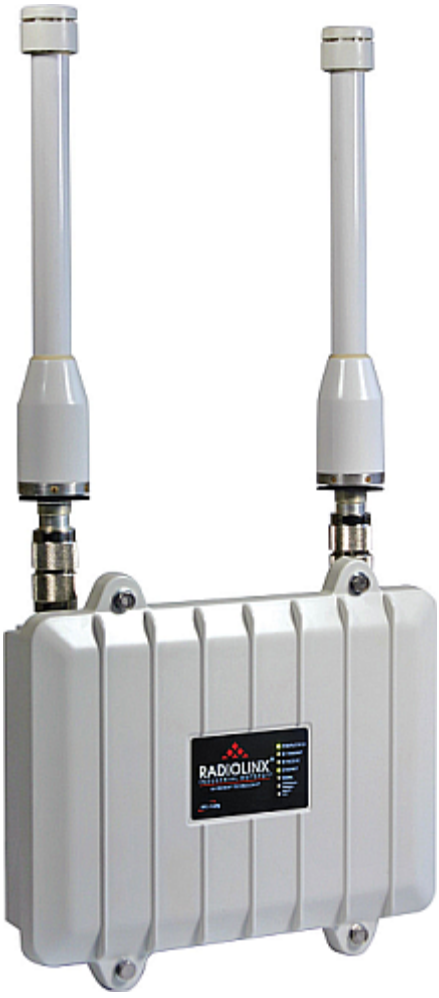
ProSoft® TECHNOLOGY

Where Automation Connects.



RadioLinx®

# RLXIB-IHW-66

**802.11a, b, g**

Industrial Hotspot

May 18, 2009

**USER MANUAL**

## United States FCC & Industry Canada rules

OQ7IHW

3656A-IHW

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: The device may not cause harmful interference, and it must accept any interference received, including interference that may cause undesired operation.
This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAUTION: Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

## Antenna spacing requirements for user safety

It is important to keep the radio's antenna a safe distance from the user. To meet the requirements of FCC part 2.1091 for radio frequency radiation exposure, this radio must be used in such a way as to guarantee at least 20 cm between the antenna and users. Greater distances are required for high-gain antennas. The FCC requires a minimum distance of 1 mW *cm2 power density from the user (or 20 cm, whichever is greater).
If a specific application requires proximity of less than 20 cm, the application must be approved through the FCC for compliance to part 2.1093.
The installer of this radio equipment must ensure that the antenna is located or pointed in such a way that it does not emit RF fields in excess of Health Canada limits for the general population; refer to Safety Code 6, obtainable from Health Canada.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

## Regulatory Approvals

### Wireless Approvals

| | |
|---|---|
| OQ7IHW | 3656A-IHW |

Visit our web site at http://www.prosoft-technology.com for current wireless approval information.

| Ordinary Locations | Hazardous Locations |
|---|---|
| 243333 | ATEX Zone 2 Category 3 |

ANSI/CSA - IEC60950-1/C22.2 No. 0-M91

## RLXIB-IHW-66: ATEX Approval

 II 3 G
Ex nA IIC T6 X
-30C° <= Ta <60°C
ProSoft Technology, Inc., Bakersfield, CA USA
Model: RLXIB-IHW-66
S/N: XXXXXXXXXX

**Caution:**

Read instructions before operating in Hazardous Areas
N. America

Product name: RLXIB-IHW-66
Safety Warning Statements
Explosive Atmosphere

Power, Input, and Output (I/O) wiring must be in accordance with the authority having jurisdiction

**A** Warning – Explosion Hazard – Do not make or break connections in an explosive atmosphere.
**B** Warning – DO NOT OPEN WHEN ENERGIZED.

## European CE certification

The radio modem has been approved for operation under the RTT&E directive, passing the following tests: ETS300-826 (EMC), ETS300-328 (Functionality), and EN60950 (Safety). LVD directive.
The following is the appropriate label that is applied to the radio modem product line to indicate the unit is approved to operate with CE certification:

The following is the appropriate label that is applied to the radio modem product line shipping package to indicate the unit is approved to operate with CE certification:

| | | | |
|---|---|---|---|
| AUS | B | DK | FIN |
| F | D | GR | IRE |
| I | LUX | NL | P |
| E | S | UK | |

Note: Member states in the EU with restrictive use for this device are crossed out. This device is also authorized for use in all EFTA member states (CH, ICE, LI, and NOR).
IMPORTANT: This device is a 2.4-GHz, low-power RF device intended for office and home use in all EU and EFTA member states, except in France where restrictive use applies.

## Connecting Power to the RLXIB-IHW-66 Radio

The radio shall be installed by trained personnel only, as outlined to the installation instructions provided with each radio.

The equipment shall be installed by a qualified installer/electrician. The installer/electrician is responsible for obtaining a secured ground connection between the lug terminal on the surge protector to a verified common ground point using a minimum 18 gauge wire. This must be done when attaching power lines to the radio during installation. .

A solid ground connection should be verified using a meter prior to applying power to the radio. Failing to secure a proper ground could result in serious injury or death as a result of a lightning strike.

## Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about the product, documentation or support, please write or call us.

**ProSoft Technology**
5201 Truxtun Ave., 3rd Floor
Bakersfield, CA 93309
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
http://www.prosoft-technology.com



RLXIB-IHW-66 User Manual
May 18, 2009



## ProSoft Technology® Product Documentation

In an effort to conserve paper, ProSoft Technology no longer includes printed manuals with our product shipments. User Manuals, Datasheets, Sample Ladder Files, and Configuration Files are provided on the enclosed CD, and are available at no charge from our web site: http://www.prosoft-technology.com

Printed documentation is available for purchase. Contact ProSoft Technology for pricing and availability.

Asia Pacific: +603.7724.2080
Europe, Middle East, Africa: +33 (0) 5.3436.87.20
Latin America: +1.281.298.9109
North America: +1.661.716.5100

# Contents

# 1 Start Here

*In This Chapter*



For most applications, the installation and configuration steps described in the following topics will work without additional programming. ProSoft Technology strongly recommends that you complete the steps in this chapter before developing a custom application.

## 1.1 About the RadioLinx® Industrial Hotspot™

The RadioLinx® 802.11abg Industrial Hotspot™ (RLXIB-IHW) is a high-speed wireless Ethernet radio, with PoE and Serial Encapsulation. The RLXIB-IHW operates at speeds up to 54 Mbps, using the IEEE 802.11b/g (2.4 GHz band) and 802.11a (5 GHz band) standards. Designed for global installations, the RLXIB-IHW offers many Industrial features including hazardous location certifications (pending), IGMP Snooping, OFDM for noise immunity, repeater mode for mesh architecture/self healing, OPC server diagnostics, extended temperature, high vibration/shock and din-rail mounting.

The RadioLinx® Industrial Hotspot (RLXIB-IHW-66) provides high speed industrial wireless Ethernet communications between Ethernet devices such as PLCs, I/O, and operator interfaces while serving as a repeater/bridge for other hotspots, and an access point for wireless clients such as Laptops and PDAs.

### *1.1.1 Specifications*

#### Radio

| | |
|---|---|
| Frequency Band<br>(Varies by Country) | **802.11b/g:**<br>2.412 to 2.462 GHz (FCC)<br>2.412 to 2.472 GHz (ETSI)<br>**802.11a:**<br>5.150 to 5.250 GHz (FCC/ETSI)<br>5.725 to 5.850 GHz (FCC) |
| Wireless Standards | 802.11a, 802.11b, 802.11g, 802.11i |
| Transmit Power<br>(Programmable) | Up to 50 mW |
| Channel data rates<br>(Modulation) | 802.11b: 11, 5.5, 2, 1 Mbps<br>(DSSS - BPSK, QPSK, CCK)<br>802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (OFDM)<br>802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (OFDM) |
| Receiver Sensitivity (Typical) | -95 dBm @ 1 Mbps<br>-90 dBm @ 11 Mbps<br>-82 dBm @ 24 Mbps<br>-75 dBm @ 54 Mbps |
| Channels Selection | 1 to 13 (802.11b/g)<br>36, 40, 44, 48, 149, 153, 157, 161, 165 (802.11a) |
| Security | WPA2/802.11i with 128/192/256 bit AES-CCM<br>Legacy WPA TKIP, WEP support<br>MAC ID filter<br>Admin password |

#### Physical

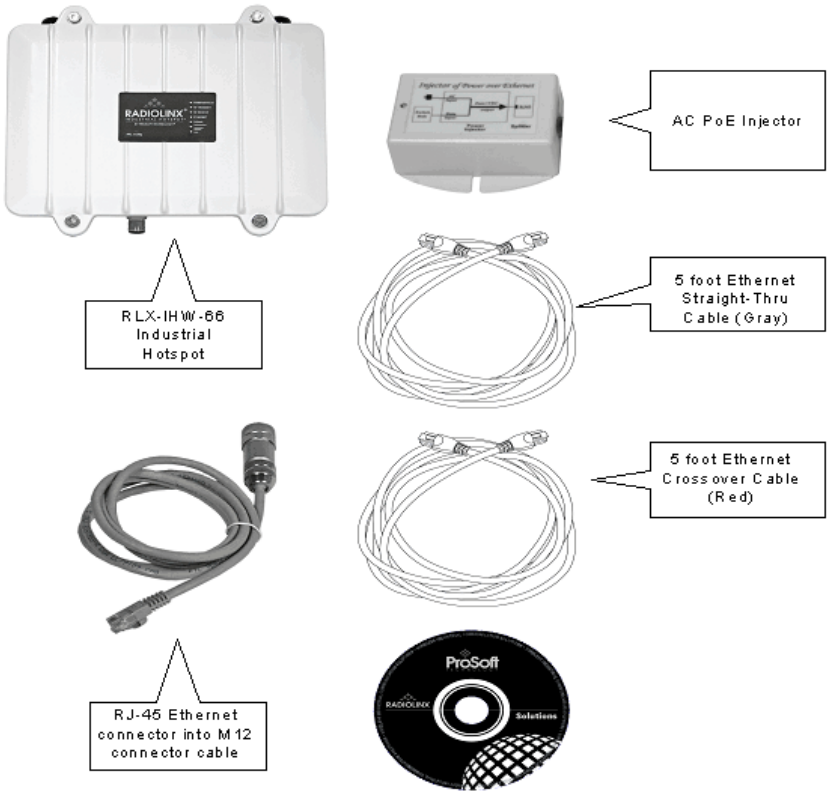
| | |
|---|---|
| Enclosure | IP-66 rated die-cast aluminum with pole mount hardware<br>6 = Dust tight - No ingress of Dust<br>6 = Protected against water jets against the enclosure from any direction shall have no harmful effects. |
| Overall Dimensions | 213 x 178 x 56 mm / 8.4 x 7.0 x 2.2 inches (W x H x D) |
| Ethernet Ports | Water/Dust Tight M12 connector<br>IEEE 802.3, 802.3u, 802.3x, 802.3af |
| Antenna Ports | (2) N-type female connectors |
| Weight | 2.4 lb (1kg) |

#### Environmental

| | |
|---|---|
| Operating Temperature | -30° C to +60° C |
| Humidity | To 90% RH, non-condensing |
| External Power | 802.3af PoE |
| Average Power | <6W |

## 1.2 Package Contents

Your RLXIB-IHW-66 Industrial Hotspot is shipped with the following:




In addition, you will need:

- A personal computer equipped with an Ethernet port
- Static IP address, Subnet Mask and Gateway information for each RLX device you plan to install. You can obtain this information from your system administrator.

Note: This Startup Guide is designed for use with two RLXIB-IHW-66 radios. One radio will be setup as a Master (AP) while the other radio will be set up as a remote repeater.

## 1.3 System Requirements

The RadioLinx IH Browser configuration tool is designed for Microsoft Windows XP, 2000 and 2003. Minimum hardware requirements are:

- Pentium® II 450 MHz minimum. Pentium III 733 MHz (or better) recommended
- Supported operating systems:
  - Microsoft Windows XP Professional with Service Pack 1 or 2
  - Microsoft Windows 2000 Professional with Service Pack 1, 2, or 3
  - Microsoft Windows Server 2003
  - Microsoft Windows Vista
- 128 Mbytes of RAM minimum, 256 Mbytes of RAM recommended
- CD-ROM drive
- 100 MB available hard drive space
- Available RS-232 serial port and null modem cable
- 256-color VGA graphics adapter, 800 x 600 minimum resolution (True Color 1024 x 768 recommended)
- Ethernet hub with standard RJ45 Ethernet cable
  *or*
  Ethernet port with RJ45 crossover cable for direct connection to module
- A web browser, for example Microsoft Internet Explorer or Firefox.

