNMP Trap Limits Parameter Reference \(on page 123\)](#)

7.1. SNMP Parameter Reference

This section contains the SNMP parameters.

Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.

7.1.1. Authentication Method

Note: This option is only available when **v3** is selected in the [SNMP Version on page 120](#).

Authentication Method	
Setting	Description
Web Parameter:	List box next to the Authentication Password text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (4) Version
Network Type:	Both
Default Setting:	MD5
Options:	MD5, SH1
Description:	Select the encryption algorithm for the SNMP agent.

7.1.2. Authentication Password (v3)

Note: This option is only available when **v3** is selected in the [SNMP Version on page 120](#).

Authentication Password (v3)	
Setting	Description
Web Parameter:	Authentication Password (v3) text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (3) Authentication Password
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text
Description:	<ul style="list-style-type: none"> This is the password needed for SNMP v3 authentication. The password must be at least 8 characters in length. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7.1.3. Min Fault Time

Min Fault Time	
Setting	Description
Web Parameter:	Min fault Time (Seconds) list box in the SNMP Trap Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (9) Min Fault Time
Network Type:	Both
Default Setting:	300
Options:	30, 60, 90, 120, 150, 180, 210, 240, 270, and 300 seconds
Description:	Select the amount of time a trap condition must be continuously present before an SNMP trap is sent to the Trap Managers.

7.1.4. Privacy Method

Privacy Method	
Setting	Description
Web Parameter:	List box next to the Privacy Password text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (6) Version
Network Type:	Both
Default Setting:	AES
Options:	<ul style="list-style-type: none"> • AES • DES
Description:	Select the encryption algorithm for the SNMP Agent.

7.1.5. Privacy Password (v3)

Note: This option is only available when **v3** is selected as the [SNMP Version on page 120](#).

Privacy Password (v3)	
Setting	Description
Web Parameter:	Privacy Password text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (5) Privacy Password
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text.

Privacy Password (v3)	
Setting	Description
Description:	<ul style="list-style-type: none"> This is the password needed for SNMP v3 privacy. The password must be at least 8 characters in length. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7.1.6. Read Community

Read Community	
Setting	Description
Web Parameter:	Read Community text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (1) Read Community
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text using a maximum of 25 characters.
Description:	<ul style="list-style-type: none"> Enter the SNMP community name that has read access. The Read Community text box is also used for the SNMPv3 username when reading SNMP information. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7.1.7. SNMP Version

SNMP Version	
Setting	Description
Web Parameter:	SNMP Version list box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (0) SNMP Version
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> Disabled v1 v2 v3

SNMP Version	
Setting	Description
Description:	The version of the Simple Network Protocol (SNMP) currently used.

7.1.8. Trap Community

Trap Community	
Setting	Description
Web Parameter:	Trap Community text box in the SNMP Trap Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (8) Trap Community
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text.
Description:	Enter the SNMP Community name that has trap access. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7.1.9. Trap Manager IP

Trap Manager IP	
Setting	Description
Web Parameter:	Trap Manager 1 IP and Trap Manager 2 IP text boxes in the SNMP Trap Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (A) Trap Manager 1 IP (6) SNMP > (B) Trap Manager 2 IP
Network Type:	Both
Default Setting:	0.0.0.0
Options:	Any valid IP address.
Description:	Enter the IP addresses of the authorized SNMP Trap Managers. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: DNS names are NOT accepted.</p> </div>

7.1.10. Trap Version

Trap Version	
Setting	Description
Web Parameter:	Trap Version list box in the SNMP Trap Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (7) Trap Version
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • v1 • v2
Description:	Select the trap version supported by the SNMP Agent.

7.1.11. Write Community

Write Community	
Setting	Description
Web Parameter:	Write Community text box in the SNMP Agent Configuration area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (2) Write Community
Network Type:	Both
Default Setting:	Blank
Options:	Any free form text up to 25 characters.
Description:	Enter the SNMP community name that has write access. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: Free form text fields CANNOT use any of these characters: % & + = < ></p> </div>

7.2. SNMP Trap Limits Parameter Reference

This section contains the high and low trap limits.

- In the [Configuration Windows](#), use the check boxes and list boxes in the **SNMP Trap Limits** section of the SNMP page to set the trap limits.

Note: See the [Parameter Preference \(on page 13\)](#) for the parameter table descriptions of the parameters and controls.

7.2.1. Delta Alarm Enable

Delta Alarm Enable	
Setting	Description
Web Parameter:	S-N Delta Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (L) S-N Delta Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<p>Enables a trap for the calculated difference between the signal level and the noise level of the radio.</p> <p>The trap condition is present based on the settings in the Delta Alarm Below parameter.</p>

7.2.2. Delta Alarm Below

Delta Alarm Below	
Setting	Description
Web Parameter:	S-N Delta Alarm Below list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (K) Below
Network Type:	Both
Default Setting:	30
Options:	Any whole number between 10 and 40 in increments of 5.
Description:	<p>If the Delta Alarm Enable on page 123 parameter is set to Enabled, a trap condition occurs if the calculated difference between the radio's signal level and noise level goes below the value selected in this parameter.</p>

7.2.3. Noise Alarm Above

Noise Alarm Above	
Setting	Description
Web Parameter:	Noise Alarm Above list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (Q) Above
Network Type:	Both
Default Setting:	-100
Options:	Any whole, negative number between -100 and -70 in increments of 5.
Description:	If the Noise Alarm Enable (on page 124) parameter is set to Enabled , a trap condition occurs if the noise level goes above the value set in this parameter.

7.2.4. Noise Alarm Enable

Noise Alarm Enable	
Setting	Description
Web Parameter:	Noise Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (P) Noise Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enables a trap for the noise level of the radio. The trap condition is present based on the setting in the Noise Alarm Above (on page 124) .

7.2.5. Reflected Alarm Above

Reflected Alarm Above	
Setting	Description
Web Parameter:	Reflected Power Above list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (K) Above
Network Type:	Both
Default Setting:	2
Options:	Any whole number between 0 and 40 in increments of 2 (i.e., 2, 4, 6, 8, etc.)

Reflected Alarm Above	
Setting	Description
Description:	If the Reflected Alarm Enable (on page 125) parameter is set to Enabled , a trap condition occurs if the reflected power goes above the value in this parameter.

7.2.6. Reflected Alarm Enable

Reflected Alarm Enable	
Setting	Description
Web Parameter:	Reflected Power Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (J) Reflected Power Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	<p>Enables a trap for the reflected power of the radio.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: The trap condition is present based on the settings in the Reflected Alarm Above (on page 124).</p> </div>

7.2.7. Rx Rate Alarm Below

Rx Rate Alarm Below	
Setting	Description
Web Parameter:	Rx % Rate Below list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (G) Below
Network Type:	Both
Default Setting:	90
Options:	Any percentage between 50 and 100 in increments of 5 (i.e., 5, 10, 15, 20, etc.)
Description:	If the Rx Rate Alarm Enable (on page 126) parameter is set to Enabled , a trap condition occurs if the receive percent goes below the value set in this parameter.

7.2.8. Rx Rate Alarm Enable

Rx Rate Alarm Enable	
Setting	Description
Web Parameter:	Rx % Rate Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (F) Rx % Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enables a trap for the receive percentage of the radio. The trap condition is present based on the settings in the Rx Rate Alarm Below (on page 125) .

7.2.9. Signal Alarm Below

Signal Alarm Below	
Setting	Description
Web Parameter:	Signal Alarm Below list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (0) Below
Network Type:	Both
Default Setting:	-90
Options:	Any whole, negative number between -100 and -70 in increments of 5.
Description:	If the Signal Alarm Enable on page 126 parameter is set to Enabled , a trap condition occurs if the signal level goes below the value set in this parameter.

7.2.10. Signal Alarm Enable

Signal Alarm Enable	
Setting	Description
Web Parameter:	Signal Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (N) Signal Trap
Network Type:	Both
Default Setting:	Disabled

Signal Alarm Enable	
Setting	Description
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enables a trap for the signal level the radio reports. The trap condition is present based on the settings in the Signal Alarm Below (on page 126) .

7.2.11. Tx Rate Alarm Below

Tx Rate Alarm Below	
Setting	Description
Web Parameter:	Tx % Rate Below list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (I) Below
Network Type:	Both
Default Setting:	90
Options:	Any percentage between 50 and 100 in increments of 5.
Description:	If the Tx Rate Alarm Enable on page 127 parameter is set to Enabled , a trap condition occurs if the transmit percent goes below the value set in this parameter.

7.2.12. Tx Rate Alarm Enable

Tx Rate Alarm Enable	
Setting	Description
Web Parameter:	Tx % Rate Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (H) Tx % Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enables a trap for the transmit percentage of the radio. The trap condition is present based on the settings in the Tx Rate Alarm Below (on page 127) .

7.2.13. Voltage Alarm Above

Voltage Alarm Above	
Setting	Description
Web Parameter:	Voltage Alarm Above list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (D) Above
Network Type:	Both
Default Setting:	30
Options:	Any whole number between 6 and 30.
Description:	If the Voltage Alarm Enable on page 128 parameter is set to Enabled , a trap condition occurs if the voltage goes above the value set in this parameter.

7.2.14. Voltage Alarm Below

Voltage Alarm Below	
Setting	Description
Web Parameter:	Voltage Alarm Below list box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (E) Below
Network Type:	Both
Default Setting:	6
Options:	Any whole number between 6 and 30 VDC.
Description:	If the Voltage Alarm Enable on page 128 parameter is set to Enabled , a trap condition occurs if the voltage goes below the value set in this parameter.

7.2.15. Voltage Alarm Enable

Voltage Alarm Enable	
Setting	Description
Web Parameter:	Voltage Enable check box in the SNMP Trap Limits area of the SNMP window (on page 173) .
Terminal Menu:	(6) SNMP > (C) Voltage Trap
Network Type:	Both
Default Setting:	Disabled
Options:	<ul style="list-style-type: none"> • Disabled • Enabled
Description:	Enables a trap for the supply voltage of the radio. The trap condition is present based on the settings in the Voltage Alarm Above (on page 128) and Voltage Alarm Below (on page 128) .

8. Viewing Radio Status and Statistics

A PLUS Radio's status and statistics are available on the [Status window on page 175](#).

Note: This window is read-only and cannot be changed.

This information appears in the header at the top of each window:

- Radio model (pink highlight).

Note: This example image shows the HT-P / PE and HTP900 **Status** window. The header information is the same for the FGR2-P / PE window.

- IP address (blue highlight).
- MAC (hardware address-green highlight).
- Serial number for the radio (orange highlight).
- The user currently logged in (yellow highlight).
- The IP address logging into the radio (yellow highlight).


		HT+	
192.168.111.100 *		MAC=00:07:E7:87:31:EB *	
		Serial#=8860139	
		'admin' From 192.168.111.200	
Status	Hardware Information		
IP Setup			
Serial Setup 1	Firmware Version	3.01.15 Dec 2 2014	
Serial Setup 2	Wireless Version	+7.71i	
Radio Setup	Software Boot Version	3	
	Hardware Version	1	

Figure 41: FGR2-P, -PE, & -PE-U Header Information



Use the [Diagnostics window](#) to view the signal level, noise level, signal-to-noise difference, and receive rate for each frequency available on the radio.

Note: When viewing diagnostic information for a Point-to-MultiPoint Gateway, the header page always shows **I am currently not connected**.

8.1. Refreshing and Resetting Statistics

To refresh the contents of the Status page automatically, select the **Auto Refresh Page** check box at the bottom of the page.

- When this check box is selected, the **Status** page is updated approximately every 10 seconds to reflect the current state of the radio.
- By default, this check box is NOT selected and the **Status** page does NOT automatically refresh.

Note: Navigating away from the **Status** page causes the **Auto Refresh page** to revert to its deselected default.

To reset all the statistics on the [Status window](#) to **0**, click the **Reset** button.

8.2. Available Statistics

8.2.1. admin From

The serial number of the radio's upstream connection, (e.g., the network Gateway or a Repeater).

Note: This information appears in the header of the [Status window on page 175](#).

8.2.2. Bad Packets

The number of Ethernet packets the radio has thrown away due to a bad CRC checksum.

8.2.3. Broadcast Packets

The number of packets sent over the radio where the broadcast address was the packet destination.

8.2.4. Connected To

The serial number of the radio's upstream connection (e.g., the network Gateway or a Repeater).

Note: This statistic is a 0 (zero) in a Multipoint Gateway.

8.2.5. Disconnect Count

Note: This statistic is NOT valid in MultiPoint Gateways or Point-to-Point Repeaters.

This is the number of times the radio has lost its RF connection to its upstream connection.

8.2.6. Distance

The distance between this radio and the radio to which it is directly linked.

- Distances greater than 3/5 of a mile are typically accurate to within 100 feet.
- Shorter distances are not reported accurately.

8.2.7. Firmware Version

The current version number of the firmware revision installed on the radio.

Note: For information about upgrading the software, see [Upgrading the FGR2-P, -PE, & -PE-U PLUS Radio Software Using a TFTP Server](#).

8.2.8. Hardware Version

For internal FreeWave use.

Note: A Technical Support representative may ask for this information.

8.2.9. Noise

The level of background noise and interference at this radio.

- The number is an average of the noise levels measured at each frequency in the radio's frequency hop table.
- Ideally, noise levels should be below -80 dBm.

FREEWAVE Recommends: The difference between the average signal level and average noise level should be 30 dBm or more.

- Noise levels significantly higher than this are an indication of a high level of interference that may degrade the performance of the link.
- High noise levels can often be mitigated with band pass filters, antenna placement, or antenna polarization.

8.2.10. Notes

Any additional information provided about the radio as defined in the **Notes** parameter on the [Tools window \(on page 178\)](#).

Note: For more information, see [Providing Site Information \(on page 32\)](#).

8.2.11. Packets Dropped

The number of Ethernet packets the radio has thrown away because its data buffer is full.

8.2.12. Packets Sent

The number of Ethernet packets and bytes of data the radio has sent over its radio link.

8.2.13. Peer to Peer Packets

Note: This statistic is only valid in a MultiPoint Gateway.

The number of packets the Gateway has received from the radio link and re-transmitted out, as the destination address was determined to be across the radio link.

8.2.14. Radio Addressed Packets

The number of packets sent over the radio where another radio in the wireless network was the packet destination.

8.2.15. Radio Parse Error

The number or errors in data transmission between the Ethernet stack and the radio interface.

8.2.16. Received

The number of Ethernet packets and bytes of data the radio has received over its radio link.

8.2.17. Reflected Power

A measurement of the transmitted power that is reflected back into the radio from mismatched antennas, mismatched cables, or loose connections between the radio and the antenna.

Reflected Power	
Reading	Value
0 to 5	Good
5 to 29	Acceptable to marginal
30+	Unacceptable

Important! Indicates that the connections should be inspected for loose connectors and cable quality.

8.2.18. RX Success Rate

Note: This statistic is only valid in a MultiPoint network.

- This is the percentage of packets this radio has successfully received.
- This statistic displays **0.00%** in a MultiPoint Gateway.

FREEWAVE Recommends: A minimum **75%** success rate for proper radio operation.

8.2.19. RX Throughput

The throughput of data being received over the radio link within the last 1 second.

8.2.20. Signal

The level of received signal at this radio.

- The signal source is the radio that transmits to this radio, shown in the **Connected To** field.
- The number is an average of the received signal levels measured at each frequency in the radio's frequency hop table.

FREEWAVE Recommends: For a reliable link, the margin between the average signal level and average noise level should be **30 dBm** or more.

- Low average signal levels can often be corrected with higher gain antennas, better antenna placement, and/or additional Repeaters.