In addition, you will need

- A connection to an existing wired or wireless Ethernet network, with a Static or Dynamic IP address for your computer
- Static IP address, Subnet Mask and Gateway address for each RadioLinx device you plan to install. Obtain this information from your system administrator

## 1.4 Install the IH Browser Configuration Tool

**1** Insert the ProSoft Solutions CD in your CD-ROM drive. On most computers, a menu screen will open automatically. If you do not see a menu within a few seconds, follow these steps:

- **a** Click the Start button, and then choose Run.
- **b** In the Run dialog box, click the Browse button.
- **c** In the Browse dialog box, click "My Computer". In the list of drives, choose the CD-ROM drive where you inserted the ProSoft Solutions CD.
- **d** Select the file **prosoft.exe**, and then click Open.
- **e** On the Run dialog box, click OK.

**2** On the CD-ROM menu, select Setup Software under RLXIB-IHW-66 Industrial Hotspot. This action opens the Setup Wizard for IH Browser.

**3** Follow the instructions on the installation wizard to install the program with its default location and settings.

**4** When the installation finishes, you may be prompted to restart your computer if certain files were in use during installation. The updated files will be installed during the restart process.

## 1.5 Planning the Network

Before you configure and install the network, you should create a plan for it. The following points assume that you are creating a bridge network of masters and repeaters, but you can also set up clients to work with devices on existing wireless LANs. For information, see Set Up a Client.

To begin, determine where you need radios and then choose locations for them accordingly. For example, you might decide to install your master radio near a PC in a central plant location. (You can use the PC to configure the radios through the Radio Configuration / Diagnostic Utility.) If the plant is an oil refinery, for example, you might decide to install radios near the oil tanks.

The next important issue is how to link the radios. Unless the radios are very close together, you must make sure that each pair of radio antennas in the network has a line of sight between them. In other words, you must be able to see from one antenna to another, either with the naked eye or binoculars.

If a line of sight does not exist between antennas, you must choose a site for installing a repeater radio, which will create a bridge between the radio antennas.

Choose the appropriate antennas for the network. If an antenna will be connected to the radio by a long cable, you might need to purchase a power amplifier, which is available from ProSoft Technology. The more distance between an antenna and its radio, the more signal loss the radio will have. For more information, see Antennas.

Consider drawing up your network plans on paper. As part of the drawing, you should assign a logical name to each radio. You can use these names later when configuring the radios in the Radio Configuration / Diagnostic Utility.

As part of your planning, you might want to conduct a site survey. ProSoft Technology can perform this survey, you can do it yourself, or you can hire a surveyor.

Protect radios from direct exposure to weather, and provide an adequate, stable power source. Make sure that your plan complies with the radio's power requirements (page 82) and cable specifications (page 83).

**Important:** Radios and antennas must be located at least 8 inches (20 cm) away from personnel.

### *1.5.1 Installation Questions*

| Answer the following questions to make your installation easier, and to familiarize yourself with your system and what you want to do. |
|---|
| How many radios in your network? |
| Master ID |
| Repeater ID |
| Client ID |
| Locations |
| Is there a Line of Sight between them? |
| Selected the appropriate antennas for your network? |

## 1.6 Configuring the Radios

To configure the network radios, follow these steps.

Use the RLX-IH Browser to display all radios on the network, and then use a Web browser or SNMP manager to view and change radio settings. The radio package includes the program CD, power supply, Ethernet cable, and a small antenna. You must install the antenna later, but it is not needed to get started.

IMPORTANT: If possible, you should configure all the radios side by side in an office setting and make sure they link before you try to install them in the field.

*To configure the radios in a network:*

**1** Start the IH Browser (page 14) configuration application.

The PC must have a wired or wireless Ethernet connection configured with a static or dynamic IP address.

**2** Plug in the Ethernet cable with PoE Injector to the RLXIB-IHW-66 radio, wait a moment for the radio to power up, and then examine the radio's LED display to make sure the radio is working properly.

**3** Assign a temporary IP address: (page 16) Double-click the radio listing in the RLX-IH Browser. In the next window, click OK to accept the temporary IP address, subnet mask, and default gateway.

**4** Double-click the radio listing again in the RLX-IH Browser to open the Radio Configuration / Diagnostic Utility in your web browser. Enter "password" (lower case, no quotes) in the next window and then click Login.

If necessary, you can enter your own password later. For information, see Change Password (page 57).

**5** Set up the master radio (page 17) first, using the Radio Settings window in the Radio Configuration / Diagnostic Utility.

6 Click Apply Changes to save the master radio settings.

To cancel the settings and start over, click the Cancel Changes button before you click Apply Changes. After they are configured, master radios are preceded by an "M" in the utility window list.

Note: The text shown in yellow at the bottom of the window indicates the status of changes you have made to the configuration.

- If the text shows "Changes not saved", click Apply Changes to save your settings.
- If the text shows "Changes not saved; Will disrupt X s", you can click Apply Changes, however the network will be disrupted temporarily while the changes are applied. The value of "X" indicates the number of seconds the network will be offline.

7 Unplug the Ethernet cable from the radio and plug it into the next radio to be configured.

8 Set Up a Repeater. (page 20) Return to the RLX-IH Browser. To be sure that you are seeing the latest status of the radio(s), go to the toolbar (page 73) and click the "Clear" icon (eraser) followed by the "Scan" icon (binoculars). Double-click the listing of the next radio to be configured, and configure it as a repeater radio.

9 Save the Radio Configuration. (page 19) Save the repeater radio settings by clicking Apply Changes at the bottom of the Radio Settings screen. Repeat steps 7 through 9 to configure each repeater in the network.

10 After configuring the network and its radios, physically label each radio. Labeling eliminates confusion about which radios correspond with which radio configurations in the software. You should identify the radio's name, network SSID, and IP address, if set.

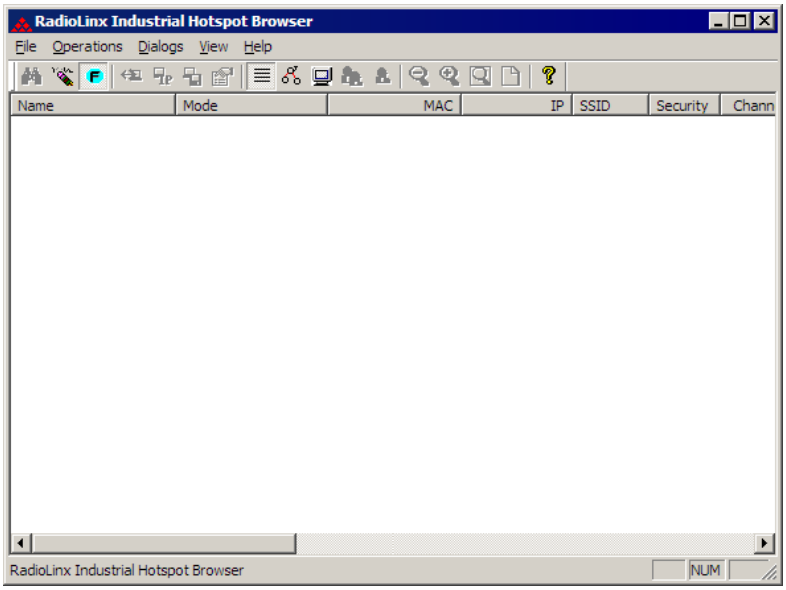
11 Install the radios and antennas (page 23).

The remainder of the topics in this section describe each of these steps in more detail.

### 1.6.1 Start IH Browser

*To start IH Browser*

1. Click the Start button, and then choose Programs.
2. In the Program menu, navigate to ProSoft Technology.
3. In the ProSoft Technology menu, navigate to RadioLinx.
4. Click RadioLinx IH Browser.




The window lists all the radios your computer can access. The MAC ID number is essentially the serial number of the radio; this number is also printed on the side of the radio. If a radio listing does not appear in the window, select Scan from the File menu. If you still do not see a radio listing, see Troubleshooting.

### 1.6.2 Plug In the Cables

You can configure the RLXIB-IHW-66 using the Ethernet port on the underside of the radio.

- If you are connecting to the radio through an Ethernet hub or switch, use the 2 gray (straight-through) cables.
- If you are connecting to the radio directly from your PC without going through an Ethernet hub or switch, you must use the red (crossover) cable and a gray (straight-through) cable.

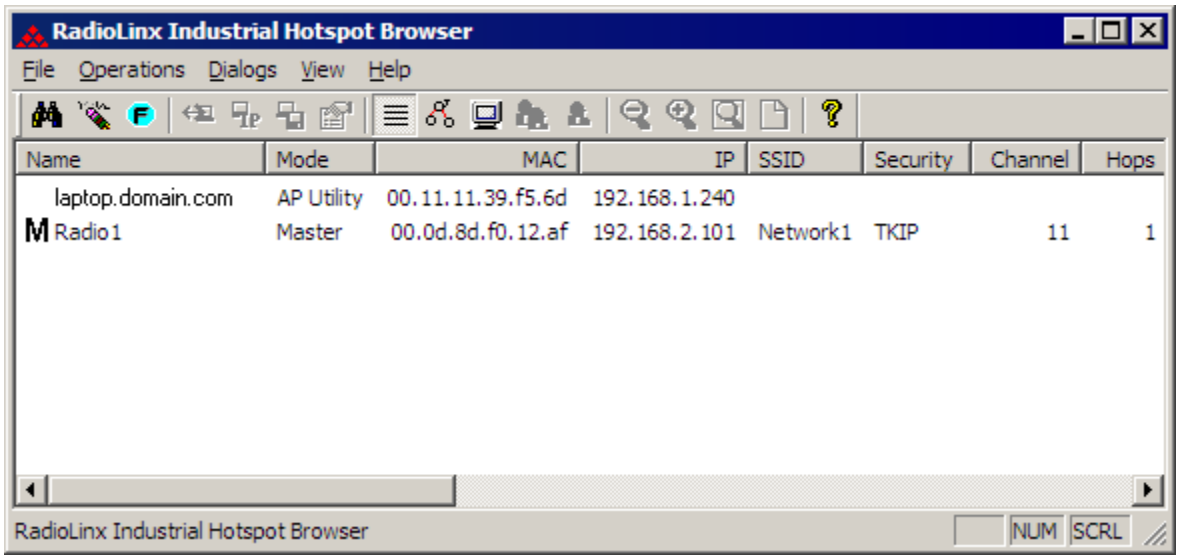
Note: After you plug in the Ethernet cable (which supplies both power and connectivity), the radio performs a startup procedure that includes a self-test, loading the main program, and initializing the radio. This startup procedure can take up to two minutes.

After the startup procedure has completed successfully, the Power/Status LED should be green, meaning that the radio has power. The Ethernet LED should also be green, meaning that the Ethernet connection is working. The RF Transmit and RF Receive LEDs should blink.

For information on making connections, see Radio power requirements (page 82) and Cable specifications (page 83).

### 1.6.3 Detecting the Radio

After the radio has completed its startup procedure, the radio will appear in the IH Browser window.




The window lists all the radios your computer can access. The MAC ID number is essentially the serial number of the radio; this number is also printed on the side of the radio. If a radio listing does not appear in the window, select Scan from the File menu. If you still do not see a radio listing, see Troubleshooting.

Tip: If a radio listing does not appear in the window, open the File menu and choose Scan. If you still do not see a radio listing, refer to Diagnostics and troubleshooting in the RLXIB User Guide.

### *1.6.4 Assign a Temporary IP Address*

You need the IP address to log into the Radio Configuration/Diagnostic Utility and configure the radio settings. If the radio is connected to a network with a DHCP server, the radio may already have an IP address assigned to it.

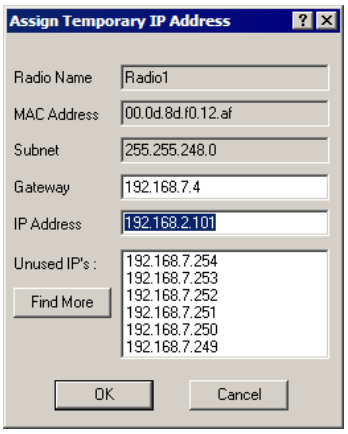
If a DHCP server is not available, or if you prefer to assign a static IP address, you can enter a temporary IP here. You will use the Radio Configuration / Diagnostic Utility (page 31) to assign a permanent IP address.

*To assign a temporary IP Address*

**1** In IH Browser, click to select the radio.

Tip: If a radio listing does not appear in the window, open the File menu and choose Scan. If you still do not see a radio listing, refer to Diagnostics and troubleshooting in the RLXIB User Guide.

**2** Open the Operations menu, and choose Assign IP. This action opens the Assign Temporary IP Address dialog box.



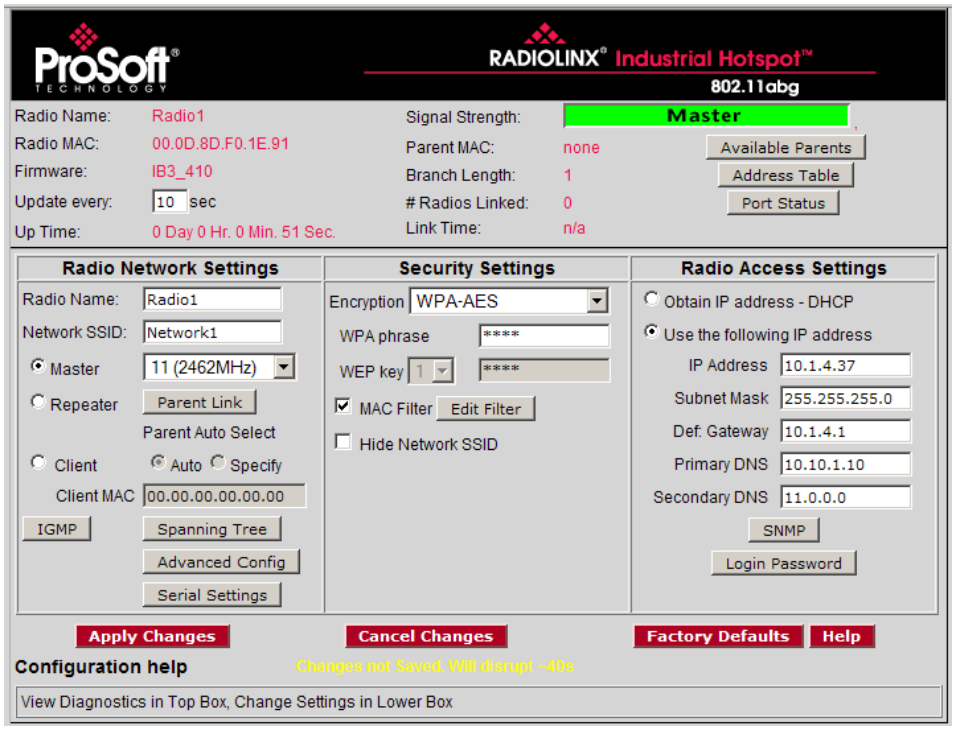

**3** Accept the dynamically assigned address, and then click OK.

For information, see Radio Access settings (page 55).

### 1.6.5 Set Up the Master Radio

To configure the radio, double click on the radio (Radio1) in the IH Browser window. This action opens a web browser (for example Microsoft Internet Explorer or Firefox) and loads the IH Radio's web configuration interface.


Important: The radio configuration is protected by a login password. The default password for the radio is "password" (lower case, no quotes). To prevent unauthorized access to the radio configuration, you should change the password when you have finished the initial configuration.
Note: The master is the "root" or top-level radio in a network. You must have at least one master radio per network. For redundancy, you can assign more than one master to a network.




To configure a Master radio, make the following changes to the web configuration form:

*Radio Network Settings*

- **Radio Name:** Enter a unique name for the radio.
- Select **Master** as the radio mode.
- **Network SSID:** Assign a network name (SSID) of up to 32 characters. The radio uses this name in all network references. All radios in a network must have the same SSID.
- **Channel:** Select a channel and frequency range for the network or accept the default value. Network channels allow radios to avoid sharing a frequency with other networks in the same location. The channel list indicates the channel number as well as the frequency (2.4 gHz or 5 gHz).

Important: The RLXIB-IHW-66 radio is supplied with a dual-band antenna that supports both frequency ranges. If you use a different antenna with the IHW radio, you must choose a channel and frequency range supported by the antenna.

*Security Settings*

- **Encryption Type:** Encryption scrambles data so that only intended viewers can decipher and understand it. Although "none" is an available encryption type, ProSoft Technology strongly recommends encrypting all data sent and received from every radio on your network, to help prevent your data from being intercepted and decoded.
- **WPA phrase:** To use WPA encryption on packets sent between the radios, select WPA in the Encryption Type field. Next, in the WPA phrase field, enter a pass phrase of between eight and 63 normal keyboard characters. This phrase automatically generates an encryption key of 128 hexadecimal characters. The default pass phrase is "passphrase" (lower case, no quotes). For more information on encryption, see Security settings (page 52).

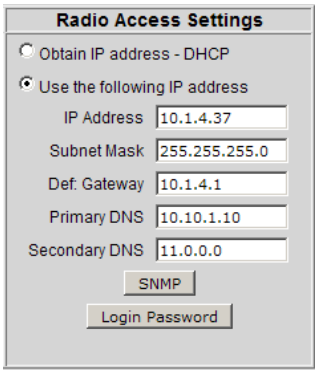
Because you must assign the same Network SSID and WPA phrase to the repeater radios later in this procedure, you should write down the settings.

Note: Network SSID and WPA phrase are both case-sensitive.

Network SSID:_____

WPA phrase:_____

*Radio Access Settings*




If a DHCP (Dynamic Host Control Protocol) server is configured on your local area network, the DHCP server can assign IP addresses automatically.

If you prefer to assign a Static (Fixed) IP address, select "Use the following IP address", and then enter the IP Address, Subnet Mask and Default Gateway in the Radio Access Settings area of the IH Radio web configuration form.

Important: If you intend to assign IP addresses manually, you must not duplicate an IP address that is already in use on your network. If you are not sure what IP addresses are available, ask your network administrator for assistance.

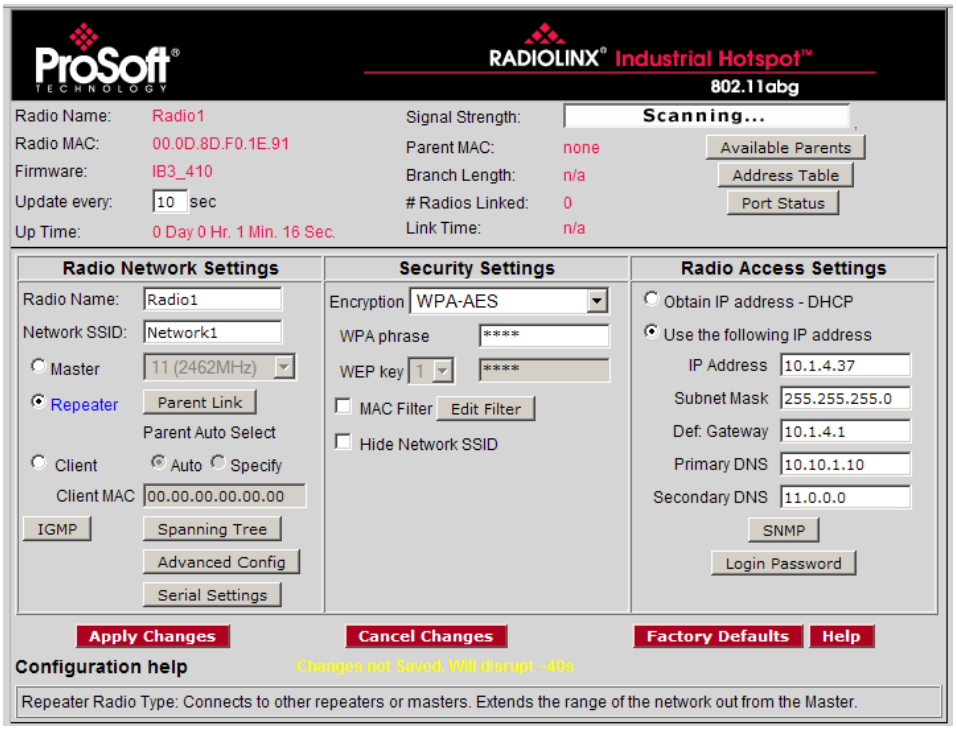
### 1.6.6 Save the Radio Configuration

Before closing the Radio Configuration window, you must apply your changes. Click Apply Changes to save your configuration and restart the radio.

Note: To discard your changes and start over, click Cancel Changes.

### *1.6.7 Set Up a Repeater*

To configure a radio as a Repeater, make the following changes to the web configuration form:




*Radio Network Settings*

- **Radio Name:** Enter a unique name for the radio.
- Select **Repeater** as the radio mode.
- **Network SSID:** Enter the SSID you configured for the Master radio. All radios in a network must have the same SSID.

*Security Settings*

- **Encryption Type:** Encryption scrambles data so that only intended viewers can decipher and understand it. Choose the same encryption type you configured for the Master radio.
- **WPA phrase:** Enter the pass phrase you configured for the Master radio.

Important: The Network SSID and WPA phrase are case sensitive. Use *exactly* the same combination of upper case and lower case letters you entered for the Master radio, otherwise the Repeater radio will not be able to connect to the Master radio.

By default, a repeater connects automatically to the best available parent radio on the network. If necessary, however, you can click the Parent Link button and specify how repeater radios connect to the network. See Parent Link settings (page 42) for information.

### *1.6.8 Set Up a Client*

Client mode is a special mode in the radio that allows a user to connect an Ethernet device to a wireless network through any 802.11a, b or g access point. Any Ethernet device that has an RJ45 Ethernet port can, in effect, be transformed into an 802.11a, b or g wireless client by attaching the radio. Only a single device can be connected to the radio in client mode. Do not connect to more than one Ethernet device (using a switch or hub).

You only use client mode if you need to connect to another brand 802.11a, b or g access point. If you are using RLXIB-IHW radios, you should always use them as repeaters (and masters).

To connect a device to a radio in client mode, click the Client button for the radio and try programming the radio's client mode using the Auto setting. To test whether the Auto setting will work:

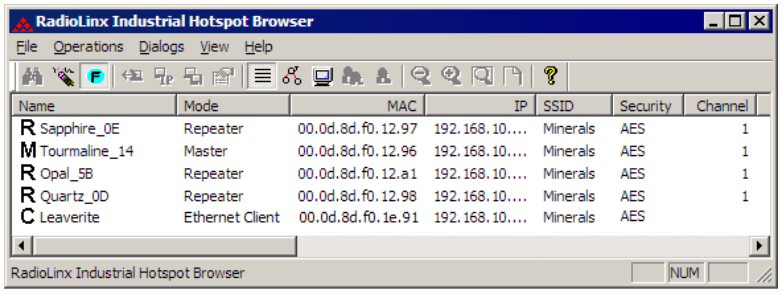
1. Connect the cable between the device and the radio.
2. Turn ON the radio power, or cycle the power if the radio is already on.
3. Turn ON the device. Watch the radio to see if it initializes. The Auto setting will work if the device advertises its MAC ID to the radio.

If the radio's RF LEDs do not show consistent activity after a few minutes, then you may need to modify the radio's client settings. Click the Specify radio button, determine the MAC ID of the Ethernet device, and type the ID into the Client MAC field.

Client radios are preceded by a 'C' in the list of radios in the RLX-IH Browser.

## 1.7 Verify Communication

When configured, the name of each radio is preceded by an M (for Master), an R (for Repeater), or a C (for Client) in the IH Browser window.




Look at the LEDs to ensure good link quality, as explained in LED display. After a repeater is configured, you can unplug the Ethernet cable from it.