Note: See the installation manual for antenna and FCC requirements.

8.2.21. Site Contact

The contact information for the radio as defined in [Providing Site Information \(on page 32\)](#).

8.2.22. Site Name

The name of the radio's site as defined in [Providing Site Information \(on page 32\)](#).

8.2.23. Software Boot Version

For internal FreeWave use.

Note: A Technical Support representative may ask for this information.

8.2.24. System Name

The name of the system in which the radio resides as defined in [Providing Site Information \(on page 32\)](#).

8.2.25. Temperature

The current operating temperature of the radio in both degrees Celsius and degrees Fahrenheit.

8.2.26. TX Success Rate

Note: This statistic is only valid on MultiPoint Endpoints.

- This is the percentage of packets the radio has sent that successfully reached the upstream radio (e.g., the Gateway or a Repeater).
- This statistic shows **0.00%** on a MultiPoint Gateway or MultiPoint Repeater.

FREEWAVE Recommends: A minimum of **75%** success rate for proper radio operation.

8.2.27. TX Throughput

The throughput of data being transmitted over the radio link within the last 1 second.

8.2.28. Un-Acked Packets

The number of Ethernet packets sent using a broadcast MAC address.

Note: The destination device does NOT acknowledge these packets.

In a network where the **Repeaters** parameter is set to **Enabled**, all packets become unacknowledged, and this statistic displays a high number of packets.

In a network where the **Repeaters** parameter is set to **Disabled**, this statistic can indicate:

- On the Gateway, this statistic shows a packet that is addressed to a device the Gateway believes is on its wireless network, the Gateway has exhausted all of its packet retries, and the Gateway never received any acknowledgments for that packet. Reasons for this include the following:
 - The destination address is not actually in the wireless network.
 - The destination could not hear the packet from the Gateway.
 - The Gateway could not hear the acknowledgment from the destination.
- On an Endpoint, this statistic shows a packet that is being sent to the Gateway, the Endpoint has received no acknowledgments from the Gateway, and the Endpoint has exhausted its maximum number of attempts per the **Slave Connect Odds** parameter.

It is still possible that any packet included in this statistic was successfully delivered, but the radio is unable to obtain an acknowledgment that the packet succeeded.

8.2.29. Upstream Noise

The value refers to the amount of noise between the FGR2-P, -PE, & -PE-U device and the upstream device.

Note: This information is only available if the FGR2-P, -PE, & -PE-U device is a Repeater or and Endpoint.

8.2.30. Upstream Signal

The value refers to the signal strength between the FGR2-P, -PE, & -PE-U device and the upstream device.

Note: This information is only available if the FGR2-P, -PE, & -PE-U device is a Repeater or and Endpoint.

8.2.31. Uptime

This is the total time the radio has been running since the last reboot.

8.2.32. Voltage

The voltage level of the power being supplied to the radio.

8.2.33. Wireless Version

This identifies the current version number of the Radio Frequency module's software.

9. Data Communication Link Examples

A FreeWave radio's versatility allows data communication links to be established using a variety of different configurations.

- [Example 1: Gateway to Endpoint \(on page 137\)](#).
- [Example 2: Gateway, Repeater, and Endpoint \(on page 137\)](#).
- [Example 3: Gateway, Two Repeaters, and Endpoint \(on page 138\)](#).
- [Example 4: Gateway, Repeater, and Multiple Endpoints \(on page 139\)](#).
- [Example 5: Standard Point-to-MultiPoint Network \(on page 140\)](#).
- [Example 6: Point-to-MultiPoint Network with an Endpoint/Repeater Site \(on page 141\)](#).

Note: Subnet examples are here: [Assigning Subnet Values on page 142](#).

9.1. Example 1: Gateway to Endpoint

This example shows the most common and straight forward link; a Gateway communicating to an Endpoint in a Point-to-Point link.

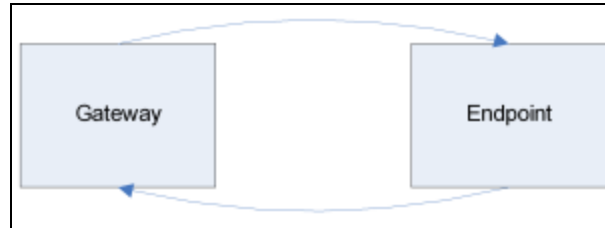


Figure 42: Example 1: Gateway to Endpoint

9.2. Example 2: Gateway, Repeater, and Endpoint

This example shows how a link might be set up using a Repeater.

- The Repeater may be located on a hilltop or other elevated structure enhancing the link from the Gateway to the Endpoint.
- In this configuration, it may be desirable to use an external Omni-directional antenna at the Repeater.
 - Yagi antennas may be used at both the Gateway and Endpoint radios.
- When a Repeater is used, the RF throughput is cut in half.

Important! Adding a Repeater to a network cuts the network throughput by 50%.

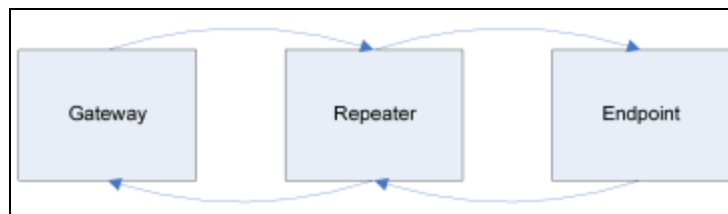


Figure 43: Example 2: Gateway, Repeater, Endpoint

9.3. Example 3: Gateway, Two Repeaters, and Endpoint

This example shows a link with two Repeaters between the Gateway and Endpoint.

- With two Repeaters, there is clearly more flexibility in getting around obstacles and greater total range is possible.
- When two Repeaters are used, there is no further degradation in the RF throughput of the link.



Use external Omni-directional antennas with the Repeaters.
Attach a Yagi to the Gateway and Endpoint to increase the range of the link.

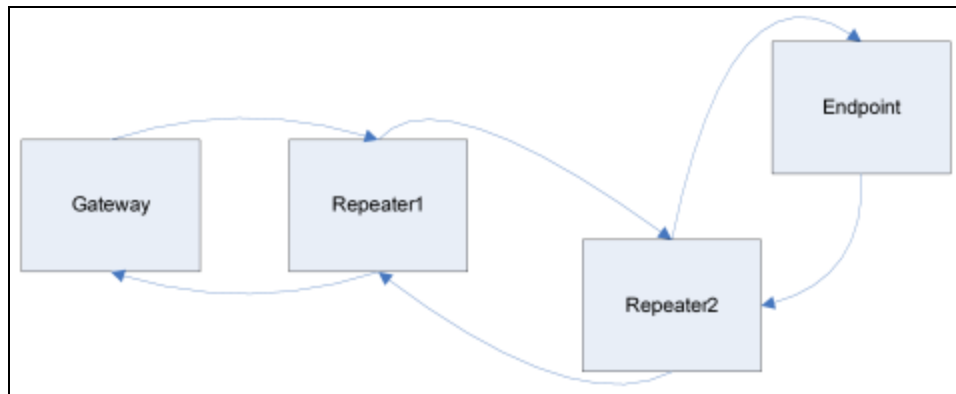


Figure 44: Example 3: Gateway, Two Repeaters, and Endpoint

9.4. Example 4: Gateway, Repeater, and Multiple Endpoints

This example shows a configuration where a Gateway routinely calls a number of Endpoints at different times.

- The Gateway is communicating with a radio designated as an Endpoint/Repeater that is connected to a remote device.
- Since this device is placed in an elevated location, the radio may also be used as a Repeater when it is not used as an Endpoint.
- At any time the Gateway may call any of the Endpoints, establish a connection, and send and receive data.

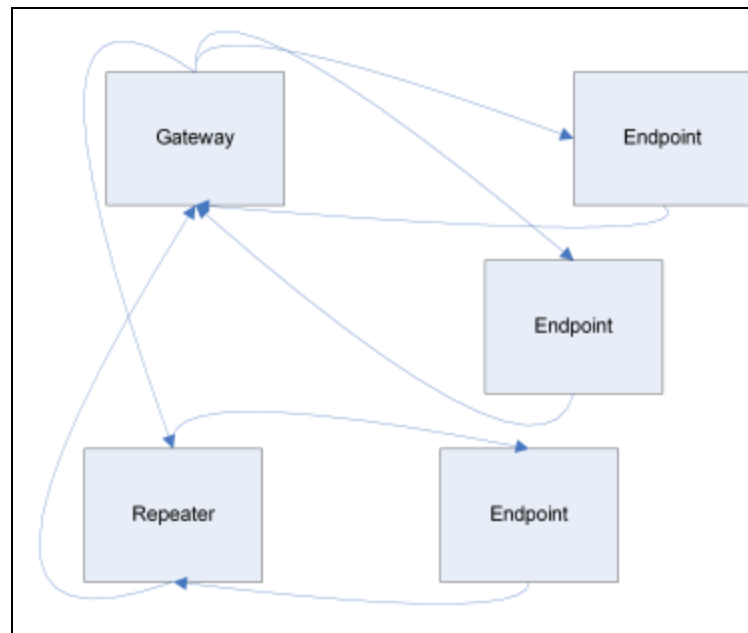


Figure 45: Example 4: Gateway, Repeater, and Multiple Endpoints

9.5. Example 5: Standard Point-to-MultiPoint Network

This example shows a standard Point-to-MultiPoint network.

- From the Gateway, any data is broadcast to all three Endpoints, one of which receives it through a MultiPoint Repeater.
- The data is sent out of the serial port of each of the three Endpoints.
- The end device should be configured to interpret the serial message and act on it, if necessary.

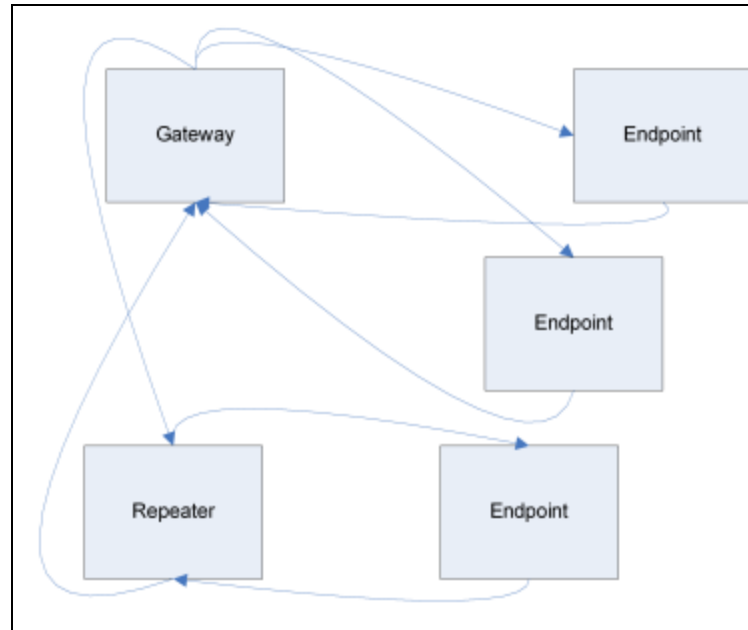


Figure 46: Example 5: Standard Point-to-MultiPoint Network

9.6. Example 6: Point-to-MultiPoint Network with an Endpoint/Repeater Site

This example is a Point-to-MultiPoint network which uses one of the sites as an Endpoint/Repeater.

- This network functions in the same manner as a standard MultiPoint network with Repeaters.
- However, the number of radios may be reduced with the use of the MultiPoint Endpoint/Repeater feature.

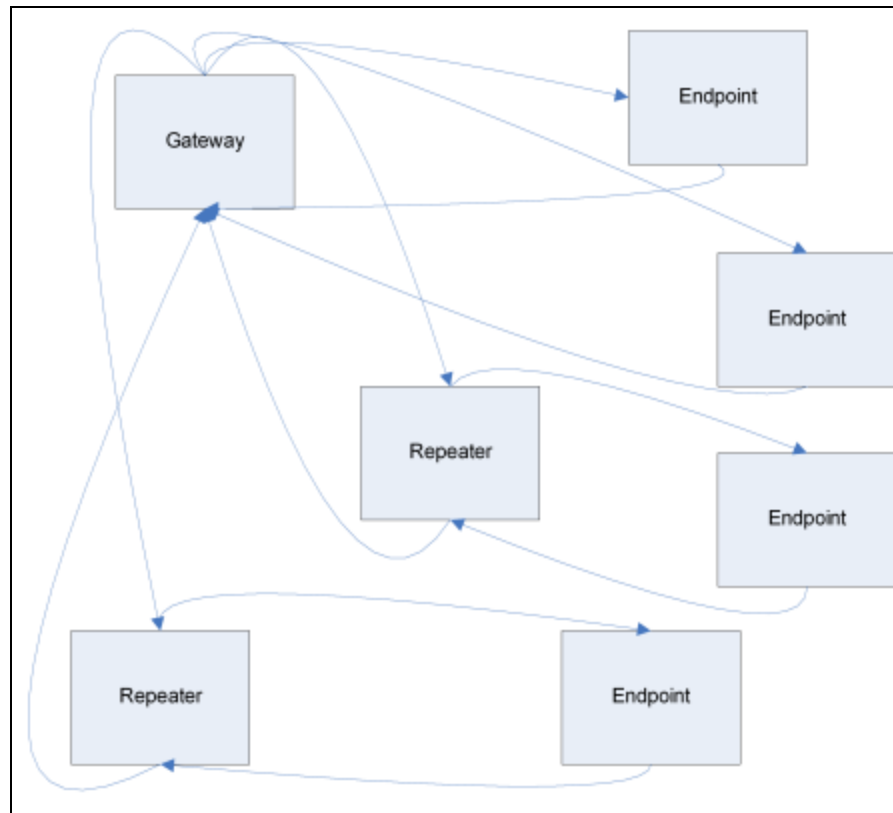


Figure 47: Example 6: Point-to-MultiPoint Network with an Endpoint/Repeater Site

Note: A poor signal path can cause a link to drop or miss data.

If a re-transmit of the missed data is required, this takes time and can cause the network to slow. When the radio network is designed, ensure that the links are set up at optimal distances to ensure good signal quality throughout the network.

9.7. Assigning Subnet Values

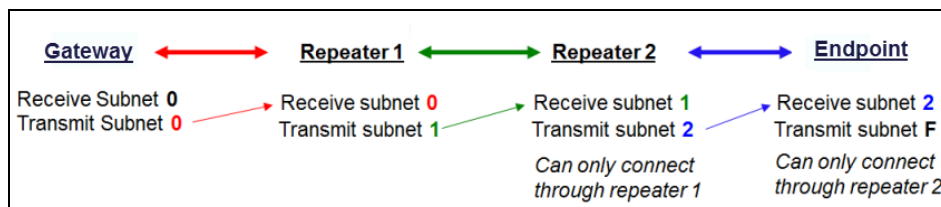
Subnet IDs consist of two parts, both available in the **Multipoint Parameters** area of the [Radio Setup window](#):

- **Rx** - This setting identifies the radio a Repeater or Endpoint listens to.
- **Tx** - This setting identifies the ID this device transmits on and which devices listen to it.
 - The **Tx Subnet ID** parameter is **only** relevant for MultiPoint Gateway radios and Repeaters.
- The default (disable) setting for both **Rx** and **Tx** is **F,F**.
 - This is a visual way to indicate that the device is the final in the line of communication and does NOT use a subnet ID.
- A MultiPoint Endpoint with a **Subnet ID** of **F,F** does NOT roam from one Repeater or network to the next.
 - It only links to a Gateway or Repeater that has either a **Tx** setting of **0 (zero)** or an **F, F Subnet ID**.
- Setting both the **Rx** and **Tx Subnet ID** to **0** allows a mobile Endpoint to roam from subnet to subnet, and possibly from network to network, provided the **Network ID**, **Max and Min Packet Size**, and **RF Data Rates** are the same between networks.