# 2 Installing the Radios

*In This Chapter*

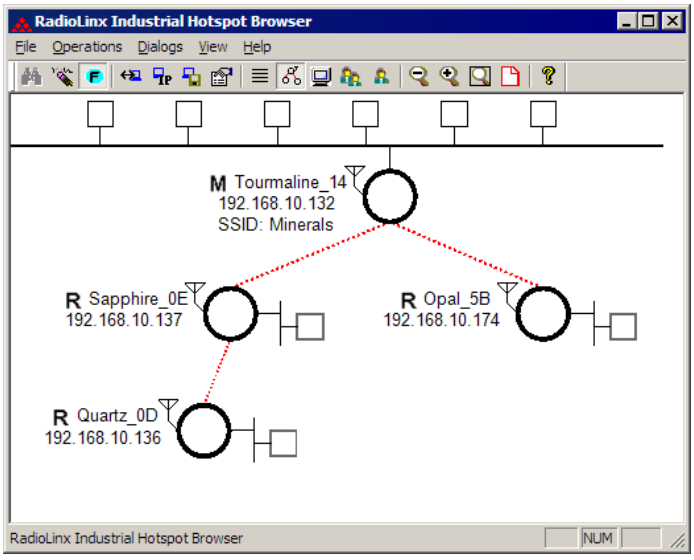


If possible, you should configure all the radios side by side in an office setting and make sure they link before you install them in the field. If feasible, it would be even better if you could set up the entire system in the office and make sure your equipment communicates properly through the radio network.

Important: If the radios are close enough to each other that their received signal strength is greater than -40dBm, performance may be degraded. Disconnect antennas from radios during bench testing, or move the radios further apart from each other.
Tip: To make it easier to physically identify the radios you are configuring, apply a label to each radio indicating the radio name and IP address.

After you have configured each radio using IH Browser and the web configuration form, you can install the radios and test their performance. Install the radios in their proposed permanent locations, then temporarily place each radio's antenna near its proposed mounting location. The temporary placement of the antenna can be by hand; however, with this testing method, one person must hold the antenna while another monitors the radio's signal strength.

To see how a radio is linked in the network, make sure that the radio is connected to a PC, and then select Topology View from the View menu in the RLX-IH Browser.



The Topology view shows a diagram of the network's wireless connections. Use this view to see whether all the radios are linked, and that you approve of the way the radios are linked. A radio that is not linked to a parent will show as a circle outlined by a flashing dashed red line. It may be near the bottom of the window, so scroll down to view all available radios. To change how radios link to the network, see Parent Link settings (page 42).

Refer to Improve Signal Quality (page 29) for more information on overcoming poor connectivity.

## 2.1 Connecting antennas

Each radio must have an antenna connected to the Main antenna port on the RLXIB-IHW-66 radio; without an antenna for each radio, the network will not function.

All antennas for radios that communicate directly with each other should be mounted so they have the same polarization. Antennas with an N-jack connector can be mounted directly to the radio using an N-plug to N-plug adapter. Screw the antenna onto the antenna port connector until it is snug.

For remote placement of antennas an extension cable with N-plugs can be used. Because the antenna cable attenuates the RF signal, use an antenna cable length that is no longer than necessary to ensure optimum performance.

# 3 Diagnostics and Troubleshooting

*In This Chapter*



Use the program's diagnostic and signal strength settings at the top of the Radio Settings window to make sure the network is working properly.

- **Signal Strength graph:** This setting graphically shows the radio's signal strength. The graph will show the word Master if a master radio is selected. The graph will show the word Scanning if the radio is scanning to find another radio to which to connect. If the radio is not connected to a network and not currently scanning, the graph will show the words Not connected.
- **Update readings every:** If you want to update the diagnostic readings according to a particular interval, specify the interval (in seconds) in this field.
- **Read-only fields** that appear with the diagnostic settings.

You can perform the following troubleshooting routines:

- Check the Ethernet cable (page 26)
- Retrieve the default password

For more troubleshooting information, go to the ProSoft Technology web site at http://www.prosoft-technology.com

## 3.1 Diagnostics

The Radio Configuration / Diagnostic Utility (the web configuration form for the radio) provides information that can help you troubleshoot problems with the radio.

Use the program's diagnostic and signal strength settings at the top of the Radio Settings window to make sure the network is working properly.

**Signal Strength graph:** This setting graphically shows the radio's signal strength.

- The graph will show the word **Master** if a master radio is selected.
- The graph will show the word **Scanning** if the radio is scanning to find another radio to which to connect.
- If the radio is not connected to a network and not currently scanning, the graph will show the words **Not connected.**

**Update every**: If you want to update the diagnostic readings according to a particular time interval, specify the interval (in seconds) in this field. After entering the new value, press Enter only if you want to save the new value; press Tab or click elsewhere to use the new value temporarily.

The following configuration forms in the Radio Configuration / Diagnostic Utility provide information about current radio operation:

- Address table (page 37)
- Port status (page 38)
- Available Parents
- Read-only fields (page 35)

The following topics describe troubleshooting routines:

- Check the Ethernet cable (page 26)
- Retrieve the default password
- Troubleshoot RLX-IH Browser error messages (page 28)
- Troubleshoot missing radios in the RLX-IH Browser (page 29)

For more troubleshooting information, visit the ProSoft web site at http://www.prosoft-technology.com

## 3.2 Check the Ethernet cable

If you connect a radio and the Ethernet LED does not light on the radio, you may have used the wrong cable type. In other words, you may have used a cross-over cable when you should have used a straight-through cable, or vice versa.

Use a straight-through cable when connecting the radio to an Ethernet hub or a 10/100 Base-T Ethernet switch. Straight-through cables are used in most cases.

Use a cross-over cable when connecting the Ethernet radio directly to any device that is NOT a switch or a hub (e.g., a direct connection to a PC, PLC, or printer).

## 3.3 LED display

The RLXIB-IHW-66 front panel includes a set of LEDs that indicate the radio's status:

| LED | Description |
|---|---|
| Power/Status | This green LED indicates that the radio has power. |
| RF Transmit | This yellow LED indicates RF transmission. |
| RF Receive | This green LED indicates RF reception. |
| Ethernet | If this green LED is lit, the Ethernet cable is connected. If this LED is flashing, an Ethernet packet is being transmitted or received. |
| Signal Strength | If only one of these three LEDs is lit, then the radio is linked. If two LEDs are lit, the radio's signal strength is fair. If all three LEDs are lit, the signal strength is good. |

If a radio is configured as a master, the middle light of the three Signal Strength LEDs will always be on, and the bottom Signal Strength LED will always be off. The top LED on the master will flash if any radios are linked to this master.

After you first plug in the power cable and Ethernet cable to the radio, the Power/Status LED should be green, meaning that the radio has power. If the Ethernet LED is green, then the Ethernet connection is working. The RF Transmit and RF Receive LEDs should blink.

All three LEDs will blink just after the radio links to the Master's signal but before it has been fully authenticated. Normally you will see this last only a few seconds. If it lasts longer or never turns solid it usually means the encryption keys are not correct.

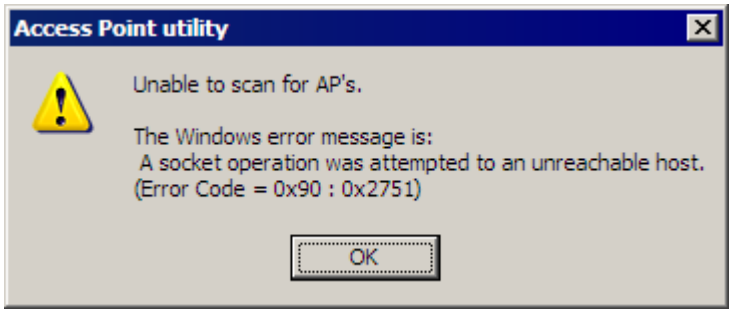
## 3.4 Retrieve the default password

If you forget your password, you will be unable to retrieve your password to change the radio settings. You can reset the default password to use the software again, but you will lose all the settings you programmed before. To reset the default password and return the radio to its default settings, follow these steps:

1. Hold down the reset switch by pressing down on the diamond shape above the word RADIOLINX and apply power to the radio. Continue holding down the reset switch for approximately 10 seconds until the radio initializes.
2. The radio will be reset to its default settings, including the password. You should now be able to log in using the default password, which is "password".

## 3.5 Troubleshoot RLX-IH Browser error messages

One error message commonly occurs when you use the RLX-IH Browser. You can easily remedy this error, which is shown in the following illustration:




This error occurs when the RLX-IH Browser attempts to scan for radios and no valid network connection exists on the PC, wired or wireless.

To correct this error, Confirm that your PC has at least one active network (LAN) connection; it could be a wired Ethernet connection or a wireless 802.11 connection. One way to determine if your network connections are active is to look in the system tray in the lower-right corner of your desktop. The two-PC icon indicates a connection and the icon with a red X indicates an inactive connection. If no connections are visible in the system tray, check Network Connections in the Control Panel.


Confirm that the network connection has a valid IP address. Your network connection might need to have a static IP address assigned to it. Check the IP address of your network connection to determine that one has been assigned.

## 3.6 Troubleshoot missing radios

If radios are not visible in the RLX-IH Browser, try the following:

- First, click the Scan button again. Scans are sent as broadcast messages, which can be dropped in RF connections, requiring the user to scan again.
- Second, make sure that the firewall is not activated on your PC. (This is most common in Windows XP). Open the Network connections folder in your Windows Control Panel, then open the Local Area Connection Properties window and verify that the check box under Internet Connection Firewall is not checked.
- If the preceding approaches do not help, the PC running the RLX-IH Browser and the radios are probably not connected to the same local network. Verify your connections.
- If you are in topological view, any unlinked radios may be at the bottom of the window. Scroll down to see all radios. If you still cannot see radios with the RLX-IH Browser, call technical support.

## 3.7 Improve signal quality

If you need to improve a radio's signal quality, try the following steps:

- Adjust the direction of the high-gain antennas.
- Increase the height of the antenna's placement.
- Use higher-gain antennas or external preamplifiers.
- Select a new location for the radio and/or its antenna.
- Decrease the length of the antenna cable.
- Determine and resolve sources of interfering electrical noise.
- Add a repeater between radios that are not communicating.

# 4 Radio Configuration / Diagnostic Utility

*In This Chapter*



The RadioLinx Industrial Hotspot radio has a built-in Radio Configuration / Diagnostic Utility (radio web configuration form) that allows you to configure the radio from any computer that can connect to the radio, through a wired Ethernet connection, or through a Wireless connection.

You can use a web browser such as Microsoft Internet Explorer or Firefox on your network-enabled desktop computer, laptop or Personal Data Assistant (PDA) to monitor and change the settings within the RadioLinx Industrial Hotspot radio.

*To open the Radio Configuration / Diagnostic Utility*

1. In the RadioLinx Industrial Hotspot Browser, select the radio to configure from the list view or topography view, and then click the right mouse button to open a shortcut menu.
2. On the shortcut menu, choose Connect. The Radio Configuration / Diagnostic Utility will open in your web browser.

   Or,
   Double-click the selected radio to launch the Radio Configuration / Diagnostic Utility.

You can also open the Radio Configuration / Diagnostic Utility directly from your web browser.

**Important:** Your desktop computer, laptop, or PDA must be connected to the same network as the RadioLinx Industrial Hotspot radio.

1. Open your web browser.
2. In the address bar, type "`http://`", followed by the IP address for the radio, and then click the "Go" button. For example,

```
http://192.168.6.10
```

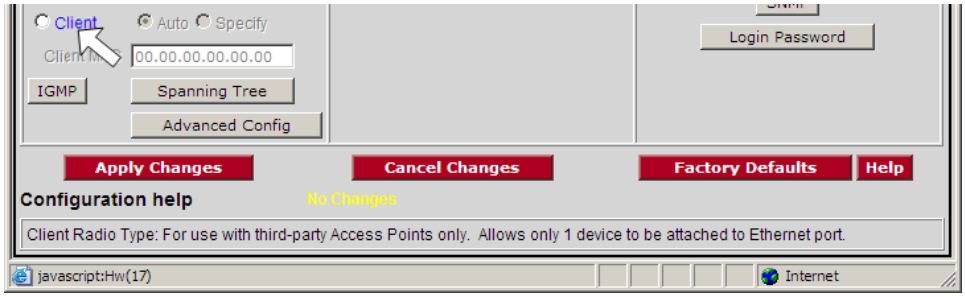
### Read-Only fields

Some of the fields on the Radio Configuration / Diagnostic Utility form are read-only, meaning that the content of the field is provided for information only, and cannot be directly modified. Notice also that depending on the way the radio is configured, some fields and buttons may be unavailable because they do not affect the configuration you have selected. Review the topics in this section for more information on when and how to use each configuration option.

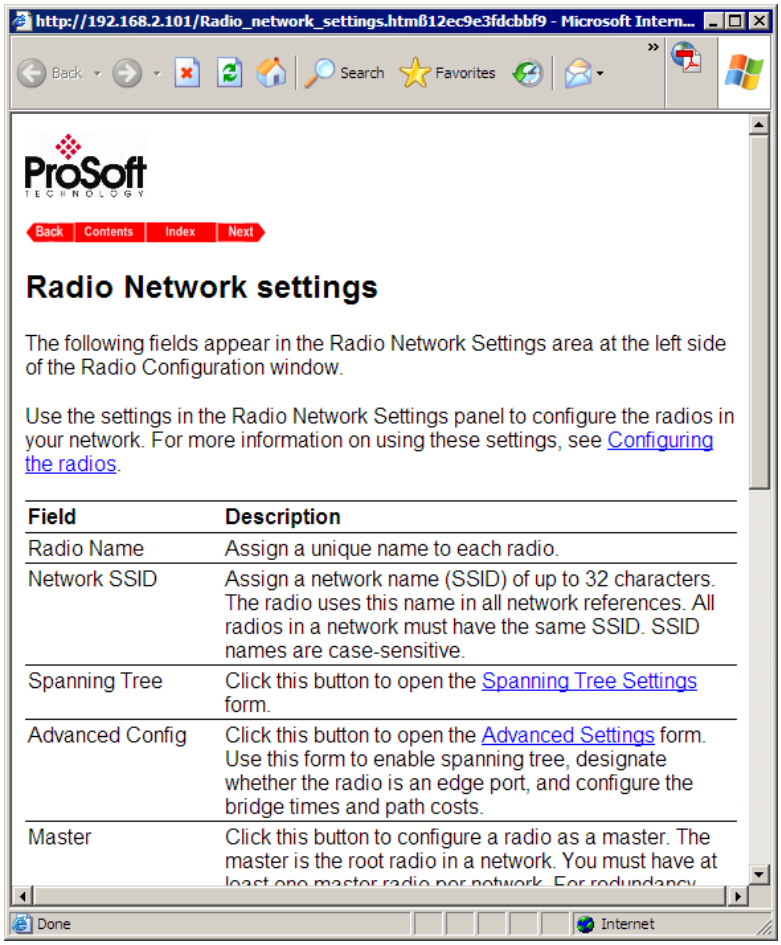
### Configuration Help

Help is available for each item in the Radio Configuration / Diagnostic Utility.

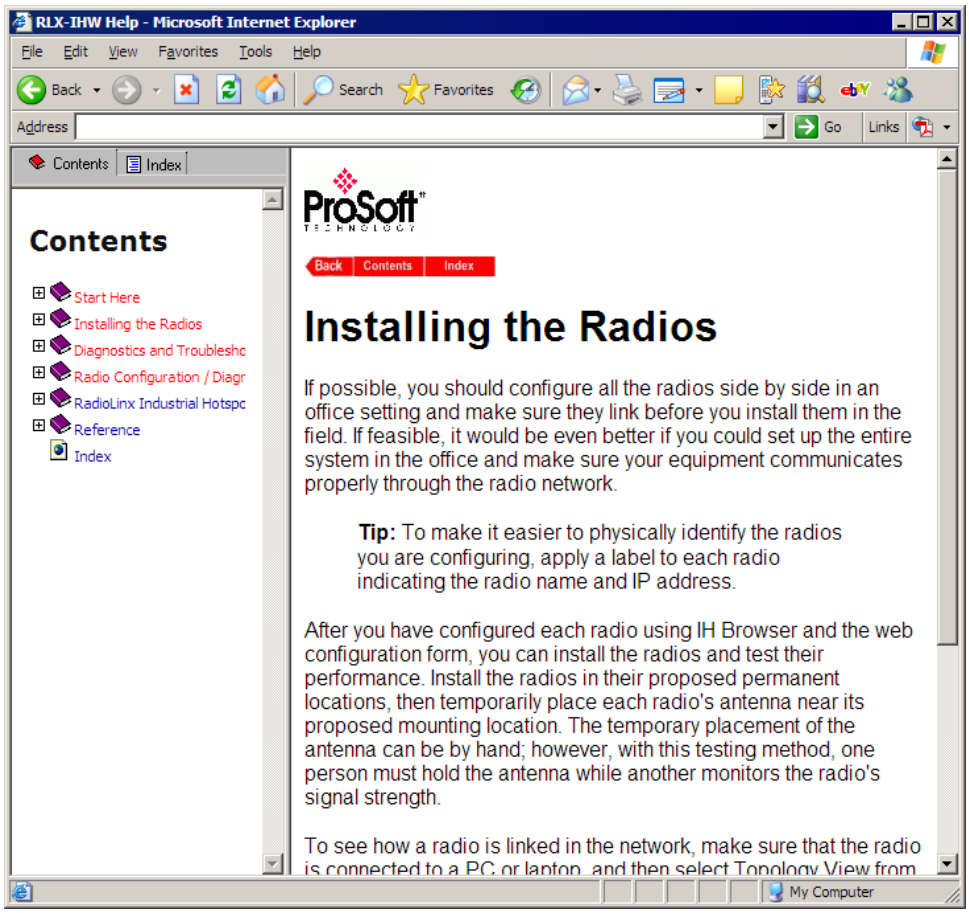
- To view a brief help message about any field on the screen, move your mouse pointer over the field, or use the **[Tab]** key, and refer to the text that appears at the bottom of the screen.



- To view more help about the selected field, click the field name. This action opens a help page in a new browser window.

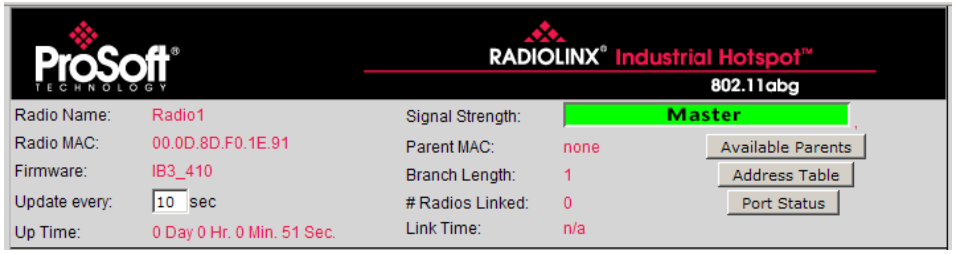


- To view the complete online documentation for your RLXIB Radio, click the Help button. This action opens the online documentation in a new browser window. Use the Contents, Index and Search tabs in the left frame to navigate the help system.



## 4.1 Radio Status

The following fields appear in the status area at the top of the Radio Configuration window.




Note: Different versions of the RLXIB Radios support different functionality. You may see more or fewer options on this page, depending on the version of the radio you purchased.

Use the settings in the Radio Status panel to view the current settings for this radio.

| Field | Description |
|---|---|
| Radio Name | The name of the selected radio. |
| Radio MAC | The MAC address of the selected radio. The MAC ID is also printed on the side of the radio. |
| Firmware | The version of firmware currently installed. All radios on the network must have the same firmware versions installed. For more information on firmware versions, refer to Update firmware (page 64). |
| Update every | This value in seconds controls how often the web configuration form automatically refreshes. To change the value temporarily, enter the new value and press the [Tab] key. To change the value permanently, enter the new value and press the [Enter] key. |
| Up Time | The length of time the radio has operated since the last system power-up or last system reset. |
| Signal Strength | Strength of the signal from the Parent radio. |
| Parent MAC | The MAC address of the parent radio to which the selected radio is linked. |
| Branch Length | The number of RF links from the radio to the master radio. |
| # Radios Linked | The number of other radios that are linked to this radio. |
| Link Time | The length of time the radio has been continuously connected to a parent radio. |
| Available Parents | Click this button to view the list of Access Points (Parents) from which this radio can detect beacons. This button is only available when the radio type is Repeater. |
| Address Table | Click this button to view a list of MAC addresses for devices entered in the radio's address table. |
| Port Status | Click this button to view spanning tree status of each switch port, for RF ports and the RJ45 (Ethernet) port. |

### 4.1.1 Available Parents

This page opens when you click the Available Parents button on the Radio Configuration Form.

Note: This form is not available when the radio type is Master.

**Available Access Points** Radio1 Only Show Same SSID: ☐ **Refresh**

00.0D.8D.F0.12.AF Network1 Radio1 *Click on column header to sort*

| MAC ID | SSID | Channel | RSSI | Security | Speed | Cost | Age(s) | Hops |
|---|---|---|---|---|---|---|---|---|
| 02:00:e1:8f:ab:e0 | PAIR_2 | 10 | -88 | none | b | 602 | 11 | na |
| 02:00:49:1e:59:49 | TestIBSS1 | 10 | -80 | none | b | 430 | 1 | na |
| 02:00:56:a6:46:f1 | TestIBSS1 | 10 | -80 | none | b | 430 | 6 | na |
| 02:00:54:92:44:c5 | TestIBSS1 | 10 | -80 | none | b | 430 | 18 | na |
| 02:00:54:26:44:71 | TestIBSS1 | 10 | -80 | none | b | 430 | 28 | na |
| 8e:bb:79:21:bb:a1 | WANetwork | 10 | -80 | none | g | 430 | 0 | na |
| 02:00:53:82:43:d5 | TestIBSS1 | 10 | -79 | none | b | 411 | 40 | na |
| 02:00:6e:36:7e:61 | TestIBSS1 | 10 | -79 | none | b | 411 | 63 | na |
| 02:00:46:32:56:65 | TestIBSS1 | 10 | -78 | none | b | 394 | 52 | na |
| 02:00:65:7f:4e:e1 | TestWAEIP | 10 | -78 | none | b | 394 | 0 | na |
| 02:00:6c:77:79:1c | PAIR_1 | 1 | -77 | none | b | 376 | 4 | na |
| 02:00:54:f2:44:a5 | TestIBSS1 | 10 | -74 | none | b | 329 | 74 | na |

This page is helpful for viewing:

- Possible parents for a repeater. The current parent should normally be the radio with the lowest cost and a matching SSID.
- Other 802.11 networks in the area.

| Field | Description |
|---|---|
| Only Show Same SSID | Select (check) this box to restrict the list of available parents to those with the same SSID as the radio you are configuring. |
| Refresh | Click this button to re-scan the network and update the devices in the list. |
| Mac ID | A unique hexadecimal number that identifies any Ethernet device. |
| SSID | Network Name (Service Set Identifier). |
| Channel | The radio channel on which the device is transmitting. The channel list indicates the channel number as well as the frequency (2.4 gHz or 5 gHz).<br><br>Important: The RadioLinx RLXIB radio is supplied with a dual-band antenna that supports both frequency ranges. If you use a different antenna with the RLXIB radio, you must choose a channel and frequency range supported by the antenna. |
| RSSI | Received Signal Strength Indication. |
| Security | The encryption type enabled for the device. |
| Speed | The IEEE 802.11 connection speed (a, b, or g). The RadioLinx RLXIB radio supports all three 802.11 connection speeds. |
| Cost | Parent selection cost. |
| Age | The length of time (in seconds) since the radio last saw a packet from this MAC address |
| Hops | The number of hops to the Master. A value of 0 (zero) is shown for non-ProSoft devices. |

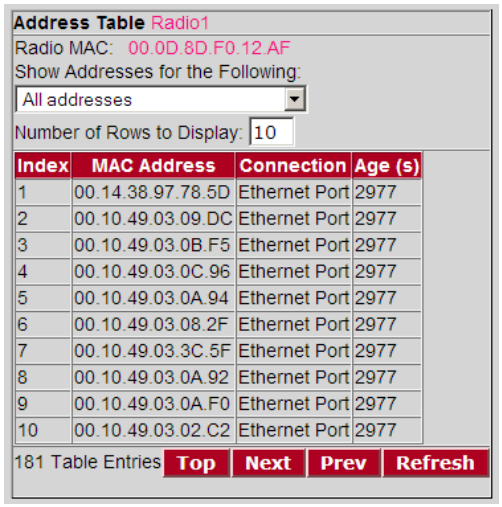
This list contains both 802.11 devices that are part of the same SSID as the RLXIB itself (for example, "Minerals") as well as devices that belong to different SSIDs (for example, "Network1" and "ProSoftInternal"). This list is updated continuously and can be used for many purposes.