The examples in this section show the subnet definitions from the Gateway radio through the network to the Endpoint radios. When the subnet path is defined, the Endpoint radios can follow the route back to the Gateway.

9.7.1. Subnet Example 1

This example shows a network where subnet IDs are used to force communications along a specific path.

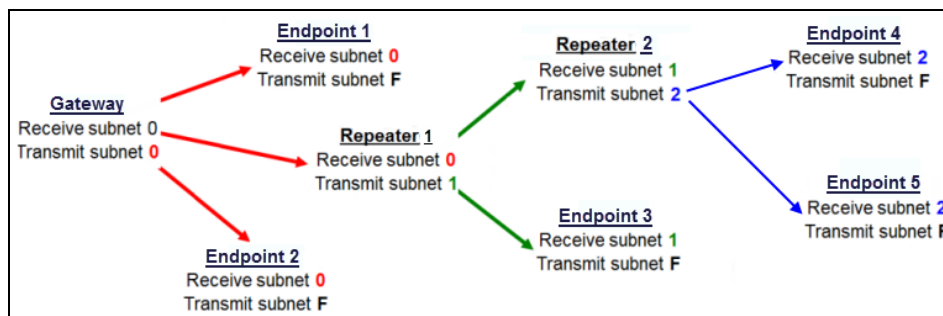


Subnet ID Settings for This Example			
Radio	Rx	Tx	Additional Information
Gateway	0	0	The default settings (F, F) actually use 0, 0. The Rx Subnet on the Gateway has no effect on the network.
Repeater1	0	1	A 0 (zero) forces the radio to link only to the Gateway.
Repeater2	1	2	Rx Subnet = 1 forces communication through Repeater 1. Repeater 1 transmits on subnet 2 .
Endpoint	2	F	Rx Subnet = 2 forces communication through Repeater 2. The Endpoint is the end of the network, so its Tx Subnet is F .

9.7.2. Subnet Example 2

In this example:

- Repeater 2 must communicate through Repeater 1.
- The Endpoint connected to Repeater 1 must route through Repeater 1.
- The other two Endpoint radios must route through Endpoint/Repeater 2.

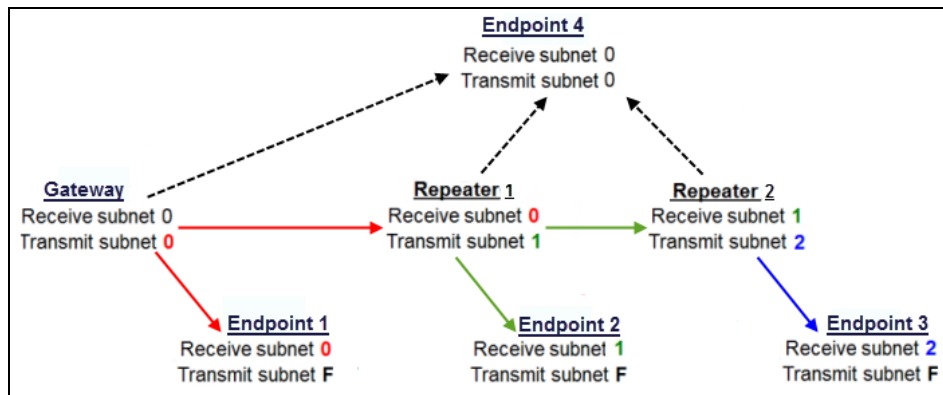


Subnet ID Settings for This Example			
Radio	Rx	Tx	Additional Information
Gateway	0	0	The default settings (F, F) actually use 0, 0. The Rx Subnet on the Gateway has no effect on the network.
Endpoint 1	0	F	Rx Subnet = 0 forces the radio to link only to the Gateway. The Endpoint does NOT transmit to any device except the Gateway, so its Tx Subnet is F.
Repeater 1	0	1	Rx Subnet = 0 forces the radio to link only to the Gateway. Transmits on subnet 1.
Endpoint 2	0	F	Rx Subnet = 0 forces the radio to link only to the Gateway.
Endpoint / Repeater 2	1	2	Rx Subnet = 1 forces the radio to link only to Repeater 1. It transmits on Tx Subnet 2 to Endpoint 4 and 5.
Endpoint 3	1	F	Rx Subnet = 1 forces the radio to link only to Repeater 1. The Endpoint does not transmit to any device except Repeater 1, so its Tx Subnet is F.
Endpoint 4	2	F	Rx Subnet = 2 forces the radio to link with Endpoint/Repeater 2.
Endpoint 5	2	F	Rx Subnet = 2 forces the radio to link with Endpoint/Repeater 2.

9.7.3. Subnet Example 3

In this example:

- Repeater 1 must talk directly to the Gateway.
- Repeater 2 must talk directly to Repeater 1.
- Endpoint 1, 2, and 3 are forced along the direction of the solid lines.
- Endpoint 4 may link to the first Gateway or Repeater it hears in the network.



Subnet ID Settings for this Example			
Radio	Rx	Tx	Additional Information
Gateway	0-F	0-F	The default settings (F, F) actually use 0, 0. The Rx Subnet on the Gateway has no effect on the network.
Repeater 1	0	1	A 0 forces the radio to link only to the Gateway.
Repeater 2	1	2	Rx Subnet = 1 forces communication through Repeater 1. Repeater 1 transmits on Subnet ID 1.
Endpoint 1	0	0 or F	Rx Subnet = 0 forces communication through the Gateway.
Endpoint 2	1	0 or F	Rx Subnet = 1 forces communication through Repeater 1.
Endpoint 3	2	0 or F	Rx Subnet = 2 forces communication through Repeater 2.
Endpoint 4	0	0	The 0,0 setting allows the Endpoint to link with the first Gateway or Repeater it hears with the same Network ID.

10. Additional Radio Information

This chapter contains additional information about the radios described in this manual:

- Operational RS422 and RS485 information
- Connector pin assignments

10.1. Operational RS422 and RS485 Information

For RS422 and RS485, the FreeWave radio can drive 32 standard unit loads and loads the bus with only 1/8 unit load. A maximum of 256 devices can be tied on the bus if all of the line receivers have 1/8 unit load.

10.1.1. RS422

RS422 is used for 4-wire or full duplex communication with one Gateway and multiple Endpoint radios.

The Gateway radio keeps the line driver asserted at all times. The maximum line length is 4,000 feet using two, 120 ohm twisted pair cables with a fifth wire for data common.

10.1.2. RS485

RS485 full duplex using 4-wire plus common is the same as RS422, except the system can have multiple Masters on the bus.

The most common operation of RS485 is a two-wire comprised of a 120 ohm impedance single twisted pair.

- In this system, the loading of the FreeWave radio as described allows a maximum of 256 1/8 unit load units on the bus.
- Maximum line length is also 4,000 feet with a third wire required for data common.
- The FreeWave radio checks the line to be certain no other device is transmitting before enabling the line driver for data transmission.

Note: There is no provision for handshaking in any of the above modes of operation, so data rates of 57.6 KBaud and above are not recommended without a protocol that can handle error detection properly.

10.2. RS422 and RS485 Full Duplex Pinouts

RS422 and RS485 Full Duplex Pinouts	
Function	RJ-45 Pin Number
RX+	5
RX-	8
TX+	6
TX-	7
Signal Ground	4

10.3. RS485 Half Duplex Pinouts

RS485 Half Duplex Pinouts	
Function	RJ-45 Pin Number
Wire to both pins for Bus +	Short 5 and 6
Wire to both pins for Bus -	Short 7 and 8
Signal Ground	4

10.4. RJ45 to DB9 Cable

Use this cable to connect a COM port on the radio to a serial device.

Pin assignments are provided in:

- [RS232 - COM1 and COM2 RJ45 Pin Assignments \(on page 147\)](#).
- [RS232 - DB9 Connector Pin Assignments \(on page 148\)](#).

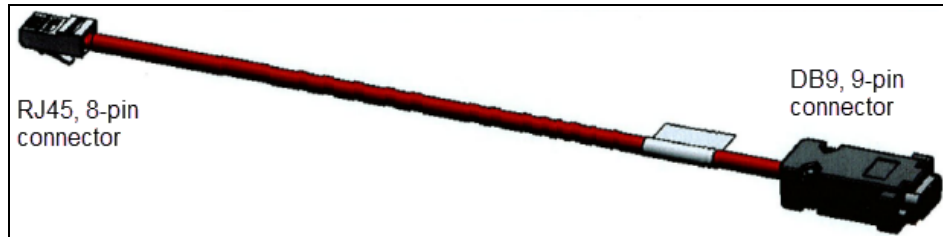
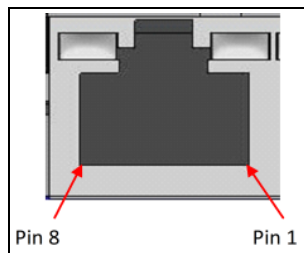


Figure 48: RJ45 to DB9 Cable

10.4.1. RS232 - COM1 and COM2 RJ45 Pin Assignments



RS232 - COM1 and COM2 RJ45 Pin Assignments			
Pin	Assignment	Signal	Definition
1	DSR - Data Set Ready	Output	Always high when the radio is powered from the Phoenix power connector. Indicates power is on to the radio.
2	CD - Carrier Detect	Output	Used to show an RF connection between radios.
3	DTR - Data Terminal Ready	Input	Not used.
4	GND - Ground		Signal return for all signal lines.
5	RX - Receive Data	Input	Used to receive data bits serially from the system device connected to the radio.
6	TX - Transmit Data	Output	Used to transmit data bits serially from the radio to the system device.

RS232 - COM1 and COM2 RJ45 Pin Assignments			
Pin	Assignment	Signal	Definition
7	CTS - Clear to Send	Output	This signal is used to tell the system device connected to the radio that the radio is ready to receive data. When asserted, the radio accepts data, when de-asserted the radio does not accept data. This should always be used for data rates above 38.4 KB or there is a risk of lost data if an RF link is not very robust.
8	RTS - Request to Send	Input	The radio does not recognize RTS for flow control.

10.4.2. RS232 - DB9 Connector Pin Assignments

RS232 - DB9 Connector Pin Assignments			
Pin	Assignment	Signal	Definition
1	CD - Carrier Detect	Output	Used to show an RF connection between radios.
2	TX - Transmit Data	Output	Used to transmit data bits serially from the radios to the system device.
3	RX - Receive Data	Input	Used to receive data bits serially from the system device connected to the radios.
4	DTR - Data Terminal Ready	Input	Used only in radios in Point-to-Point Slave/Master switchable mode or for DTR Connect.
5	GND - Ground		Signal return for all signal lines shared with Pin 9.
6	DSR - Data Set Ready	Output	Always high when the radio is powered from the 2-pin power connector. Indicates power is on to the radio.
7	RTS - Request to Send	Input	The radio does not recognize RTS for flow control. RTS is used as a control line in RTS/CTS mode.
8	CTS - Clear to Send	Output	This signal is used to tell the system device connected to the radio that the radio is ready to receive data. When asserted, the radio will accept data, when de-asserted the radio does not accept data. This should always be used for data rates above 38.4 KB or a risk of lost data may occur if an RF link is not very robust.
9	GND - Ground		Signal return for all signal lines shared with Pin 5

11. Approved Antennas

11.1. 900MHz Directional Antennas

Note: Per FCC approval, for FGR2-P, -PE, & -PE-U PLUS Radios, the maximum approved directional antenna gain is 10dBi.

900MHz Directional Antennas			
Gain (dBi)	Manufacturer	Manufacturer Model Number	FreeWave Model Number
6	Larsen	YA6-900	EAN0906YA
6	Bluewave	BMY890G5502N4	EAN0906YC
10	Bluewave	BMY890K5502N4	EAN0900YC

11.2. 900MHz Omni-directional Antennas

Note: Per FCC approval, for FGR2-P, -PE, & -PE-U PLUS Radios, the maximum approved directional antenna gain is 6dBi.

900MHz Omni-directional Antennas			
Gain (dBi)	Manufacturer	Manufacturer Model Number	FreeWave Model Number
0	Mobile Mark	PSTG0-915FW	EAN0900RQ
0	Mobile Mark	PSTN3-915N	EAN0900NH
0	Mobile Mark	PSTG0-915SE	EAN0900SQ
0	Mobile Mark	PSTN3-915S	EAN0900SH

900MHz Omni-directional Antennas			
Gain (dBi)	Manufacturer	Manufacturer Model Number	FreeWave Model Number
0	JEMA	JA900SS	EAN0900WR
3	Maxrad	MAX-9053	EAN0900WC
5	Antennex	EB8965C	EAN0905WC
5	Maxrad	BMEFC8985HD	EAN0905WC
6	Antennex	FG9026	EAN0906NF

12. Configuration Windows

This section provides a visual reference to each of the configuration windows.



Use these images as a reference to the windows when there currently is no access to the radio.

Note: For more information about using the configuration Web pages, see [Navigating the Configuration Windows \(on page 29\)](#).

- [Add User window \(on page 181\)](#).
- [Call Book window \(on page 158\)](#).
- [Diagnostics window \(on page 152\)](#).
- [IP Setup window \(on page 153\)](#).
- [Radio Setup window \(on page 156\)](#).
- [Security window \(on page 163\)](#).
- [Serial Port Status window \(on page 171\)](#).
- [Serial Setup window \(on page 168\)](#).
- [SNMP window \(on page 173\)](#).
- [Status window \(on page 175\)](#).
- [Tools window \(on page 178\)](#).
- [Users window \(on page 180\)](#).
- [View Log window \(on page 167\)](#).

12.1. Diagnostics window

The **Diagnostics** window is used to identify frequency regions that may be overlapping with other devices or be somehow impaired.

Access and Window Description

On the **Menu** bar, click **Diagnostics**.

Frequency Information By Channel				
Frequency (MHz)	Signal (dBm)	Noise (dBm)	Delta	%Rev Rate
902.2464	0	0	0	0.00%
902.4768	0	0	0	0.00%
902.7072	0	0	0	0.00%
902.9376	0	0	0	0.00%
903.1680	0	0	0	0.00%
903.3984	0	0	0	0.00%
903.6288	0	0	0	0.00%
903.8592	0	0	0	0.00%
904.0896	0	0	0	0.00%
904.3200	0	0	0	0.00%
904.5504	0	0	0	0.00%

©2006-2014 FreeWave Technologies, Inc.

Figure 49: FGR2-P, -PE, & -PE-U Diagnostics window

Note: This window is read-only and cannot be changed.

Diagnostics window	
Control Title	Control Description
Frequency (MHz) column	This is the frequency range that the signal strength and noise is being reported for.
Signal (dBm) column	This is the signal strength for the specific frequency region.
Noise (dBm) column	This is the noise for the specific frequency region.
Delta column	This is the difference between the information in the Signal and Noise columns.
% Rev Rate column	This is the number of successful packets as a percentage of the total of packets.

12.2. IP Setup window

In the **IP Setup** window, these are the available parameters:

- **LAN Network Interface Configuration (Management)** - The local area network (LAN) settings.
- **VLAN Configuration (Data)** - The virtual local area network (VLAN) settings.
 - A VLAN is a group of devices with a common set of requirements that communicate as if they were attached to the same domain, regardless of their network location.

Note: Not every network needs or uses VLAN IDs.
The **VLAN Mode** setting is typically set to **Disabled**.
Changes to VLAN settings should be approved by a network administrator.