The IH radio updates this list with each 802.11 packet that is received, whether from a radio of the same network or one that belongs to another SSID. It can also see radios from other vendors.

Once per second the IH radio evaluates the link it has to its parent to determine if this link is the best parent to use. A cost is calculated for each entry and can be seen in the column labeled "Cost" in the preceding table. The cost calculation is based not only on the strongest signal, but on several other factors to provide optimum network communication.

### *4.1.2 Address table*

This configuration page opens when you click the Address Table button on the Radio Configuration form.



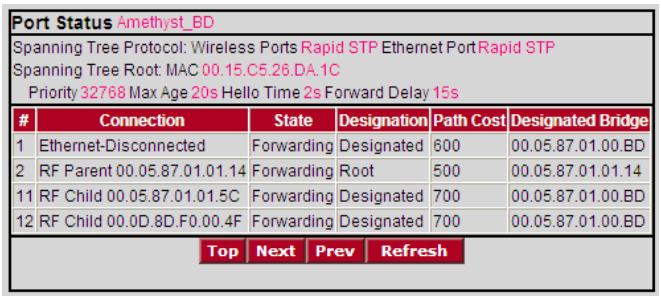

The Address Table shows the port through which each MAC address is connected, along with the age in seconds since the radio last saw a packet from this MAC address.

| Field | Description |
|---|---|
| Radio MAC | The MAC address of the selected radio. The MAC ID is also printed on the side of the radio. |
| Show Addresses for the Following | Use this dropdown list to filter the address list. Options are:<br>▪ Devices Out Ethernet Port<br>▪ Directly Linked Radios/Clients<br>▪ Devices beyond Direct RF Links<br>When the table is filtered to show only Directly linked radios/clients, an additional RSSI column is listed, showing the Received Signal Strength from each radio or client linked to the radio. |

| Field | Description |
|---|---|
| Number of Rows to Display | Use this field to choose how many MAC addresses to display on this page. Use the Next and Prev buttons to scroll through the available MAC addresses. |
| Index | Position in the list. Each page shows up to 10 devices. Use the Next and Previous buttons to move up and down through the table. |
| MAC Address | The MAC address for the device. |
| Connection | The connection type |
| Age (s) | The length of time (in seconds) since the radio last saw a packet from this MAC address |
| Top | Click the Top button to see the top of the table. The radio will display updated data in the table entries. |
| Next / Prev | If the table has more MAC addresses than it can display in the window, use the Next and Prev buttons to move up and down through the table. |
| Refresh | Click Refresh to update the table. |

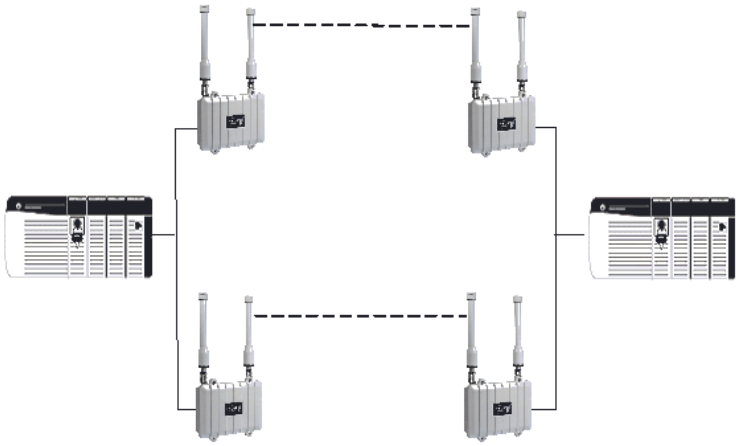
### *4.1.3 Port status*

This configuration page opens when you click the Port Status button on the Radio Configuration form.




When you click the Port Status button, you can see information about all the active ports on the radio. Above the table, you can see information about the current Spanning Tree (page 49), including the MAC address of the "root" device, and the timing parameters that are set for the current Spanning Tree. Each radio can have up to 34 active ports—one Ethernet cable, one parent RF link, and up to 32 child RF links.

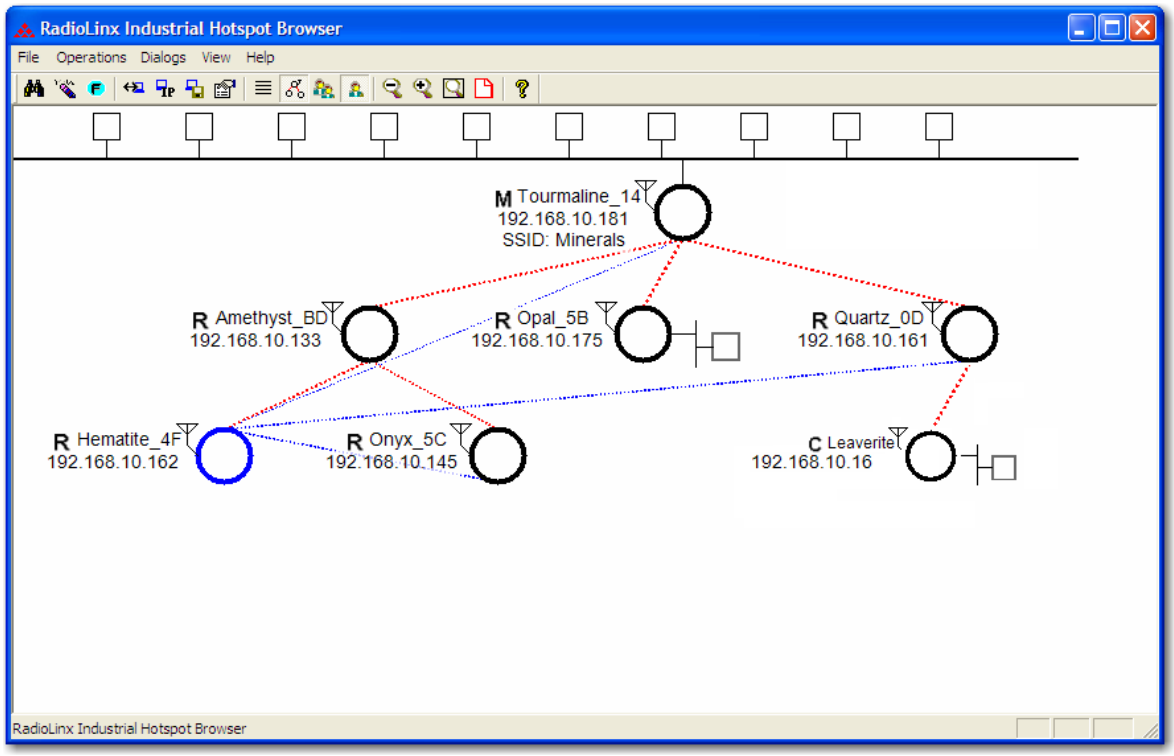
The primary reason for creating a Spanning Tree is that it allows you to create fully redundant paths. If any single radio in a redundant path loses its connection, another path still exists, and the connection will be updated and communication restored.



| Field | Description |
|---|---|
| Spanning Tree Protocol: Wireless Ports | The Spanning Tree Protocol level for the wireless port. (Rapid STP or STP). |
| Ethernet Port | The Spanning Tree Protocol level for the Ethernet port. (Rapid STP or STP). |
| Spanning Tree Root MAC | The MAC ID of the root device in the spanning tree. |
| Priority | The Spanning Tree device with the lowest-priority value is elected the root of the tree |
| Max Age | The length of time a port can stay enabled without any new spanning updates. |
| Hello Time | The length of time between the transmission of spanning update packets. |
| Forward Delay | The length of time a port must listen for spanning information before being activated. |
| # | Position in the list. Each page shows up to 10 ports. Use the Next and Previous buttons to move up and down through the table. |
| Connection | This field indicates what the port represents: Ethernet, a parent radio, or a child radio. |
| State | The current Spanning Tree state of the port. Possible states are Blocking, Learning, Listening, and Forwarding. Forwarding packets can be transferred. |
| Designation | The Spanning Tree designation for the branch off the port. Possible designations are Root (ports going to the root), Designated (ports going to a branch), or Normal. |
| Path Cost | The cumulative cost of all wired and wireless links from the port to the Spanning Tree root. |
| Designated Bridge | The next bridge toward the Spanning Tree root for this port. |
| Top | Click the Top button to see the top of the table. |
| Next / Prev | If the table has more ports than it can display in the window, use the Next and Prev buttons to move up and down through the table. |
| Refresh | Click Refresh to update the table. |

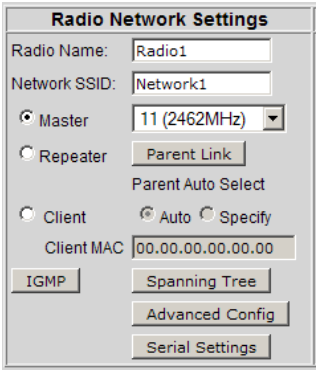
The following illustration shows the RadioLinx Industrial Hotspot Browser (page 59) application provided with the radios. Notice it shows the radio named Hermatite_4F, linked to Amethyst_BD. This link is shown with a red dotted line. Also visible is the level of redundancy in their network. Each of the blue lines represents an alternate parent. From this view, you can easily tell how much redundancy exists in their network.

To display the redundant paths, select the toolbar button denoting two "parents." To view the redundancy on a per-radio basis, select the single "parent" button, and then click on the radio to view its available redundancies.



## 4.2 Radio Network settings

The following fields appear in the Radio Network Settings area at the left side of the Radio Configuration window.




Note: Different versions of the RLXIB Radios support different functionality. You may see more or fewer options on this page, depending on the version of the radio you purchased.

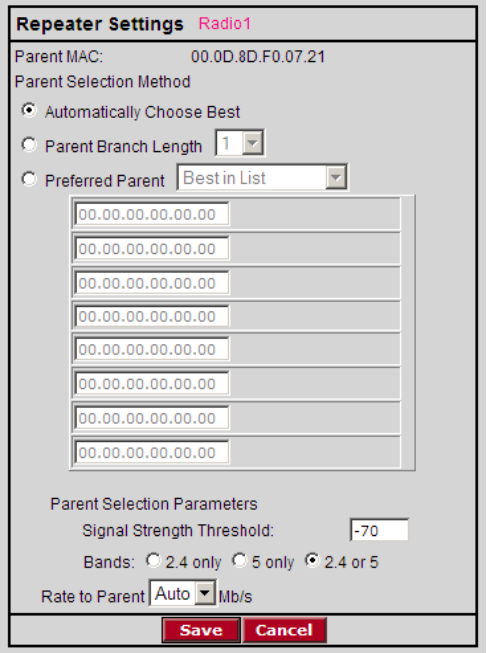
Use the settings in the Radio Network Settings panel to configure the radios in your network. For more information on using these settings, see Configuring the radios.

| Field | Description |
|---|---|
| Radio Name | Assign a unique name to each radio. |
| Network SSID | Assign a network name (SSID) of up to 32 characters. The radio uses this name in all network references. All radios in a network must have the same SSID. SSID names are case-sensitive. |
| Master | Click this button to configure a radio as a master. The master is the root radio in a network. You must have at least one master radio per network. For redundancy, you can assign more than one master to a network. For information, see Redundancy, |
| Channel list (master radio) | The channel list indicates the channel number as well as the frequency (2.4 gHz or 5 gHz).<br>**Important:** The RLXIB-IHW-66 radio is supplied with a dual-band antenna that supports both frequency ranges. If you use a different antenna with the IHW radio, you must choose a channel and frequency range supported by the antenna. |
| Repeater | Click this button to configure a radio as a repeater. The repeater mode is the normal radio mode for the network, while the master mode is more of a special setting to establish the network channel and define the root of the network tree. Repeater radios help extend the range of a network and help create the signal "bridges" that allow networked radios to communicate. All RLXIB-IHW-66 radios are capable of repeating. |
| Parent Link settings | Click this button to specify how a repeater radio connects to the network. For information, see Parent Link settings. |
| Client | This is a special mode that allows you to connect an Ethernet device to any 802.11 a, b or g access point. You would only use this mode in the special event that you wanted to connect a device to another brand access point. For information on setting up a client, see Configuring clients. |

| Field | Description |
|---|---|
| Auto / Specify | Only choose "specify" if device does not send out any unsolicited Ethernet packets. Try Auto first. |
| Client MAC | The MAC ID of the device connected to the radio, only if the device does not advertise its MAC address. |
| IGMP | Click this button to open the IGMP Settings form. Use this form to enable (default) or disable IGMP, and to configure how the RLXIB-IHW-66 radio will be have when IGMP is enabled. |
| Spanning Tree | Click this button to open the Spanning Tree Settings form. |
| Advanced Config | Click this button to open the Advanced Settings form. |
| Serial Settings | Click this button to open the Serial Settings form. |

### *4.2.1 Parent Link Settings*

This configuration page opens when you click the Parent Link button on the Radio Configuration form.