- **NTP Client** - The Network Time Protocol (NTP) settings.
 - The device with the IP address entered here is the device that the radios in the network use to synchronize their internal clocks.
- **Syslog Server** - The system logging settings.
 - Enabling and setting IP addresses in the system server settings instructs the radio to send all its log entries to a system server.

Note: For more information, see [Viewing the System Log \(on page 103\)](#).

Access and Window Description

On the **Menu** bar, click **IP Setup**.

Figure 50: FGR2-P, -PE, & -PE-U IP Setup window

IP Setup window		
Control Area	Control Title	Control Description
LAN Network Interface Configuration (Management)	IP Address text box	IP Address (on page 53) .
LAN Network Interface Configuration (Management)	Subnet Mask text box	Subnet Mask (on page 57) .
LAN Network Interface Configuration (Management)	Default Gateway text box	Default Gateway (on page 52) .
LAN Network Interface Configuration (Management)	Web Page Port (http) text box	Web Page Port (http) (on page 62) .
LAN Network Interface Configuration (Management)	Spanning Tree check box	Spanning Tree (on page 56) .
LAN Network Interface Configuration (Management)	MTU (68-1500) text box	MTU (on page 54) .
VLAN Configuration (Data)	Mode list box	VLAN Mode (on page 61) .

IP Setup window		
Control Area	Control Title	Control Description
VLAN Configuration (Data)	IP Address text box	VLAN IP Address (on page 60).
VLAN Configuration (Data)	Subnet Mask text box	VLAN Subnet Mask (on page 61).
VLAN Configuration (Data)	Default Gateway text box	VLAN Default Gateway (on page 59).
VLAN Configuration (Data)	Management VLAN ID text box	Management VLAN ID (on page 60).
VLAN Configuration (Data)	Data VLAN ID text box	Data VLAN ID (on page 59).
VLAN Configuration (Data)	VLAN Trunk text box	VLAN Trunk ID 1 to VLAN Trunk ID 5 (on page 62).
NTP Client	Enable check box	NTP Client Enable (on page 55).
NTP Client	IP Address text box	NTP IP Address (on page 55).
Syslog Server	Push to Server check box	Push to (Syslog) Server (on page 56).
Syslog Server	Syslog Server 1 text box	Syslog Server 1 (on page 58).
Syslog Server	Syslog Server 2 text box	Syslog Server 2 (on page 58).
Syslog Server	Save / Apply button	Click to save the changes made in the window.

12.3. Radio Setup window

The **Radio Setup** window is used to set the general functioning of the radio.

Access and Window Description

On the **Menu bar**, click **Radio Setup**.

Figure 51: FGR2-P, -PE, & -PE-U Radio Setup window

Radio Setup window		
Control Area	Control Title	Control Description
Operation Mode	Network Type list box	Network Type on page 94.
Operation Mode	Modem Mode list box	Modem Mode on page 90.
Transmission Characteristics	Frequency Key list box	Frequency Key on page 85.

Radio Setup window		
Control Area	Control Title	Control Description
Transmission Characteristics	Zones check boxes	Frequency Zones on page 86.
Transmission Characteristics	Max Packet Size list box	Max Packet Size and Min Packet Size on page 88.
Transmission Characteristics	Min Packet Size list box	Max Packet Size and Min Packet Size on page 88.
Transmission Characteristics	Transmit Power list box	Transmit Power on page 100.
Transmission Characteristics	Retry Timeout list box	Retry Timeout on page 95.
Transmission Characteristics	RF Data Rate list box	RF Data Rate on page 96.
Point-to-Point Parameters	Transmit Rate list box	Transmit Rate on page 101.
Point-to-Point Parameters	Call Book link	Click to open the Call Book window (on page 158).
MultiPoint Parameters	Addressed Repeat list box	Addressed Repeat on page 83.
MultiPoint Parameters	Broadcast Repeat list box	Broadcast Repeat on page 84.
MultiPoint Parameters	Slave Connect Odds list box	Slave Attempts on page 97.
MultiPoint Parameters	AND THEN list box	Slave Connect Odds on page 98.
MultiPoint Parameters	Master Tx Beacon list box	Master Tx Beacon on page 87.
MultiPoint Parameters	Network ID text box	Network ID on page 93.
MultiPoint Parameters	Repeaters list box	Repeaters on page 94.
MultiPoint Parameters	Subnet ID (RX) list box	Subnet ID on page 99.
MultiPoint Parameters	Subnet ID (TX) list box	Subnet ID on page 99.
MultiPoint Parameters	Save / Apply button	Click to save the changes made in the window.

12.4. Call Book window

Using the Call Book offers both security and flexibility in determining how FreeWave radios communicate with each other.

The Call Book window is used to designate this communication between the radios.

Important! The Call Book is **required** in Point-to-Point networks.
The instructions in this section are for Point-to-Point mode only.

Note: When functioning as an Endpoint, the **Entry to Call** feature in the radio's Call Book is not operational.

FREEWAVE Recommends: While the Call Book is an option in Point-to-MultiPoint networks, FreeWave strongly recommends using the **Network ID** feature in most applications.
If a large MultiPoint network is implemented using the Call Book and a radio needs to be added or replaced in the network, each radio **MUST** be physically reprogrammed in the network and the new serial number entered in the radio's Call Book.
This can be a time consuming process and can cause a delay in getting the network back up and running.

Required: Set these options for two FreeWave radios to communicate in Point-to-Point mode:

1. The Gateway serial number must be listed in the Endpoint Call Book (**Endpoint** column).
2. The Endpoint serial number must be listed in the Call Book on the Gateway Call Book (**Endpoint** column).
3. The Gateway must be programmed to call the Endpoint (**Entry to Call** option).

The Call Book allows a maximum of 10 FreeWave radios.

- Designate:
 - 1 to 4 Repeaters to use with each radio.
 - which Endpoint the Gateway calls.
- To set the **Entry to Call** option:
 - a. Click the list box arrow and select the number in the **Entry to Call** list.
 - b. Select **All** to direct the Gateway to call all Endpoints.

If a Call Book entry uses 3 or 4 Repeaters:

- The total number of available Endpoint entries is reduced.
- An extra Call Book line is in use for Repeaters #3 and #4.
- To set the **Entry to Call** option, click the list box arrow and select the appropriate Entry number in the **Entry to Call**.

Important! The Call Book slots (0-9) **MUST** be filled sequentially starting with slot **0 (zero)**.

- When a Gateway is instructed to **Call All**, it calls all Endpoints listed until it reaches the first serial number of 000-0000 (or a blank slot).

- If a serial number is entered after the all zero number or as a Repeater, the Gateway does not recognize it as a valid number.
- To call an Endpoint through one or more Repeaters, that Endpoint must be called individually.
 - The line containing the Endpoint and Repeaters must be specifically selected in **Entry to Call**.
 - With **Call All** selected, the Gateway will not connect with any Endpoints through Repeaters.
 - This is because, when **Call All** is selected, the Gateway calls every Endpoint in the list and will connect with the first Endpoint that responds.
- When calling through a Repeater, the Gateway must first call that Repeater and establish a communication link with it prior to making contact with the Endpoint.

Access and Window Description

On the [Radio Setup window \(on page 156\)](#), click the **Call Book** link.

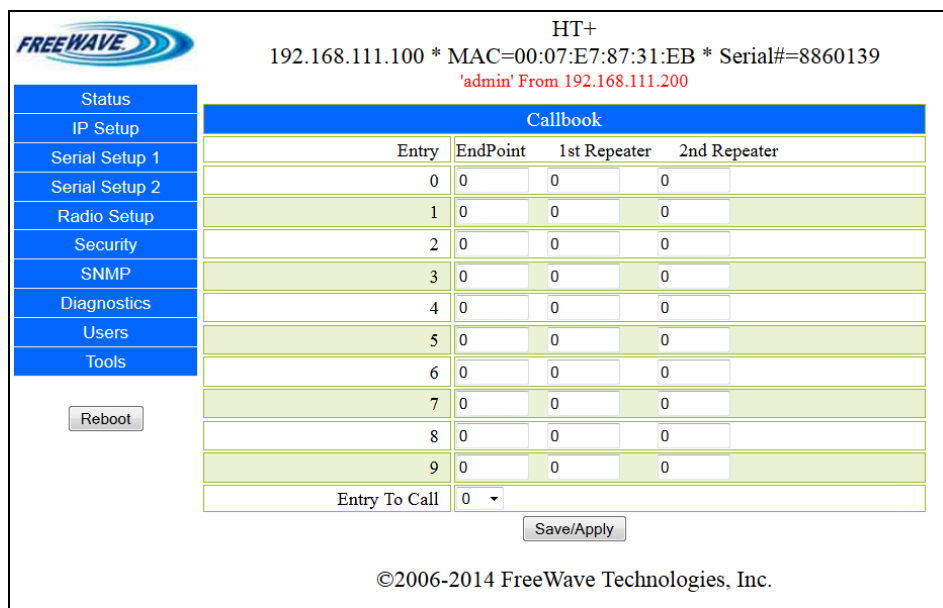


Figure 52: FGR2-P, -PE, & -PE-U Call Book window

Call Book window		
Control Area	Control Title	Control Description
Entry 0 to 9	EndPoint text box	This is the serial number of the devices registered in the Call Book as Endpoints.
Entry 0 to 9	1st Repeater text box	This is the serial number of the first repeater.
Entry 0 to 9	2nd Repeater text box	This is the serial number of the second repeater.

Call Book window		
Control Area	Control Title	Control Description
Entry to Call	Entry to Call list box	Click the list box arrow and select a single Entry to cycle through.
	Save / Apply button	Click to save the changes made in the window.

12.4.1. Programming Point-To-Point Extended Call Book to Use Three or Four Repeaters

In a Point-to-Point configuration, FreeWave radios can use a maximum of four Repeaters.

Procedure

1. Program the Call Book with the Endpoint serial number, followed by the first two Repeaters.
2. On the next line enter **999-9999** as the radio to call.
3. When prompted for the Repeaters enter the third and fourth Repeaters in the link.

Example

This Tool Suite example table shows a Point-to-Point link where an Endpoint is called through four Repeaters.

The Gateway is calling:

- a. the Endpoint, 884-3872.
- b. through Repeater 1, 884-1234.
- c. then Repeater 2, 884-0234.
- d. then Repeater 3, 884-9456.
- e. lastly Repeater 4, 884-4567.

Entering the serial number **999-9999** in line 1 instructs the Gateway to continue calling through the Repeaters programmed on that line.

Entry	Number	Repeater 1	Repeater 2
0	a 884-3872	b 884-1234	c 884-0234
1	999-9999	d 884-9456	e 884-4567
2			
3			
4			
5			

Figure 53: Example: Tool Suite Call Book table

To call an Endpoint radio through one or more Repeaters, that Endpoint must be called individually.

- With **Call All** selected, the Gateway will not connect with any Endpoint radios through Repeaters.
- The Gateway calls every Endpoint in the list and connects with the first Endpoint that responds.
- When calling through a Repeater, the Gateway must first call that Repeater and establish a communication link with it prior to making contact with the Endpoint.

12.4.2. Programming Point-to-MultiPoint Call Book

FREEWAVE Recommends: While the Call Book is an option in Point-to-MultiPoint networks, FreeWave strongly recommends using the **Network ID** feature in most applications. If a large MultiPoint network is implemented using the Call Book and a radio needs to be added or replaced in the network, each radio **MUST** be physically reprogrammed in the network and the new serial number entered in the radio's Call Book. This can be a time consuming process and can cause a delay in getting the network back up and running.

In a MultiPoint network, the Endpoints and Repeaters are not listed in the Gateway's Call Book. An Endpoint **MUST** have the Gateway and any Repeater it is going to use in **its** Call Book.

These examples show the Call Book of a MultiPoint network comprised of a Gateway, Repeater, and Endpoint where the Endpoint can communicate either through the Repeater or directly to the Gateway:

12.4.3. MultiPoint Master Call Book (Unit Serial Number 884-1111)

Entry	Endpoint Serial Number	Repeater 1	Repeater 2
(0)	000-0000		
(1)	000-0000		

Note: No serial number entries are necessary in the Gateway's Call Book.

12.4.4. MultiPoint Repeater Call Book (Unit Serial Number 884-2222)

Entry	Endpoint Serial Number	Repeater 1	Repeater 2
(0)	884-1111		
(1)	000-0000		

12.4.5. MultiPoint Slave Call Book (Unit Serial Number 884-3333)

Entry	Endpoint Serial Number	Repeater 1	Repeater 2
(0)	884-1111		
(1)	884-2222		
(2)	000-0000		



Sometimes there is a need to force an Endpoint to go through a specific MultiPoint Repeater. In this scenario, the Endpoint's Call Book should contain only the serial number for that Repeater as the entry on line 0.

12.4.6. Programming Point-to-MultiPoint Extended Call Book

In a MultiPoint network, Endpoint radios can be programmed to roam between Gateway radios and Repeaters using the **MultiPoint Extended Call Book** function.

Endpoint radios with Call Book configured similar to this example, communicates with any radio whose serial number appears in any of the three columns.

Procedure

1. Set the **Network ID** to **255**.
2. In the Call Book, enter **999-9999** as the last entry in the first and second columns.
3. In the Call Book, set **Entry to Call** to **All**.

Callbook			
Entry	EndPoint	1st Repeater	2nd Repeater
0	8401111	8402222	8403333
1	8404444	8405555	8406666
2	8407777	8408888	8409999
3	8401010	8401212	8401313
4	8401414	8401515	8401616
5	8401717	8401818	8401919
6	8402020	8402121	8402323
7	8402424	8402525	8402626
8	8402727	8402828	8402929
9	9999999	9999999	8403030
Entry To Call	0		

Save/Apply

Figure 54: Call Book

12.5. Security window

The **Security** window is used to define elements that enhance the security of the network and the data it passes. Typically, a Network Administrator addresses security parameters.

Access and Window Description

On the **Menu** bar, click **Security**.

The screenshot shows the 'Security' configuration window for a device labeled 'D2+'. The interface includes a sidebar with navigation options like 'Status', 'IP Setup', 'Serial Setup 1', 'Serial Setup 2', 'Radio Setup', 'Security', 'SNMP', 'Diagnostics', 'Users', and 'Tools'. The main content area is divided into several sections: 'RADIUS Authentication Configuration' with fields for 'Enable RADIUS' (checkbox), 'RADIUS IP Address' (text box), and 'RADIUS Port Number' (1812); 'AES Encryption' with 'Version' (128) and 'Key' (text box); 'MAC Filter' with an 'Add' button and 'Delete'/'Clear' buttons; and 'Misc' with 'Detach Local Eth' (checkbox), 'Force SSL (https)' (checkbox), 'Peer To Peer' (checked), and 'Reboot interval' (Disabled). At the bottom, there are links for 'Syslog Dump' and 'System Memory Information', and a 'Save/Apply' button. The copyright notice at the bottom reads '©2006-2016 FreeWave Technologies, Inc.'.

Figure 55: FGR2-P, -PE, & -PE-U Security window

Security window		
Control Area	Control Title	Control Description
RADIUS Authentication Configuration	Enable RADIUS check box	RADIUS Enable (on page 113).
RADIUS Authentication Configuration	RADIUS IP Address text box	RADIUS IP Address (on page 114).

Security window		
Control Area	Control Title	Control Description
RADIUS Authentication Configuration	RADIUS Port Number text box	RADIUS Port (on page 115) .
RADIUS Authentication Configuration	Shared Secret text box	Shared Secret (on page 115) .
RADIUS Authentication Configuration	User Password text box	User Password (on page 116) .
AES Encryption	Version list box	AES Version (on page 110) .
AES Encryption	Key text box	AES Encryption Key (on page 109) .
MAC Filter	MAC Filter scroll box	MAC Filter (on page 111) .
MAC Filter	MAC Filter text box	In the MAC Filter text box, enter the MAC address to add to the MAC Filter scroll box.
MAC Filter	Add button	Click the Add button to add the MAC address entered in the MAC Filter text box.
MAC Filter	Delete button	Click the Delete button to delete the selected MAC address from the MAC Filter scroll box.
MAC Filter	Clear button	Click the Clear button to delete all MAC address from the MAC Filter scroll box.
Misc	Detach Local Eth check box	Detach Local Ethernet (on page 110) .
Misc	Force SSL (https) check box	Force SSL (https) (on page 111) .
Misc	Peer to Peer check box	Peer To Peer (on page 112)
Misc	Reboot Interval list box	Reboot Interval (on page 115) Note: See Specify a Reboot Interval Schedule (on page 105) .
Customer Support Information	Syslog Dump - View Log link	Click to open the View Log window (on page 167) . Note: See Viewing the System Log (on page 103) .

Security window		
Control Area	Control Title	Control Description
Customer Support Information	System - Memory Information link	Click to open the Memory Information window (on page 166) .
Customer Support Information	Save / Apply button	Click to save the changes made in the window.

12.5.1. Memory Information window

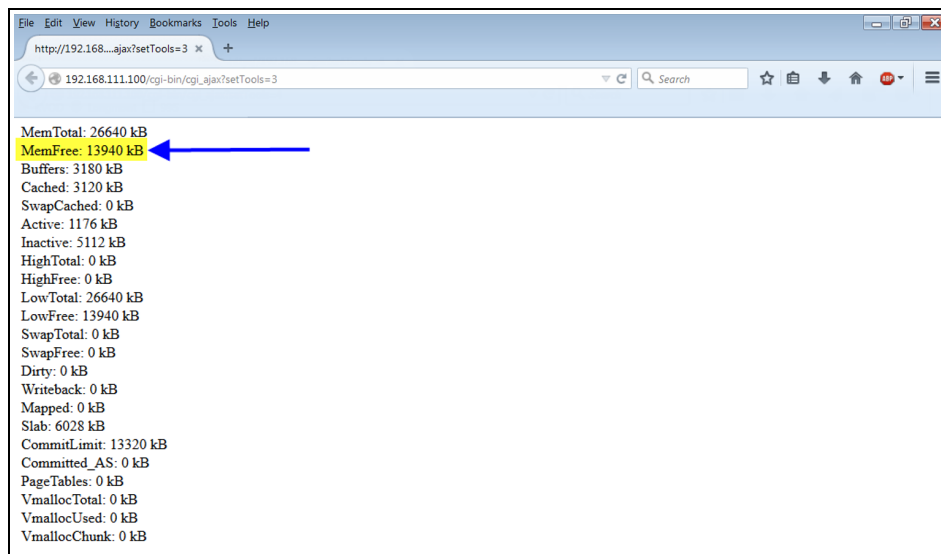
The **System Memory Information** window is used to provide the internal memory characteristics of the device reporting.

Important! If the **MemFree** line is less than 8000, schedule a time over the next two weeks to reboot the device to maintain both good device throughput and potential issues related to memory starvation.

Access and Window Description

On the [Security window](#), click the **Memory Information** link.

Note: This window is read-only and cannot be changed.



```
MemTotal: 26640 kB
MemFree: 13940 kB
Buffers: 3180 kB
Cached: 3120 kB
SwapCached: 0 kB
Active: 1176 kB
Inactive: 5112 kB
HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 26640 kB
LowFree: 13940 kB
SwapTotal: 0 kB
SwapFree: 0 kB
Dirty: 0 kB
Writeback: 0 kB
Mapped: 0 kB
Slab: 6028 kB
CommitLimit: 13320 kB
Committed_AS: 0 kB
PageTables: 0 kB
VmallocTotal: 0 kB
VmallocUsed: 0 kB
VmallocChunk: 0 kB
```

Figure 56: System Memory Information window

12.5.2. View Log window

The **View Log** window is used to show the system events of the FGR2-P, -PE, & -PE-U.

Access and Window Description

On the [Security window](#), click the **View Log** link.

Note: This window is read-only and cannot be changed.

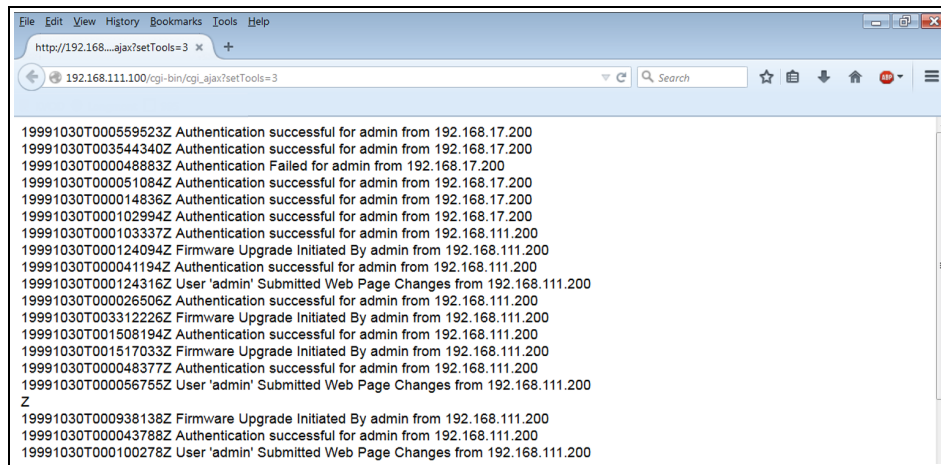


Figure 57: View Log window

12.6. Serial Setup window

Each serial port is setup independently and configured on its own tab or [Configuration Windows \(on page 151\)](#). The ports can have different baud rates, parity, protocol, etc., but must match the device it is connected to. To access either port, a client needs to call the IP address of the radio plus its assigned port number.

The **Serial Setup** window is where the port numbers and data settings for each serial port are assigned using these parameters:

- **Serial Port Mode** - This setting defines whether the port acts as a TCP terminal server, TCP client, UDP client, or Multicast.
- **Serial Settings** - This setting defines data transmission settings (e.g., **Baud Rate** and **Flow Control**).
 - Set these parameters to match the device the port is connected to.

Note: See [Viewing the Serial Port Status \(on page 67\)](#) to view the status of each serial port.

Access and Window Description

On the **Menu** bar, click either **Serial Setup 1** or **Serial Setup 2**.

Note: **Serial Setup 1** MUST be configured before a **Serial Setup 2**.

Figure 58: FGR2-P, -PE, & -PE-U Serial Setup window

Serial Setup window		
Control Area	Control Title	Control Description
TCP Server Settings	Enable check box	TCP Server Enable (on page 78).
TCP Server Settings	Port text box	TCP Server Port (on page 80).
TCP Server Settings	Enable Keepalive check box	TCP Server Keep Alive (on page 79).
TCP Server Settings	Inactivity Timeout (Seconds) check box	TCP Server Inactivity Timeout (on page 79).
TCP Client Settings	Enable check box	TCP Client Enable (on page 76).
TCP Client Settings	IP Address text box	TCP Client IP Address (on page 77).
TCP Client Settings	Port text box	TCP Client Port (on page 77).
UDP Settings	Enable check box	UDP Enable (on page 80).

Serial Setup window		
Control Area	Control Title	Control Description
UDP Settings	UDP IP text box	UDP IP Address (on page 80).
UDP Settings	Port text box	UDP IP Port (on page 81).
MULTICAST Settings	Enable check box	Multicast Enable (on page 69).
MULTICAST Settings	Multicast IP text box	Multicast IP Address (on page 69).
MULTICAST Settings	Port text box	Multicast Port (on page 70).
Serial Settings	Baud Rate list box	Baud Rate (on page 72).
Serial Settings	Data Bits list box	Data Bits (on page 74).
Serial Settings	Parity list box	Parity (on page 76).
Serial Settings	Stop Bits list box	Stop Bits (on page 76).
Serial Settings	Flow Control list box	Flow Control (on page 74).
Serial Settings	CD Mode list box	CD Mode (on page 73).
Serial Settings	Interface list box	Interface (on page 74).
Serial Settings	Runtime Serial Setup 'U' check box	Runtime Serial Setup "U" (on page 72).
RTU Mode Timing Settings	Modbus RTU check box	Modbus RTU (on page 75).
RTU Mode Timing Settings	Pre-Packet Timeout (ms) text box	Pre-Packet and Post-Packet Timeouts (on page 70).
RTU Mode Timing Settings	Post-Packet Timeout (ms) text box	Pre-Packet and Post-Packet Timeouts (on page 70).
RTU Mode Timing Settings	Save / Apply button	Click to save the changes made in the window.

12.6.1. Serial Port Status window

The **Serial Port Status** window is used to provide the number of used sockets for each serial port.

Access and Window Description

On the [Serial Setup window \(on page 168\)](#), click the **Serial Port Status** link.

Note: This window is read-only and cannot be changed.

D2+
 192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
 'admin' From 192.168.111.1

Serial Port 1	
Socket 1 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 2 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 3 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 4 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Socket 5 Status	Waiting For Client To Connect On Port 7000
	Rx=0, Tx=0
Serial Port 2	
Socket 1 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 2 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 3 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 4 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0
Socket 5 Status	Waiting For Client To Connect On Port 7001
	Rx=0, Tx=0

[Refresh](#)

©2006-2014 FreeWave Technologies, Inc.

Figure 59: FGR2-P, -PE, & -PE-U Serial Port Status window

Important! This example image shows both a TCP Server (**Serial Port 1**) and a UDP Multicast Server (**Serial Port 2**).

The information in this window will change depending on the connected radio and the selection made in [Serial Setup window on page 168](#).

Serial Port Status window		
Control Area	Control Title	Control Description
Serial Port 1	Socket 1 to 5 Status rows	These rows show the IP address and TCP connection number of the remote device bound to the socket.
Serial Port 1	Socket 1 Status - Rx=0, Tx=0 row	<ul style="list-style-type: none"> Rx shows how many packets were received on the specific socket. Tx shows how many packets were transmitted on the specific socket.
Serial Port 2	Socket 1 to 5 Status rows	These rows show the UDP and Multicast modes. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: This example image does not have a UDP Client connected. If a UDP Client were connected, the row would show the IP address and UDP connection number of the remote device bound to the socket.</p> </div>
Serial Port 2	Socket 1 Status - Rx=0, Tx=0 row	<ul style="list-style-type: none"> Rx shows how many packets were received on the specific socket. Tx shows how many packets were transmitted on the specific socket.
	Refresh link	Click to refresh the information in the Serial Port Status window.

12.7. SNMP window

The **SNMP** window is used to monitor the state of the radio for conditions that may require special attention.

Access and Window Description

On the **Menu** bar, click **SNMP**.

Figure 60: FGR2-P, -PE, & -PE-U SNMP window

SNMP window		
Control Area	Control Title	Control Description
SNMP Agent Configuration	SNMP Version list box	SNMP Version (on page 120).
SNMP Agent Configuration	Read Community text box	Read Community (on page 120).
SNMP Agent Configuration	Write Community text box	Write Community (on page 122).
SNMP Agent Configuration	Authentication Password (v3) text box	Authentication Password (v3) (on page 118).
SNMP Agent Configuration	Authentication Password (v3) list box	Authentication Method (on page 118).
SNMP Agent Configuration	Privacy Password (v3) text box	Privacy Password (v3) (on page 119).

SNMP window		
Control Area	Control Title	Control Description
SNMP Agent Configuration	Privacy Password (v3) list box	Privacy Method (on page 119).
SNMP Trap Configuration	Trap Version list box	Trap Version (on page 122).
SNMP Trap Configuration	Trap Community text box	Trap Community (on page 121).
SNMP Trap Configuration	Min Fault Time (Seconds) list box	Min Fault Time (on page 119).
SNMP Trap Configuration	Trap Manager 1 IP text box	Trap Manager IP (on page 121).
SNMP Trap Configuration	Trap Manager 2 IP text box	Trap Manager IP (on page 121).
SNMP Trap Limits	Voltage Enable check box	Voltage Alarm Enable (on page 128).
SNMP Trap Limits	Voltage Alarm Above list box	Voltage Alarm Above (on page 128).
SNMP Trap Limits	Voltage Alarm Below list box	Voltage Alarm Below (on page 128).
SNMP Trap Limits	Rx% Rate Enable check box	Rx Rate Alarm Enable (on page 126).
SNMP Trap Limits	Rx% Rate Alarm Below list box	Rx Rate Alarm Below (on page 125).
SNMP Trap Limits	Tx% Rate Enable check box	Tx Rate Alarm Enable (on page 127).
SNMP Trap Limits	Tx% Rate Alarm Below list box	Tx Rate Alarm Below (on page 127).
SNMP Trap Limits	Reflected Power Enable check box	Reflected Alarm Enable (on page 125).
SNMP Trap Limits	Reflected Power Alarm Above list box	Reflected Alarm Above (on page 124).
SNMP Trap Limits	S-N Delta Enable check box	Delta Alarm Enable (on page 123).
SNMP Trap Limits	S-N Delta Alarm Below list box	Delta Alarm Below (on page 123).
SNMP Trap Limits	Signal Enable check box	Signal Alarm Enable (on page 126).
SNMP Trap Limits	Signal Alarm Below list box	Signal Alarm Below (on page 126).
SNMP Trap Limits	Noise Enable check box	Noise Alarm Enable (on page 124).
SNMP Trap Limits	Noise Alarm Above list box	Noise Alarm Above (on page 124).
SNMP Trap Limits	Save / Apply button	Click to save the changes made in the window.

12.8. Status window

The **Status** window is used to view the FGR2-P, -PE, & -PE-U PLUS Radio's status and statistics.

Access and Window Description

On the **Menu** bar, click **Status**.

Note: This is the default window when the [Configuration Windows \(on page 151\)](#) are opened.

192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
'admin' From 192.168.111.1

Hardware Information	
Firmware Version	
Wireless Version	+8.80a
Software Boot Version	3
Hardware Version	1
Country Code	
Uptime	0 days 0 hours 13 minutes 41 seconds

RF Stats	
Connected To	0
Signal	0
Noise	0
Upstream signal	0
Upstream Noise	0
Voltage	10.92v
RX Success Rate	0.00%
TX Success Rate	0.00%
Reflected Power	0
Disconnect Count	0
Temperature	-31°C ~ 88°F
Distance	~0 meters or 0.0 miles

Packet Stats	
Received	0 packets - 0 Bytes
Packets Sent	45 packets - 8140 Bytes
Packets Dropped	353
RF Packets Skipped	0
RF Buffer Overflow Skip	0
Bad Packets	0
Un-Ackd Packets	0 (0.00%)
Broadcast Packets	0 (0.00%)
Radio Addressed Packets	3 (6.67%)
Radio Parse Error	0
RX Throughput	0.00 kbps - 0.00 avg/min
TX Throughput	0.00 kbps - 0.00 avg/min

Site Information	
Site Name	
Site Contact	
System Name	
Notes	

Auto Refresh Page

Figure 61: FGR2-P, -PE, & -PE-U Status window

Status window		
Control Area	Control Title	Control Description
Hardware Information	Firmware Version text box	Firmware Version (on page 131).
Hardware Information	Wireless Version text box	Wireless Version (on page 135).
Hardware Information	Software Boot Version text box	Software Boot Version (on page 133).
Hardware Information	Hardware Version text box	Hardware Version (on page 131).
Hardware Information	Country Code text box	Note: This is a read-only field used by FreeWave Customer Support.
Hardware Information	Uptime text box	Uptime (on page 135).
RF Stats	Last Connected To text box	Identifies the last upstream the FGR2-P, -PE, & -PE-U device was connected to.
RF Stats	Connected To text box	Connected To (on page 130).
RF Stats	Signal text box	Signal (on page 133).
RF Stats	Noise text box	Noise (on page 131).
RF Stats	Upstream Signal text box	Upstream Signal (on page 135).
RF Stats	Upstream Noise text box	Upstream Noise (on page 134).
RF Stats	Voltage text box	Voltage (on page 135).
RF Stats	RX Success Rate text box	RX Success Rate (on page 133).
RF Stats	TX Success Rate text box	TX Success Rate (on page 134).
RF Stats	Reflected Power text box	Reflected Power (on page 132).
RF Stats	Disconnect Count text box	Disconnect Count (on page 131).
RF Stats	Temperature text box	Temperature (on page 134).
RF Stats	Distance text boxes	Distance (on page 131).
Packet Stats	Received text box	Received (on page 132).
Packet Stats	Packets Sent text box	Packets Sent (on page 132).