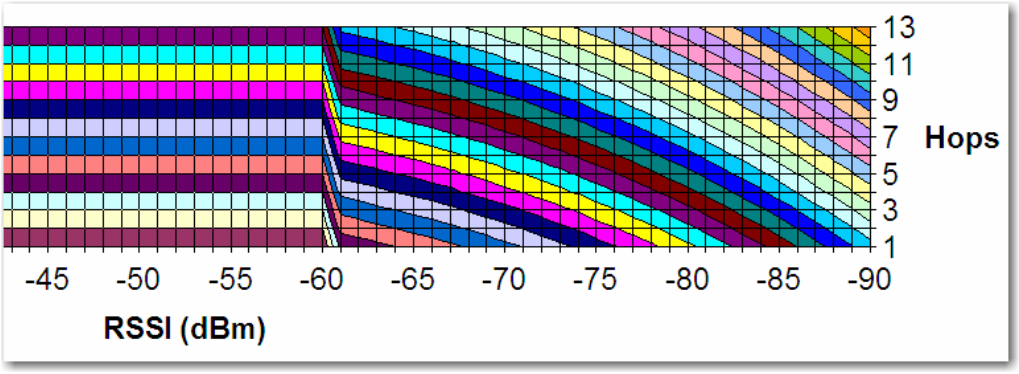



| Field | Description |
|---|---|
| Parent MAC | The MAC Address of the radio's Parent node. |
| **Parent Selection Method** | |
| Automatically Choose Best | The Automatic Parent Selection algorithm uses a calculation to create a cost for each possible parent radio that it detects.<br>In the calculation the radio includes,<br>▪ RSSI - Stronger signals receive a better cost.<br>▪ Hop Count - Fewer hops from the Master radio is given preference and therefore a lower cost<br>Choose this setting to allow the radio to determine the best parent to select. |

| Field | Description |
|---|---|
| Parent Branch Length | With the branch length setting the IH will choose its parent strictly by the number of repeaters between it and the Master radio. If Branch Length of 1 is chosen, the IH will link only to the Master radio. If Branch Length of 2 is chosen, the IH will link only to an IH that is linked to the Master radio, and so on. |
| Preferred Parent | With the preferred parent setting the IH radio will select its parent from a list of possible parents specified by the user. The user can list up to eight radios to choose from.<br>▪ Best in List<br>When Best in List is selected the IH will select its parent using the "Automatic Parent Selection" algorithm, but it will limit the selection to the list of radios in the list. Therefore, the radio in the list with the lowest cost according to the algorithm will be chosen as its parent.<br>▪ Follow List Priority<br>When Follow List Priority is chosen the IH will select its parent from the list giving preference to the 1st entry followed by the 2nd entry and so on. |
| **Parent Selection Parameters** | |
| Signal Strength Threshold | When the signal from a parent reaches a high enough value, a stronger signal will not improve the quality of the link any further. For signals that are above that threshold, only fewer hops from the Master give preference. You can adjust that threshold here. |
| Bands | This setting controls which bands a Repeater will scan to look for a possible parent. It will scan the 2.4GHz band only, the 5GHz band only, or both 2.4GHz and 5GHz bands. |
| Rate to Parent | The default setting is auto which allows the radio to select the best rate to use to the parent radio, and adapt over time. You might specify a fixed rate rather than auto for example if the link to the parent has a low signal strength in which case fixing a lower rate can improve performance. The actual rate used between this radio and its parent is the lower value of this setting and the Max Data Rate setting in the parent (see Max Data Rate). So use these two controls in conjunction if desired to tailor the rate of each parent link. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

When you save a selection and return to the Radio Network Settings panel, notice that your selection is indicated under the Parent Link button.

The Automatic Parent Selection algorithm uses a calculation to create a cost for each possible parent radio that it detects. The following graph describes how the cost is calculated when the signal strength threshold is set to -60 dBm.

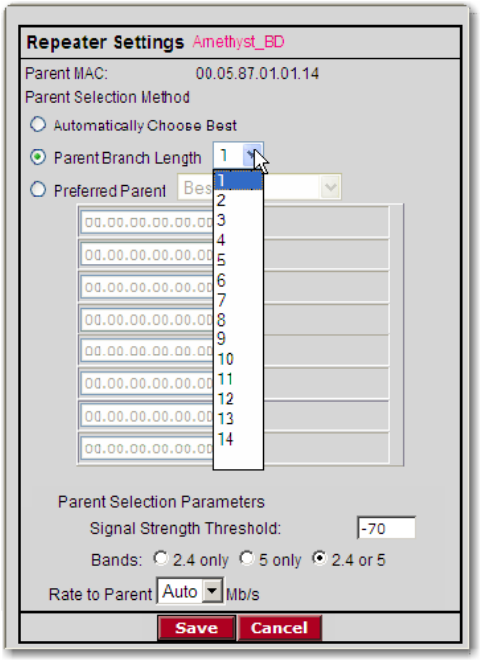


Once per second the RLXIB radio evaluates the link it has to its parent to determine if this link is the best parent to use. A cost is calculated for each entry and can be seen in the column labeled "Cost" in the preceding table. The cost calculation is based not only on the strongest signal, but on several other factors to provide optimum network communication.

### *Prioritized Parent Selection*

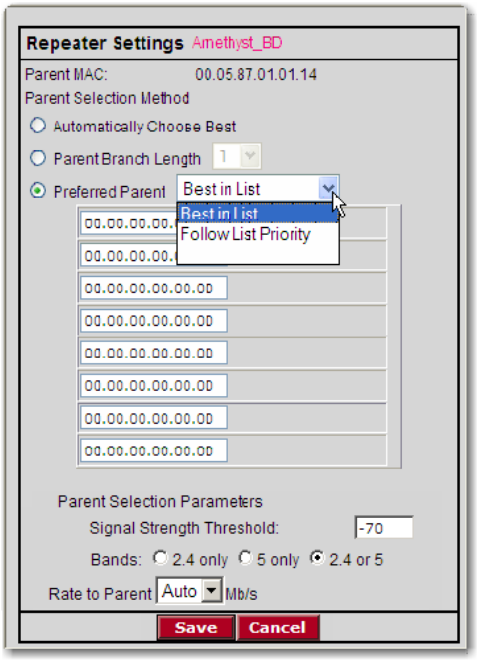
If you need more control than the automatic algorithm allows, you can also define a priority list of parents for the IH Radio to choose.

Prioritized Parent by Branch Length




With **Parent Branch Length,** the IH will choose its parent strictly by the number of repeaters between it and the Master radio. If Branch Length of 1 is chosen, the IH will link only to the Master radio. If Branch Length of 2 is chosen, the IH will link only to an IH that is linked to the Master radio, and so on.

Prioritized Parent by Preferred Parent List




With **Preferred Parent,** the IH radio will select its parent from a list of possible parents that you specify. You can list up to eight radios to choose from.

- **Best in List**

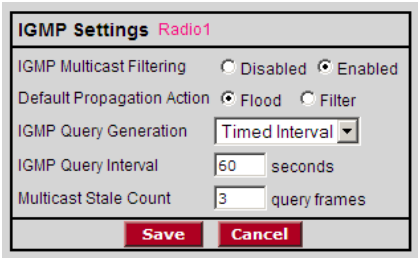
  The IH will select its parent using the "Automatic Parent Selection" algorithm described above but it will limit the selection to the radios in the list. The radio in the list with the lowest cost according to the algorithm will be chosen as its parent.

- **Follow List Priority**

  The IH will select its parent from the list giving preference to the first entry, followed by the second entry, and so on.

### 4.2.2 IGMP Settings

This configuration page opens when you click the IGMP button on the Radio Configuration form.




RLXIB radios support IGMP v1 and v2. The default operation of the RLXIB radios is to have IGMP functionality enabled, although the user can disable IGMP entirely. Additionally, the user can specify settings associated with IGMP filtering and snooping. Unknown multicast addresses can be sent to all ports (flood) or to none (filtered) by changing the IGMP Multicast Filtering option. The user can specify whether or not the radio will generate IGMP queries, and configure the query interval time.

By RFC specification, only one device on a network should generate IGMP queries. As such, RLXIB radios will only send a query if another device has not sent a query within its Query Interval setting, even if Query Generation is enabled.

| Field | Description |
|---|---|
| IGMP Multicast Filtering | Disabling filtering will cause the radio flood multicast packets to all ports. |
| Default Propagation Action | Determines how to handle multicast addresses that are not in the radio's address table. |
| IGMP Query Generation | Enables or disables query generation from this radio. |
| IGMP Query Interval | Number of seconds between queries (if not pre-emptied by another devices queries). |
| Multicast State Count | Number of queries generated before a device is removed from the multicast group on this radio if no response is received. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

### 4.2.3 Rapid Spanning Tree Functionality

The software's built-in Rapid Spanning Tree (RSTP) functionality enables you to set up full redundancy between radios or other devices. Spanning Tree shuts off ports as necessary to prevent loops. If loops are created in an Ethernet network, packets can be circulated endlessly, consuming all the bandwidth and making the network unusable.

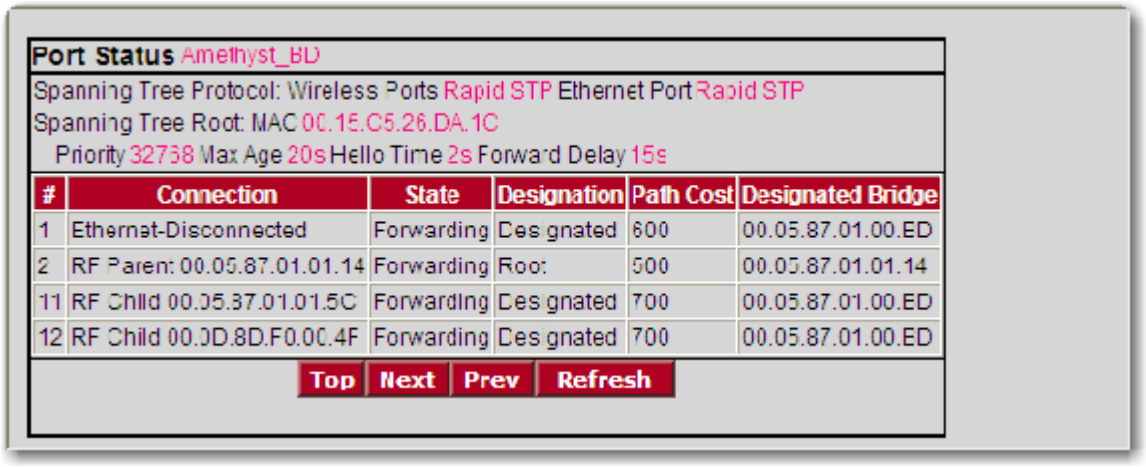
RSTP allows users to create truly redundant connections between any two points in the network. The radios detect the redundant paths and keep one connection alive for communications. If the primary connection fails for any reason, the secondary connection is quickly transitioned to a state to forward packets, allowing the network to adapt itself to handle problems without customer intervention.

RSTP uses active communications between network devices to propagate changes in the network and to cause transitions to occur much more quickly. Because RSTP is an IEEE standard, IH radios work in conjunction with wired Ethernet switches to form a redundant network.

Each RSTP device (RLXIB Radio or Ethernet switch) communicates with other RSTP devices in the network via packets called Bridge Protocol Data Units (BPDUs). BPDUs are sent out each of the devices ports. In a wired switch this would be from each of the Ethernet ports. In an RLXIB Radio, in addition to the Ethernet port, each wireless link is considered a port. These BPDUs are the communications means to allow each RSTP device in the network to make sure that the proper connections still exist.