Status window		
Control Area	Control Title	Control Description
Packet Stats	Packets Dropped text box	Packets Dropped (on page 132) .
Packet Stats	RF Packets Skipped text box	This shows the duplicate packets received.
Packet Stats	RF Buffer Overflow Skip text box	This shows the packets dropped due to the RX buffer overflow.
Packet Stats	Bad Packet text box	Bad Packets (on page 130) .
Packet Stats	Un-Ackd Packets text box	Un-Acked Packets (on page 134) .
Packet Stats	Broadcast Packets text box	Broadcast Packets (on page 130) .
Packet Stats	Radio Addressed Packets text box	Radio Addressed Packets (on page 132) .
Packet Stats	Peer to Peer Packets text box	Peer to Peer Packets (on page 132) .
Packet Stats	Radio Parse Error text box	Radio Parse Error (on page 132) .
Packet Stats	RX Throughput text box	RX Throughput (on page 133) .
Packet Stats	TX Throughput text box	TX Throughput (on page 134) .
Packet Stats	RX RF Usage text box	RX Success Rate (on page 133) .
Packet Stats	TX RF Usage text box	TX Success Rate (on page 134) .
Packet Stats	Reset button	Click to manually refresh the information in the Status window.
Site Information	Site Name text box	Site Name (on page 133) .
Site Information	Site Contact text box	Site Contact (on page 133) .
Site Information	System Name text box	System Name (on page 133) .
Site Information	Notes text box	Notes (on page 131) .
Site Information	Auto Refresh Page check box	Select to automatically refresh the information in the Status window.

12.9. Tools window

The **Tools** window is used to edit of the Site Information and for software upgrades.

Note: The **Change Site Information** area is used for user-identified information only and does NOT have any impact on the FGR2-P, -PE, & -PE-U usage.

Access and Window Description

On the **Menu** bar, click **Tools**.

Figure 62: FGR2-P, -PE, & -PE-U Tools window

Tools window		
Control Area	Control Title	Control Description
Change Site Information	Site Name text box	Site Name (on page 133) .
Change Site Information	Site Contact text box	Site Contact (on page 133) .
Change Site Information	System Name text box	System Name (on page 133) .
Change Site Information	Notes text box	Notes (on page 131) .
Change Site Information	Change Site Information button	Click the Change Site Information button to save the information in the Change Site Information area.

Tools window		
Control Area	Control Title	Control Description
Global Change Capability	ENABLE Global Change Functionality button	Click the ENABLE Global Change Functionality button to push configuration changes throughout the network. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> Note: Contact FreeWave Technical Support about using this feature. </div>
TFTP Firmware Upgrade	Address of TFTP Server text box	Enter the IP address of the computer the TFTP Server is installed on.
TFTP Firmware Upgrade	File Name text box	Enter the exact name of the software upgrade file saved in the Root directory on the computer in Configuring the TFTP Server (on page 42) .
TFTP Firmware Upgrade	Upgrade Firmware button	Click to retrieves the software file from the TFTP Server.
TFTP Firmware Upgrade	Global Firmware Upgrade button	Click to upgrade the software to all connected FGR2-P, -PE, & -PE-U PLUS Radios of the same type.

12.10. Users window

The **Users** window is used to control access and privileges to the FGR2-P, -PE, & -PE-U device.

Access and Window Description

On the **Menu** bar, click **Users**.

D2+
192.168.111.100 * MAC=00:07:E7:82:B6:FD * Serial#=8566525
'admin' From 192.168.111.1

User Accounts	
Level	
admin	0
guest	3
Add User	

Edit Group Level Rights			
Level	1	2	3
IP Setup	Read Only	Read Only	Read Only
Serial Setup	Read Only	Read Only	Read Only
Radio Setup	Read Only	Read Only	Read Only
Security	No Access	No Access	No Access
SNMP	Read Only	Read Only	Read Only
RMS	Read Only	Read Only	Read Only
Tools	No Access	No Access	No Access

©2006-2014 FreeWave Technologies, Inc.

Figure 63: FGR2-P, -PE, & -PE-U Users window

Users window		
Control Area	Control Title	Control Description
User Accounts	Level - admin text box	The default setting is always 0 (zero). Note: This control is read-only and cannot be changed.
User Accounts	Level - guest list box	Click the list box arrow and select the Group Level Rights this user is assigned to.
User Accounts	Add User link	Click to open the Add User window (on page 181) .
Edit Group Level Rights	Level 1 2 3	These levels define the authorization and privileges the user is assigned and allowed.

Users window		
Control Area	Control Title	Control Description
Edit Group Level Rights	IP Setup list boxes Serial Setup list boxes Radio Setup list boxes Security list boxes SNMP list boxes Tools list boxes	Click the list box arrow and select one of these options to define the authorization and privileges the user has to view the Configuration Windows : <ul style="list-style-type: none"> • No Access - This assignment blocks the user from viewing the designated Configuration Windows. • Read Only - This assignment allows the user to read only from the designated Configuration Windows. <ul style="list-style-type: none"> • No changes are allowed with this assignment. • Read / Write - This assignment allows the user to read and write the information on the designated Configuration Windows.
Edit Group Level Rights	RMS list box	Note: As of v3.01, this setting is not used.
Edit Group Level Rights	Save / Apply button	Click to save the changes made in the window.

12.10.1. Add User window

The **Add User** window is used to add a new user to the FGR2-P, -PE, & -PE-U.

Access and Window Description

On the [Users window](#), click the **Add User** link.

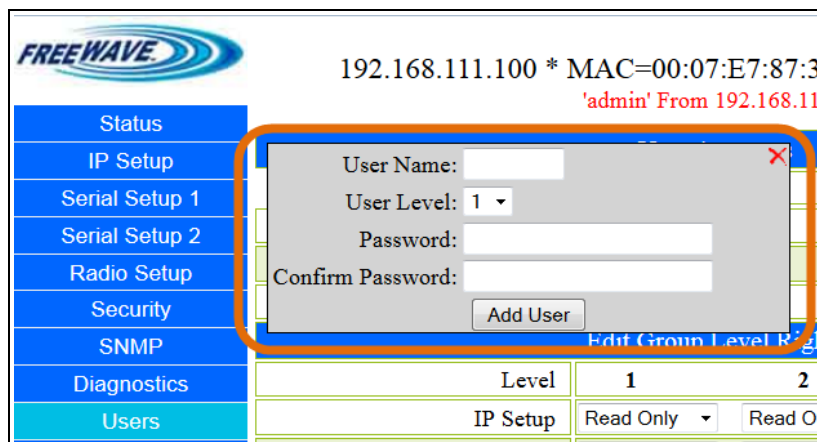


Figure 64: FGR2-P, -PE, & -PE-U Add User window

Add User window	
Control Title	Control Description
User Name text box	Enter the new user's name. This text box has these restrictions: <ul style="list-style-type: none"> • Lower case characters. • No numbers. • Maximum of 10 characters.
User Level list box	Click the list box arrow and select either 1, 2, or 3 as defined in the Users window (on page 180) .
Password text box	Enter the new user's password.
Confirm New Password text box	Re-enter the new user's password.
Add User button	Click to add the new user to the radio.

12.10.2. Change Password window

The **Change Password** window is used to change the password of a user.

Access and Window Description

On the [Users window](#), click the  next to the user to change the password for.

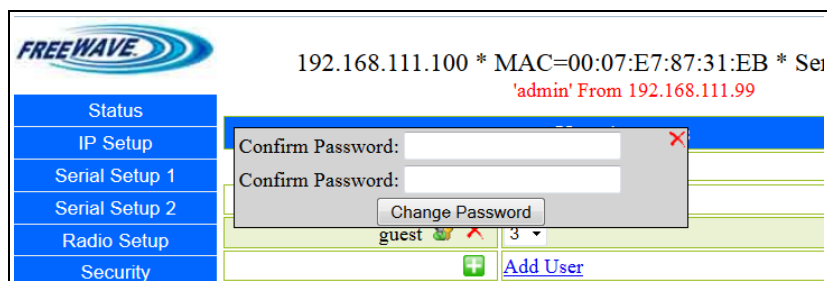


Figure 65: FGR2-P, -PE, & -PE-U Change Password window

Change Password window	
Control Title	Control Description
Confirm Password text boxes	<ol style="list-style-type: none"> 1. In the first Confirm Password text box, enter the user's new password. 2. In the second Confirm Password text box, re-enter the user's new password.

13. Release Notes: FGR2-P, -PE, & -PE-U PLUS Radios

These sections describe the updates and known limitations in each software version. The most recent version is listed first.

Important! Radios running versions 2.26 through 2.29 MUST upgrade to version 2.34.



The latest software versions and the most recent list of known limitations and workarounds are available at <http://support.freewave.com/>.

13.1. Version 3.14

Release Date: March 2017

PLUS Software 3.14 is released for FGR2-P and FGR2-PE PLUS Radios to correct a range decrease of 25-50% below the product specifications that was observed.

13.2. Version 3.13

Release Date: August 2016

Software 3.13 is released for FGR2-P, -PE, & -PE-U PLUS Radios.

Additions and Changes

In the [Security window \(on page 163\)](#), in the **Miscellaneous** area, a new **Reboot Interval** list box option has been added.

- By default, the **Reboot Interval** is **Disabled**.
- If **Disabled** is selected, the PLUS Radio will operate without automatically rebooting.

- When an interval (e.g., **1 Hour**, **1 Day**, **30 Days**) is selected, the scheduler automatically reboots the PLUS Radio when the reboot interval expires.

Note: See [Specify a Reboot Interval Schedule \(on page 105\)](#) to use this feature.

The screenshot shows the FreeWave web interface for a D2+ radio. The top header displays the IP address (192.168.111.100), MAC address (00:07:E7:82:B2:EF), and serial number (8565487). A navigation menu on the left includes Status, IP Setup, Serial Setup 1, Serial Setup 2, Radio Setup, Security, SNMP, Diagnostics, Users, and Tools. The main content area is titled 'RADIUS Authentication Configuration' and includes fields for 'Enable RADIUS' (checkbox), 'RADIUS IP Address', 'RADIUS Port Number' (1812), 'Shared Secret', and 'User-Password'. Below this is the 'AES Encryption' section with 'Version' (128) and 'Key' fields. The 'MAC Filter' section has a 'Force SSL' checkbox. The 'Peer To Peer' section has an 'Enable' checkbox. The 'Reboot interval' dropdown menu is highlighted with a red circle and shows 'Disabled'. The 'Customer Support Information' section includes links for 'Syslog Dump' (View Log) and 'System Memory Information' (Memory Information). A 'Reboot' button is visible on the left side of the interface. The footer contains the copyright notice: ©2006-2016 FreeWave Technologies, Inc.

Figure 66: Security window - Reboot Interval list box

13.3. Version 3.11

Release Date: June 2016

Additions and Changes

Software 3.11 is released for FGR2-P, -PE, & -PE-U PLUS Radios to correct the non-locked Frequency Zones.

- If any Frequency Zones are locked or restricted based on Model Number, v3.11 correctly displays the Frequency Zones that are locked and not available for setting or clearing.

13.4. Version 3.06

Release Date: May 2015

Additions and Changes

Software 3.06 is released for FGR2-P, -PE, & -PE-U PLUS Radios to address the so-called 45-day lock-up issue experienced by several users.

- This issue appears as a lock-up of the radio, requiring a reboot, on a periodic basis.
- This lock-up is caused by a memory register that overfills and corrupts nearby data.

- Units that are installed in different applications and with different equipment than the units that sparked this investigation, may experience the same issue, but with different time scales.

Note: This version becomes the default version of firmware and is backward compatible with all supported previous versions.

13.5. Version 3.01

Release Date: January 2015

PLUS Software 3.01 is released for the FGR2-P, -PE, & -PE-U PLUS Radios to correct a number of software issues.

Additions and Changes

- Radios running version 3.01 are now compatible with Discovery Server.
- IP Multicast traffic originating from the Endpoint side of the network is now fully propagated over-the-air to the Gateway side of the network.
- When using UDP functions (e.g., **Multicast** or Discovery Server), a valid **Default Gateway** MUST be set.
- When using **UDP Unicast**, a behavior change has been introduced.
 - Prior to v3.01, the Gateway would send to the last device that sent it data regardless of what IP address was defined in the **Serial Setup** window, **UDP IP** text box.
 - Now, in v3.01, the Gateway will only send to the device IP address listed in the **UDP IP** text box.

Known Limitations and Workarounds

- With VLANs and some other specific configurations, TCP/IP traffic can periodically time out over links unless the **MTU** parameter is adjusted to be lower than the 1500 byte default value.
 - The networks MUST BE adjusted accordingly.

FREEWAVE Recommends: Start with 1400 bytes in this scenario.

- If the network includes Repeaters, the **Repeaters** parameter in the **Radio Setup** settings must be set to **Enabled** for **ALL** radios, not just the Gateway.
 - Setting only the Gateway can result in packet loss.



Warning! Set the **Repeaters** parameter to **Enabled** on all radios in the network BEFORE upgrading.
Doing so after the upgrade is complete can still result in packet loss.

- **Multicast** port CANNOT be changed using the **Configuration Windows**.
 - Use the serial interface to change this parameter.

13.5.1. Warning: Extreme Set-Up Parameters

Important! As of release [Version 3.06 \(on page 184\)](#), this parameter setup has been addressed. The 30 day reboot recommendation is no longer in effect.

If these **Setup** parameters are used, a reboot of the network is recommended every 30 days:

- [IP Setup \(on page 186\)](#)
- [Serial Setup \(on page 186\)](#)
- [Security Setup \(on page 186\)](#)
- [SNMP Setup \(on page 187\)](#)

IP Setup

IP Setup	
Parameter	Setting
Spanning Tree	Enabled
MTU	1498
VLANs	Enabled
NTP	Enabled
Syslog	Enabled

Serial Setup

Serial Setup	
Parameter	Setting
TCP Server	Disabled
TCP Client	Disabled
UDP	Disabled
Multicast	Disabled
Runtime Serial Setup 'U'	Enabled
Modbus RTU	Disabled

Security Setup

Security Setup	
Parameter	Setting
RADIUS	Enabled
Peer to Peer	Disabled

SNMP Setup

SNMP Setup	
Parameter	Setting
SNMP Agent	Enabled
SNMP Trap	Enabled

13.5.2. ERRATA Information

- When upgrading from v2.22, the **Power Up Dest. IP & Port** text boxes were replaced with the **UDP IP & Port** text boxes in v3.01.
- When upgrading from v2.34, the **Power-Up / mcast IP & Port** text boxes were replaced with the **UDP IP & Port** text boxes in v3.01.

Important! Contact FreeWave Technical Support for assistance with the **Alarm** and **Drop Link** features.

These features have changed significantly from v2.22 and v2.34 to v3.01.

Using the serial ports as **Alarm Clients**, these parameters were hidden from the v3.01 **Serial Setup** window:

- **Enable Alarm** check box (v2.22 only)
- **Alarm IP & Port** text boxes (v2.22 only)
- **Utilize For Alarm** check box (v2.34 only)
- **Alarm Retry Limit (Attempts)** text box
- **Maintain / Drop Link** check box

If the FGR2-P, -PE, & -PE-U device is configured as an Alarm Client **and**

- it is sending the alarms to another device acting as a Terminal Server **and**
 - if the **Maintain Link** is enabled (cleared check box in v2.22 and v2.34) **then**
 - the Client will open multiple sockets on the Terminal Server.
- ALL of the multiple sockets will remain open.



Warning! The Terminal Server in v3.01 is limited to five (5) sockets.

These sockets will quickly become full.

Additional alarms from the Alarm Client to the Terminal Server will **NOT** be heard.

Return messages from the Terminal Server to the Alarm Client will **NOT** be heard.

13.5.3. Specific Upgrade Notes for the Serial Setup window

Upgrading from v2.22 to v3.01

- **TCP Server Settings** (i.e., the **Enabled** check box is checked) is enabled on both ports regardless of what setting was enabled in the v2.22 **Mode** list box.
- The **Mode** list box does not exist in v3.01.

FREEWAVE Recommends: Disable (clear the **TCP Servers Enable** check box) if a different **Mode** was used in v2.22.

- In v2.22, the **Local IP Port** setting in the **UDP Settings** area is now in the **UDP Settings** area as the **Port** text box in v3.01.
- The v2.22 **Power Up Dest. IP & Port** text boxes and their values are NOT transferred to v3.01.

Note: Settings established in previous versions are lost when upgrading to v3.01.

Important! If using the **UDP Unicast** mode, the user must re-program the **UDP** settings in ALL appropriate FGR2-P, -PE, & -PE-U devices.

Upgrading from v2.34 to v3.01

- If a port is configured for **Multicast** only in v2.34 then, after upgrade to v3.01, it is set to **UDP** mode AND **Multicast** mode (i.e., their respective **Enable** check box is checked).

FREEWAVE Recommends: Disable (clear the **Enable** check box) for the mode NOT in the network.

- In v2.34, the **Local UDP Port** setting in the **UDP/MULTICAST Settings** area is now in the **UDP Settings** area as the **Port** text box in v3.01.
- The **Power-Up / mcast IP & Port** text boxes and their values in v2.34 are NOT transferred to v3.01.

Note: Settings established in previous versions are lost when upgrading to v3.01.

- In v2.34, the **UDP** and **Multicast** settings were combined.
 - In v3.01, the **Multicast IP and Port** settings are in their own area of the **Serial Setup** window.
 - When upgrading from v2.34, the user's previous **Multicast** settings are replaced with the FreeWave defaults.

13.6. Version 2.34

Release Date: June 2014

Software 2.34 is released for the FGR2-P, -PE, & -PE-U PLUS Radios radios to correct a number of software issues.

Important! The critical bug fix is the RF Link Lock issue seen in some networks.

Additions and Changes

These are the issues corrected in PLUS Software 2.34:

- Ethernet Gateway radios (FGR2-P and FGR2-PE radios) locking up after 30 to 75 days.
- Global software upgrade causes radio to be non-functional.
- Default settings leave radio in a transmitting mode.

Known Limitations and Workarounds

- Radios running this current version of firmware are NOT compatible with Discovery Server.
 - Use the serial setup to obtain IP addresses.
- If the network includes Repeaters, the **Repeaters** parameter in the **Radio Setup** settings must be set to **Enabled** for **ALL** radios, not just the Gateway.
 - Setting only the Gateway can result in packet loss.



Warning! Set the **Repeaters** parameter to **Enabled** on all radios in the network BEFORE upgrading.
Doing so after the upgrade is complete can still result in packet loss.

- IP Multicast traffic originating **from the Endpoint side** of the network IS NOT fully and properly propagated over-the-air to the Gateway side of the network.
 - Multicast traffic **from the Gateway side** of the network IS properly propagated over-the-air to the Endpoint side of the network.
 - Therefore, the Multicast functionality for the terminal server is broken for any Endpoint/Repeater where responses are sent to the serial link on the Gateway radio's terminal server.
- With VLANs and some other specific configurations, TCP/IP traffic can periodically time out over links unless the **MTU** parameter is adjusted to be lower than the 1500 byte default value.

FREEWAVE Recommends: Start with 1400 bytes in this scenario.

- **Modem Stats** require a radio link to be accurate.

Note: Local Diagnostics are NOT supported.

- IP addresses throughout the configuration Web pages allow entries higher than 255.
- Free form text fields CANNOT use any of these characters: % & + = < >
- Time stamps included in SYSLOG messages appear in Unix time format.
 - With **NTP Client** enabled, the time shown in the configuration Web page status is in Unix time format and reported as GMT.
- Changing the MAC address filter using the global change functionality at the Gateway does not change the MAC address filter list in the Endpoints.
- Changing the **Transmit Rate** parameter using the terminal interface accessed through the serial port does not change the setting's value.

- Serial Port 2 does not maintain the correct setting for the **Runtime Serial Setup** parameter.

13.7. Version 2.22

Release Date: April 2011

Additions and Changes

- Added:
 - NTP options to the web server and the config server.
 - Logging to local file and to remote syslog server.
 - Ability to view log in separate window to the **Security** page.
 - Logging reboot messages.
 - **Users** page for user-level and password management.
 - **Global Save/Apply** functionality to **IP**, **Serial**, **Radio**, **Security**, **SNMP**, and **Users** pages.
 - **Global Enable/Disable** button to **Tools** page.
 - One second timeout to slaves during global upgrade to minimize rewind requests for packets that were already in the masters Tx buffer.
- Changed the **Program Radio** function to program all zones to 0xFFFF if in mode 3 or 7.
- Moved the **Password Manager** to the **Users** page.

Additional Notes

FreeWave only supports these versions:

- | | |
|-------------------------------|-------------------------------|
| • SSLv3 128 bits AES 128-SHA | • TLSv1 128 bits AES128-SHA |
| • SSLv3 128 bits RC4-MD5 | • TLSv1 128 bits RC4-MD5 |
| • SSLv3 128 bits RC4-SHA | • TLSv1 128 bits RC4-SHA |
| • SSLv3 168 bits DES-CBC3-SHA | • TLSv1 168 bits DES-CBC3-SHA |
| • SSLv3 256 bits AES 256-SHA | • TLSv1 256 bits AES 256-SHA |



The **Users** page is used to define who can edit the settings on the radio. Setting the user's permissions on this page determines whether they can save settings through Tool Suite and the Web pages.

Known Limitations and Workarounds

- **Modem Stats** require a radio link to be accurate.
- **Master Tx Beacon** is not supported on a setting higher than **1** in MultiPoint networks with Repeaters.

Appendix A: Factory Default Settings

FGR2-P, -PE, & -PE-U PLUS Radio Factory Default Settings	
Parameter	Setting
Serial Setup (1 and 2) Parameter	
Mode	TCP Server
TCP Server Port	Setup 1: 7000 Setup 2: 7001
TCP Server Alarm	Disabled
TCP Server Alarm IP & Port	Setup 1: 0.0.0.0 : 8000 Setup 2: 0.0.0.0 : 8001
TCP Server Maintain / Drop Link	Disabled
TCP Server Alarm Retry Limit (Attempts)	0
TCP Server Inactivity Timeout (Seconds)	0
TCP Client IP Address & Port	Setup 1: 0.0.0.0 : 9000 Setup 2: 0.0.0.0 : 9001
UDP Local IP Port	Setup 1: 6000 Setup 2: 6001

FGR2-P, -PE, & -PE-U PLUS Radio Factory Default Settings	
Parameter	Setting
UDP Power Up Dest. IP & Port	0.0.0.0 : 0 Setup 1: 0.0.0.0 : 0 : 6000 Setup 2: 0.0.0.0 : 0 : 6001
Multicast Address & Port	Setup 1: 225.0.0.38 : 11111 Setup 2: 225.0.0.38 : 22222
Baud Rate	19200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None
CD Mode	Normal
Interface	RS232
Modbus RTU	Enabled
IP Setup Parameter	
IP Address	192.168.111.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.111.1
Web Page Port	80
Spanning Tree	Disabled
Mode	Disabled
IP Address (VLAN Configuration)	192.168.111.100
Management VLAN ID	0
Data VLAN ID	0
NTP Client Enable	Disabled
NTP Client IP Address	0.0.0.0
Syslog Server Push To Server	Disabled
Syslog Server 1	0.0.0.0
Syslog Server 2	0.0.0.0
Radio Setup Parameter	
Network Type	Point-to-Point in software earlier than 2.30 Point-to-MultiPoint in software 2.30 and later

FGR2-P, -PE, & -PE-U PLUS Radio Factory Default Settings	
Parameter	Setting
Modem Mode	Gateway in software earlier than 2.30 MultiPoint Endpoint in software 2.30 and later
Frequency Key	5
Zones	All enabled
Max Packet Size	9
Min Packet Size	1
Transmit Power	10
Retry Timeout	255
RF Data Rate	154 kbps
Long Distance	Disabled
Point-to-Point Parameter	
Transmit Rate	Normal
MultiPoint Parameter	
Addressed Repeat	3
Broadcast Repeat	3
Slave Connect Odds	9 / Try Forever
Master Tx Beacon	9
Network ID	255 in software earlier than 2.30 1 in software 2.30 and later
Repeaters	Disabled
Subnet ID (RX)	F
Subnet ID (TX)	F in software earlier than 2.30 0 in software 2.30 and later
Security Parameter	
Enable RADIUS	Disabled
RADIUS IP Address	Blank
RADIUS Port Number	1812
Shared Secret	Blank
User-Password	Blank
AES Version	128
AES Encryption Key	Blank
MAC Filter	Blank
Detach Local Eth	Disabled

FGR2-P, -PE, & -PE-U PLUS Radio Factory Default Settings	
Parameter	Setting
Force SSL (https)	Disabled
Peer to Peer	Enabled
SNMP Parameter	
SNMP Version	Disabled
Read Community	Public
Write Community	Private
Authentication Password (v3)	Blank / MD5
Privacy Password (v3)	Blank / AES
Trap Version	Disabled
Trap Community	Blank / Private
Min Fault Time	300
Trap Manager1 IP	Blank
Trap Manager2 IP	Blank
Voltage	Alarm Above: 30 Alarm Below: 6
Rx % Rate	Alarm Below: 90
Tx % Rate	Alarm Below: 90
Reflected Power	Alarm Above: 2
S-N Delta	Alarm Below: 30
Signal	Alarm Below: - 90
Noise	Alarm Above: - 90
Users Parameter	
User Accounts	admin (permanent) guest
User Account Level	admin: 0 (permanent) guest: 3
Edit Group Level Rights	
IP Setup	Level 1: Read Only Level 2: Read Only Level 3: Read Only
Serial Setup	Level 1: Read Only Level 2: Read Only Level 3: Read Only


FGR2-P, -PE, & -PE-U PLUS Radio Factory Default Settings	
Parameter	Setting
Radio Setup	Level 1: Read Only Level 2: Read Only Level 3: Read Only
Security	Level 1: No Access Level 2: No Access Level 3: No Access
SNMP	Level 1: Read Only Level 2: Read Only Level 3: Read Only
RMA	Level 1: Read Only Level 2: Read Only Level 3: Read Only
Tools	Level 1: No Access Level 2: No Access Level 3: No Access
Tools Parameter	
Site Name	Blank
Site Contact	Blank
System Name	Blank
Notes	Blank
Global Change Capability	Disabled
Address of TFTP Server	Blank
File Name	Blank

Appendix B: FGR2-P, -PE, & -PE-U Technical Specifications

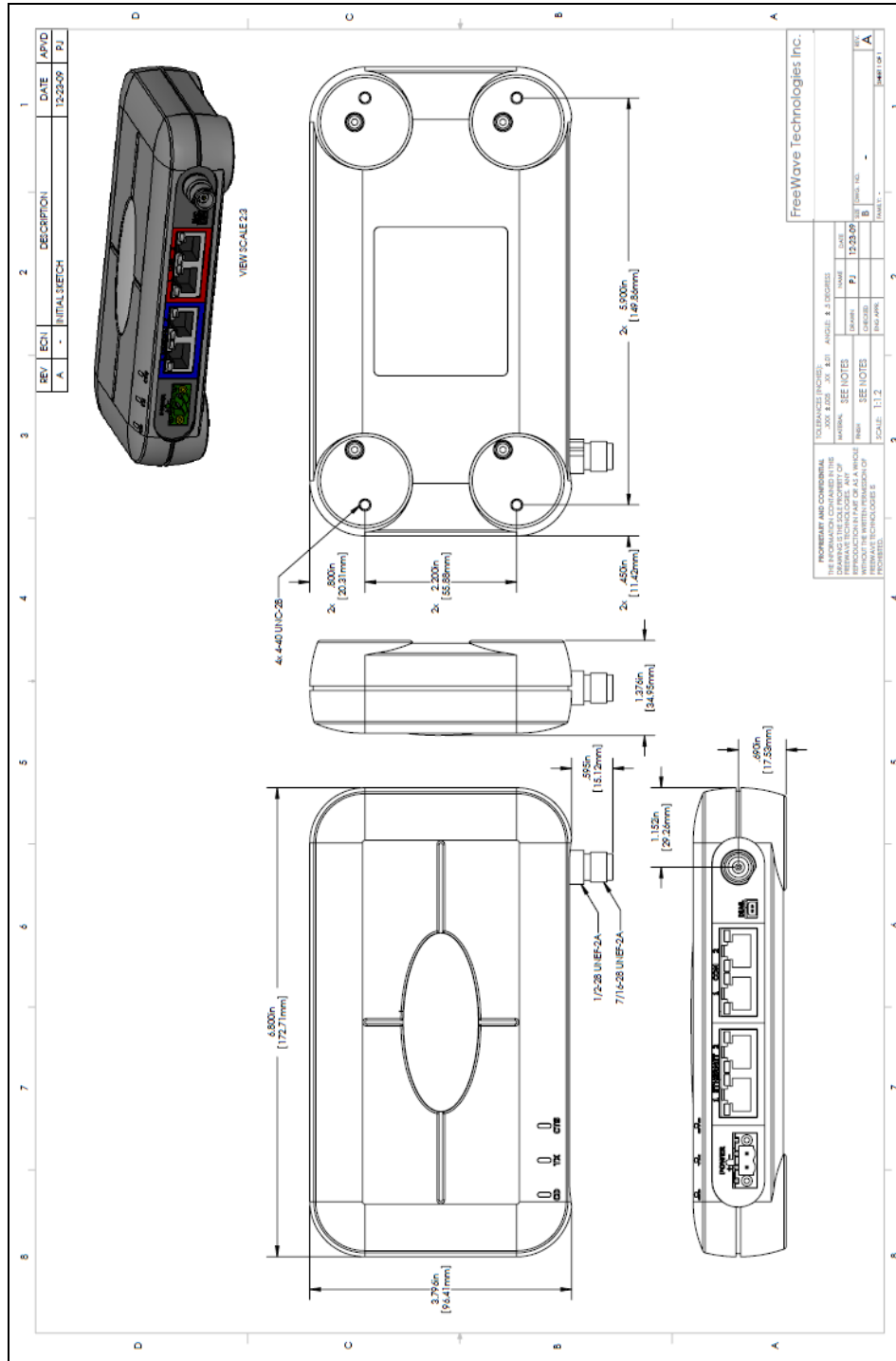
Specifications may change at any time without notice. For the most up-to-date specifications information, see the product's data sheet available at www.freewave.com.

FGR2-P, FGR2-PE, and FGR2-PE-U Technical Specifications	
Specification	Description
Frequency Range	902 to 928 MHz (FHSS)
Transmitter	
Output Power	5 mW to 1 W
Range—Line-of-Sight	60 miles, Clear Line of Sight
Modulation	2 level GFSK
RF Data Rate	<ul style="list-style-type: none"> • 153.6 Kbps High Speed • 115.2 Kbps Standard Speed
Occupied Bandwidth	230.4 kHz
Hopping Patterns	<ul style="list-style-type: none"> • 15 per band • 105 user selectable
Hopping Channels	112
Frequency Zones	<ul style="list-style-type: none"> • 16 zones • 7-8 channels per zone
Receiver	

FGR2-P, FGR2-PE, and FGR2-PE-U Technical Specifications				
Specification	Description			
Sensitivity	<ul style="list-style-type: none"> -108 dBm for 10⁻⁴ bit error rate at 115 Kbps -104 dBm for 10⁻⁴ bit error rate at 153.6 Kbps 			
Selectivity	20 dB at fc ± 230 kHz			
Data Transmission				
Error Detection	32 Bit CRC, retransmit on error			
Data Security	AES 128-bit encryption and FHSS Technology			
Data Throughput	<ul style="list-style-type: none"> 115.2 Kbps High Speed 80 Kbps Standard Speed 			
Serial Data Interface	RS232/RS422/RS485, programmable 2x RJ-45 Connector			
Ethernet Data Interface	<ul style="list-style-type: none"> 10/100 Base T 2x RJ-45 802.3 TCP ARP P Auto Crossover DHCP DNP3 over TCP ICMP Multicast TFT UDP 			
Diagnostics Connector	4-pin			
Power Requirements				
Operating Voltage	+6.0 to +30.0 VDC			
Typical Current	Mode	+6.0 VDC	+12.0 VDC	+30.0 VDC
	Transmit	1.1A	550 mA	220 Ma
	Receive	252 mA	150 mA	63 mA
	Idle	140 mA	71 mA	32 mA
General Information				
Operating Temperature	<ul style="list-style-type: none"> -40°C to +75°C -40°F to +167°F 			
Humidity	0 to 95% non-condensing			
Dimensions	<ul style="list-style-type: none"> FGR2-P: <ul style="list-style-type: none"> 7.0 L x 3.25 W x 1.25 H (inches) FGR2-PE and PE-U: <ul style="list-style-type: none"> 6.8 L x 3.8 W x 1.4 H (inches) (17.3 cm L x 9.6 cm W x 3.5 cm H) 			

FGR2-P, FGR2-PE, and FGR2-PE-U Technical Specifications	
Specification	Description
Weight	<ul style="list-style-type: none"> • FGR2-P: 0.5 lbs (215 g) • FGR2-PE and PE-U: 1.3 lbs (608 g)
RF Connector	<ul style="list-style-type: none"> • FGR2-PE_U and FGR2-PE: TNC, (Female) • FGR2-P: SMA, (Female)
Product Safety	
Standards	EN 60079-0:2012 + A11:2013 and EN 60079-15:2010
Labeling Information	 II 3 G Ex nA IIC Gc DEMKO 14 ATEX 1209313U

Appendix D: FGR2-PE and PE-U Mechanical Drawing



Appendix E: Object List for FREEWAVE-TECHNOLOGIES-MIB

Object List for FREEWAVE-TECHNOLOGIES-MIB			
Object	Description	Access	Syntax
fwtPlusModemIndex	An index used to identify a specific radio modem within the system.	Not Accessible	Unsigned32
fwtPlusModemSignal	The received signal level for this radio modem, in dBm.	Read Only	Integer 32
fwtPlusModemNoise	The detected noise for this radio modem, in dBm.	Read Only	Integer 32
fwtPlusModemSupplyVoltage	The supply voltage to this radio modem, in units of one hundredth of a volt.	Read Only	Hundredth
fwtPlusModemRxRate	The current receive rate as a percentage of the maximum, in units of one hundredth of a percent.	Read Only	Hundredth
fwtPlusModemReflectedPower	The current amount of reflected RF power.	Read Only	Unsigned32
fwtModemTemperature	The current temperature of this radio modem in degrees Celsius.	Read Only	Integer 32

Object List for FREEWAVE-TECHNOLOGIES-MIB			
Object	Description	Access	Syntax
fwtPlusModemRange	The current approximate range of this radio modem from its peer, in meters.	Read Only	Unsigned32
fwtPlusModemTxRate	The current transmit rate as a percentage of the maximum, in units of one hundredth of a percent.	Read Only	Hundredth
fwtPlusModemSNDelta	The current margin (absolute) between the received signal and the noise at this radio.	Read Only	Integer32
fwtPlusModemVendorString	The name of the vendor of this radio modem.	Read Only	DisplayString
fwtPlusModemConnectedTo	The serial number of the radio that we currently have an RF link with.	Read Only	Integer32
fwtPlusModemUpstreamSignal	The received signal level that the upstream radio receives from this radio, in dBm.	Read Only	Integer32
fwtPlusModemUpstreamNoise	The Noise level that the upstream radio receives from this radio, in dBm.	Read Only	Integer32
fwtPlusModemDisconnectCount	The Number of times this radio has lost its RF link.	Read Only	Unsigned32
fwtPlusModemPacketRxCount	The Number of Ethernet packets the radio has received over its RF link.	Read Only	Unsigned32
fwtPlusModemPacketTxCount	The Number of Ethernet packets the radio has sent over its RF link.	Read Only	Unsigned32
fwtPlusModemDroppedCount	The Number of Ethernet packets the radio has dropped	Read Only	Unsigned32

Object List for FREEWAVE-TECHNOLOGIES-MIB			
Object	Description	Access	Syntax
fwtPlusModemBadCount	The Number of BAD/corrupt Ethernet packets the radio has received over its RF link.	Read Only	Unsigned32
fwtPlusModemNetworkMode	The network mode to be used by a radio modem.	Read/Write	INTEGER {pointToPoint (1), Multipoint (2)}
fwtPlusModemMode	The modem mode to be used by a radio modem.	Read/Write	INTEGER {gateway (1), repeater (2), endpoint (3)}
fwtPlusModemFrequencyKey	The frequency key to be used by a radio modem.	Read/Write	Unsigned32 (0..14)
fwtPlusModemMinPacketSize	The minimum packet size to be used by a radio modem.	Read/Write	Unsigned32 (0..9)
fwtPlusModemMaxPacketSize	The maximum packet size to be used by a radio modem.	Read/Write	Unsigned32 (0..9)
fwtPlusModemTxPower	The transmit power to be used by a radio modem.	Read/Write	Unsigned32 (0..10)
fwtPlusModemRetryTimeout	How many times a radio modem should try to transmit a packet before timing out.	Read/Write	Unsigned32 (0..255)
fwtPlusModemRFDataRate	The RF data rate to be used by a radio modem. Permissible values are 1200,867,614,154,115 depending on the radio series radios.	Read/Write	Unsigned32
fwtPlusModemBroadcastRepeat	The number of times a Gateway will send out a packet of information before moving on to the next.	Read/Write	Unsigned32 (0..9)
fwtPlusModemNetworkID	A numerical ID that radios use to decide which network they are allowed to link to.	Read/Write	Unsigned32 (0..4095)

Object List for FREEWAVE-TECHNOLOGIES-MIB			
Object	Description	Access	Syntax
fwtPlusModemRepeaters	Allows for repeaters in the network, or not.	Read/Write	INTEGER {enabled (1), disabled (2)}
fwtPlusModemRxSubnetID	A numerical ID that radios use to decide which subnet they are allowed to link to.	Read/Write	Unsigned32 (0..15)
fwtPlusModemTxSubnetID	A numerical ID that radios use to decide which subnet they will transmit on.	Read/Write	Unsigned32 (0..15)
fwtPlusModemReboot	Set to 1 to reboot radio. This will force any changes to take effect.	Read/Write	INTEGER (0..1)
fwtPlusModemMaxSlaveRetry	The maximum number of times an Endpoint can attempt to deliver data to the Gateway before it discards the data.	Read/Write	Unsigned32 (0..9)
fwtPlusModemSystemName	A textual identifier for a given system.	Read/Write	DisplayString (SIZE (0..32))
fwtPlusModemFreqZoneIndex	An index used to identify a specific frequency zone for a specific radio modem.	Not Accessible	Unsigned32
fwtPlusModemFreqZoneDescr	A textual description of a specific frequency zone for a specific radio modem.	Read Only	DisplayString
fwtPlusModemFreqZoneEnabled	If the value of this object is true(1) then the referenced frequency zone is enabled for the relevant radio modem; if the value of this object is false(2), then the frequency zone is disabled.	Read/Write	TruthValue

Group Object List for FREEWAVE-TECHNOLOGIES-MIB

Group Object List for FREEWAVE-TECHNOLOGIES-MIB		
Group Object	Description	Objects
fwtPlusModemSupplyVoltageBad	This notification is generated when the supply voltage for a radio modem goes out of specification.	fwtPlusModemSupplyVoltage fwtPlusModemVendorString fwtPlusModemSystemName
fwtPlusModemRxRateBad	This notification is generated when the receive rate for a radio modem goes out of specification.	fwtPlusModemRxRate fwtPlusModemVendorString fwtPlusModemSystemName
fwtPlusModemTxRateBad	This notification is generated when the transmit rate for a radio modem goes out of specification.	fwtPlusModemTxRate fwtPlusModemVendorString fwtPlusModemSystemName
fwtPlusModemReflectedPowerBad	This notification is generated when the reflected power for a radio modem goes out of specification.	fwtPlusModemReflectedPower fwtPlusModemVendorString fwtPlusModemSystemName
fwtPlusModemSNDeltaBad	This notification is generated when the Signal to Noise delta for a radio modem goes out of specification.	fwtPlusModemSNDelta fwtPlusModemVendorString fwtPlusModemSystemName

Group Object List for FREEWAVE-TECHNOLOGIES-MIB		
Group Object	Description	Objects
fwtPlusModemSignalBad	This notification is generated when the Signal to Noise delta for a radio modem goes out of specification.	fwtPlusModemSNDelta fwtPlusModemVendorString fwtPlusModemSystemName
fwtPlusModemNoiseBad	This notification is generated when the Noise for a radio modem goes out of specification.	fwtPlusModemNoise fwtPlusModemVendorString fwtPlusModemSystemName

Group Object List for FREEWAVE-TECHNOLOGIES-MIB		
Group Object	Description	Objects
fwtPlusModemStatusGroup	A collection of objects concerned with the current status of a radio modem.	fwtPlusModemSignal fwtPlusModemNoise fwtPlusModemSupplyVoltage fwtPlusModemRxRate fwtPlusModemReflectedPower fwtPlusModemTemperature fwtPlusModemRange fwtPlusModemTxRate fwtPlusModemSNDelta fwtPlusModemVendorString fwtPlusModemConnectedTo fwtPlusModemUpstreamSignal fwtPlusModemUpstreamNoise fwtPlusModemDisconnectCount fwtPlusModemPacketRxCount fwtPlusModemPacketTxCount fwtPlusModemPacketDroppedCount fwtPlusModemPacketBadCount

Group Object List for FREEWAVE-TECHNOLOGIES-MIB		
Group Object	Description	Objects
fwtPlusModemControlGroup	A collection of objects concerned with the current status of a radio modem.	fwtPlusModemNetworkMode fwtPlusModemMode fwtPlusModemFrequencyKey fwtPlusModemMinPacketSize fwtPlusModemMaxPacketSize fwtPlusModemTxPower fwtPlusModemRetryTimeout fwtPlusModemRFDataRate fwtPlusModemBroadcastRepeat fwtPlusModemNetworkID fwtPlusModemRepeaters fwtPlusModemRxSubnetID fwtPlusModemTxSubnetID fwtPlusModemReboot fwtPlusModemMaxSlaveRetry fwtPlusModemSystemName fwtPlusModemFreqZoneDescr fwtPlusModemFreqZoneEnabled

Appendix F: FreeWave Legal Information

Export Notification

FreeWave Technologies, Inc. products may be subject to control by the Export Administration Regulations (EAR) and/or the International Traffic in Arms Regulations (ITAR). Export, re-export, or transfer of these products without required authorization from the U.S. Department of Commerce, Bureau of Industry and Security, or the U.S. Department of State, Directorate of Defense Trade Controls, as applicable, is prohibited. Any party exporting, re-exporting, or transferring FreeWave products is responsible for obtaining all necessary U.S. government authorizations required to ensure compliance with these and other applicable U.S. laws. Consult with your legal counsel for further guidance.

Restricted Rights

Any product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

This manual is only for use by purchasers and other authorized users of FreeWave products.

No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, or for any purpose without the express written permission of FreeWave Technologies, Inc. FreeWave reserves the right to make changes to this manual without notice. FreeWave assumes no responsibility or liability for the use of this manual or the infringement of any copyright or other proprietary right.

FreeWave products are designed and manufactured in the United States of America.

FCC Notifications

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: 1) This device may not cause harmful interference and 2) this device must accept any interference received, including interference that may cause undesired operation.

The content of this guide covers FreeWave Technologies, Inc. models sold under FCC ID: KNY-42182112519.

All models sold under the FCC ID(s) listed above must be installed professionally and are only approved for use when installed in devices produced by FreeWave Technologies or third party OEMs with the express written approval of FreeWave Technologies, Inc. Changes or modifications should not be made to the device.

FCC NEMA Installation and Label

Where applicable, the models described in this guide must be installed in a NEMA enclosure. When any FreeWave Technologies, Inc. module is placed inside an enclosure, a label must be placed on the outside of the enclosure. The label must include the text "**Contains Transmitter Module with FCC ID: KNY-42182112519.**"

FCC Notification of Power Warning

The FGR2-P, -PE, & -PE-U covered in this document have a maximum transmitted output power of 1W. The antennas used **MUST** have a separation distance of at least 23 cm from all persons and **MUST NOT** be co-located or operate in conjunction with any other antenna or transmitter.

IC Notifications

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Ce dispositif est conforme aux normes permis-exemptes du Canada RSS d'industrie. L'opération est sujette aux deux conditions suivantes : (1) ce dispositif peut ne pas causer l'interférence, et (2) ce dispositif doit accepter n'importe quelle interférence, y compris l'interférence qui peut causer le fonctionnement peu désiré du dispositif.

UL Notifications / Warnings - Class1 Div2

Warning! The FGR2-PE is NOT UL certified.
Use the FGR2-PE-U if an enclosed solution that is UL certified is needed.

The FGR2-P and FGR2-PE-U radios are suitable for use in Class I, Division 2, Groups A, B, C, and D or non-hazardous locations only.

Important! Do NOT connect any connectors while the circuit is live unless the area is known to be non-hazardous.

UL Power Source

Important! Input power **MUST** be derived from a single Class 2 power source.

Note: Input voltage for the listed models is +6.0 to +30.0 VDC.

**GNU License Notification**

Some of the software in the software is licensed under the GNU General Public License and other Open Source and Free Software licenses. You can obtain corresponding source by contacting FreeWave and requesting the source on CD.

...
FREEWAVE