In the following illustration, this RLXIB Radio has 4 RSTP "ports":

- Ethernet port (1)
- A port for its parent connection (2)
- A port for each of its two child connections (11 and 12).



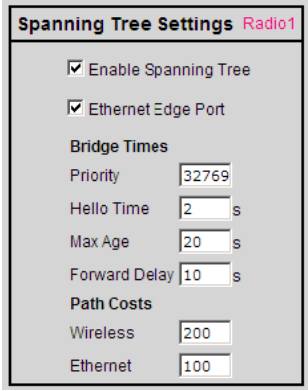
BPDUs are sent out the port at a rate called the "Hello Time". The accepted standard value for this is 2 seconds. If a radio (or any other RSTP device) does not get a BPDU for 2 Hello Times, it assumes the RSTP device that had been there is no longer available. It can then open an alternate path if one is available. This process is much like the STP process. If other devices on the network are not operating in rapid spanning tree mode, the radio will revert to normal spanning tree operation on a per-port basis.

RSTP provides a performance enhancement over STP operation. By comparison, the radio using the STP algorithm would revert its port to the listening state, and then to the learning state, before returning to the forwarding state. Each of these states takes at least 15 seconds, during which the STP devices are listening for BPDUs to re-negotiate the network topology. The advantage of using the RSTP functionality is that is uses active handshaking between adjacent RSTP devices to re-negotiate the network topology. This process takes one to two seconds.

Each RLXIB Radio contains a switch table, which tells it how to forward Ethernet packets to get them to their proper destination. When the network topology changes, the RLXIB Radio flushes its Ethernet switch table immediately. This allows it to pass traffic immediately over the new network topology and learn the configuration in the process. Until the learning is complete, the packets are broadcast to their destination. As each packet is seen and the switch table rebuilds, the radios return to directing packets to their destinations.

### 4.2.4 Spanning Tree Settings

This configuration page opens when you click the Spanning Tree button on the Radio Configuration form.




| Field | Description |
|---|---|
| Enable Spanning Tree | Spanning Tree is enabled when this box is checked. Without spanning tree, redundant connections might exist if multiple radio links are created in parallel with each other. Redundant connections are blocked only if spanning tree is enabled. Additionally, spanning tree is used to flush the Ethernet switch table when the network topology changes as described in the section on Automatic Parent Selection. Firmware versions 2.5xx and above for RLX-IH, and all versions of RLXIB radios also support Rapid Spanning Tree (RSTP), and will default to this mode when enabled.<br>The recommended setting for spanning tree is "Enabled". |
| Ethernet Edge Port | Because RSTP is an active protocol, it depends on communication between RSTP devices. If no RSTP device is connected to the radio's Ethernet port, the handshake cannot take place. In this case RSTP reverts to STP. This means that the Ethernet port will be forced to adhere to the timer based transition protocol of STP.<br>Therefore on network transitions and power up, communications will not be allowed over the Ethernet port for 30 to 45 seconds. This setting is an indication that no redundant connections exist out this port and communication can immediately be allowed. If for some reason a BPDU is received on this port, the RSTP protocol will negotiate properly and handle any possible redundant paths.<br>The recommended setting for Ethernet Edge Port is "Enabled". |
| **Bridge Times** | The values in this list configure the timing intervals to use. |
| Priority | This setting determines who should be the root of the RSTP. The RSTP device with the lowest priority becomes the root. The accepted standard value for this is 32768. If wired switches exist in the network that support RSTP, they should always be allowed to be the root.<br>Set this value to 32769 to prevent the radio from being the root over a wired switch. Use this setting when a radio is configured to be a Master.<br>Set this value to 32770 when the radio is configured to be a Repeater. In this way, if only IHs exist in the network, the Master radio will become the root. |

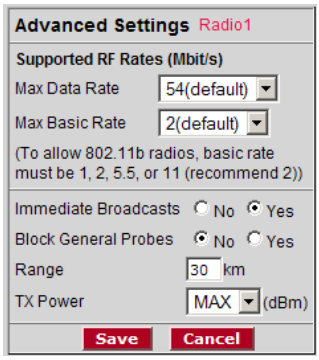
| Field | Description |
|---|---|
| Hello Time | The rate at which BPDUs are sent out. The industry standard is 2 seconds. |
| Max Age | Measures the age of the received protocol information recorded for a port and ensures that this information is discarded when its age limit exceeds the value to the maximum age parameter recorded by the switch. The timeout value for this timer is the maximum age parameter of the switches. |
| Forward Delay | Monitors the time spent by a port in the learning and listening states. The timeout value is the forward delay parameter of the switches. |
| **Path Costs** | The RSTP and STP algorithms use a cost to determine which connections should be used. The "spanning tree" is formed by determining the least cost paths from any RSTP device back to the root. |
| Wireless | To give preference to a wired connection, set the Wireless cost to 200. |
| Ethernet | To give preference to a wired Ethernet connection, set the Ethernet cost to 100. |

You can define multiple master radios on the same network. Then, if one master radio goes down, any radios linked to it can switch over to the other master, so the networked radios remain connected and transmitting. In order to be redundant, the two masters should typically be on the same segment—in other words, they should be wired together into the same switch. These two masters can be assigned different channels to increase network bandwidth, but they must be assigned the same SSID.

Also, because all radios are repeaters, you can set up each radio to be able to reach a master radio via multiple repeater paths. Then, if a repeater goes down, the linked radios can use a different path to get back to a master radio.

### *4.2.5 Advanced Settings*

This configuration page opens when you click the Advanced Configuration button on the Radio Configuration form.



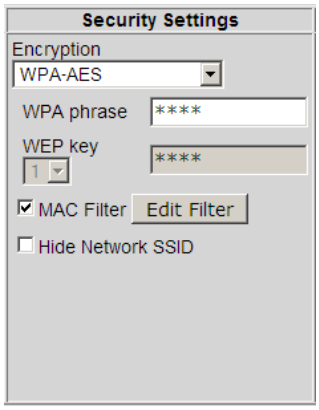
It is important to allow many industrial protocols to communicate properly over the RLXIB radios. The standard 802.11 AP operation for transmitting broadcast messages is to accumulate them and transmit them only on specific time intervals. This allows clients that are in power-save mode to wake up at the synchronized time interval and receive the broadcast packets. However, the power-save mode is rarely used in industrial networks. Additionally, many industrial protocols utilize multicast traffic, which is sent as broadcast messages over the wireless network. By enabling immediate broadcasting, these multicast messages are not delayed by the wait for the next time interval to occur before they can be transmitted. This results in improved network performance.

The settings on this form also allow you to configure the transmission rate and broadcast mode to optimize this radio's use on an industrial network.

| Field | Description |
|---|---|
| Max Data Rate | The maximum data transmission rate, in megabits per second, for this radio. Available settings range from 1 to 54. |
| Max Basic Rate | In addition to the Data Rate setting which controls generic data traffic, the Basic Rate setting adjusts the rate at which control packets such as Beacons and Acks are sent at as well as packets that need to go to the whole network such as Broadcasts. Because these packets are intended for the whole network, the Max Basic Rate setting of the Master is advertised to each of the radios in the network through Beacons. Each radio, other than the Master, then inherits the Max Basic Rate setting of the Master. Therefore the setting only needs to be made in the Master radio. The setting in each of the other radios is disregarded. |
| Immediate Broadcasting | Forward multicast traffic immediately, rather than waiting for specific time intervals. |
| Block General Probe Requests | Do not respond to general probe requests that are not specific to the radio's SSID. |
| Range | The Range setting allows the radios to account for round trip delays. The Range settings should be the same in all radios in the network and should be at least large enough to account for the length of any links. However, increasing the Range beyond what is necessary can cause a slight decrease in throughput. |
| TX Power | This sets the output power of the radio. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

## 4.3 Security settings

The following fields appear in the Security Settings area in the middle of the Radio Configuration window.




Note: Different versions of the RLXIB Radios support different functionality. You may see more or fewer options on this page, depending on the version of the radio you purchased.

You can assign the following security settings:

| Field | Description |
|---|---|
| Encryption type (page 53) | WPA-AES is the preferred encryption method. It contains the latest updates to the 802.11 standards for best security. However, some legacy devices do not yet support these updates. Therefore, you can choose combinations of legacy methods.<br>Available encryption types are:<br>▪ None (not recommended)<br>▪ WPA-AES - Latest security setting using WPA (pre-shared key) authentication and AES encryption.<br>▪ WPA-TKIP - Security setting using WPA (pre-shared key) authentication and TKIP encryption.<br>▪ WEP128 - Legacy security setting using a 128-bit key and WEP encryption.<br>▪ WEP64 - Legacy security setting using a 64-bit key and WEP encryption. |
| WPA phrase (page 53) | Enter a WPA pass phrase of between eight and 63 normal keyboard characters. |
| WEP key (page 53) | Enter five normal text characters in the WEP key field |
| MAC Filter (page 54) | Check (select) this field to restrict connections by MAC address. |
| Edit Filter | Opens the MAC filter (page 54) form, allowing you to specify the MAC addresses of devices to allow in the network. |
| Hide Network SSID (page 55) | Hides the Network SSID (Network Name) from other 802.11 users. You can still connect clients to the "hidden" network by typing the Network SSID. |

The following topics describe each security setting in more detail.

### 4.3.1 Encryption type

The preferred encryption type is WPA (WiFi Protected Access). You should only select WEP (wired equivalency protocol) for use with an older client radio that only has WEP encryption. For compatibility with clients that do not support WPA, you can select WPA+WEP128 (bits) or WPA+WEP64 (bits) as the encryption type. Then the older clients can connect to an access point using the WEP setting, but new clients will use WPA and the RLXIB radios will still use WPA among themselves.

IMPORTANT: If WPA+WEP is selected, some clients using WPA might not be able to connect unless you use a WEP key other than number 1, due to limitations in these clients. In such cases, you should set a WEP key other than key 1 and set this same key in all clients that are using WEP. See WEP key (page 53).

WEP is the original security protocol used by 802.11 networks, but WPA offers better protection against attacks, for several reasons: WPA distances the encryption key from the actual data by performing several algorithms to the key before generating the encrypted data, it performs dynamic key management by changing keys frequently, and it performs message integrity checks to prevent forgery and replay.

You can also select WEP 128, WEP 64, or None (no encryption) as the encryption type, but none of these settings are recommended.

Note: If an RLXIB is set to use WPA+WEP, it will connect to other radios set to WPA only or WPA+WEP, but it will not communicate with radios set to WEP only. Likewise, an RLXIB in client mode with WPA+WEP selected will not connect to an access point with WEP only selected.

### 4.3.2 WPA phrase

To use WPA encryption on packets sent between the radios, enter a WPA pass phrase of between eight and 63 normal keyboard characters. This phrase automatically generates an encryption key of 128 hexadecimal characters. This field is only available if you select WPA as the encryption type.

The default WPA-AES Phrase when a module ships is 'passphrase'.

### 4.3.3 WEP key

A key is a set of hexadecimal (hex) or ASCII characters used to encrypt data. This field is only available if you select WEP as the encryption type. Write down your WEP encryption key as you create it, because you must enter the same key on your client.

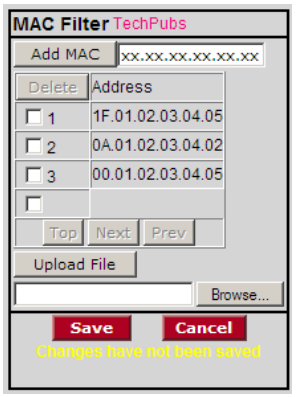
To create a 64-bit WEP key, enter five normal text characters in the WEP key field, which converts the characters automatically to 10 hex digits. Alternatively, you can enter 10 hex digits (0 to 9, a to f, A to F) directly in the WEP key field. To create a 128-bit key, enter 13 normal text characters, which convert to 26 hex digits, or enter 26 hex digits (0 to 9, a to f, A to F) directly.

Note: Clients often support more than one WEP key. Packets received can be decrypted using any one of the keys if programmed, but packets are always transmitted with the "default" WEP key number. If you set a transmit key number on the RLXIB, make sure all other radios and clients have this key programmed. To set keys other than key 1 on some clients using Windows, you might have to use the Advanced settings.

Programming more than one key on the RLXIB requires setting the key number to the key you want to program, entering the key, and saving your changes. Repeat these steps for each key you want to program, saving after each one; finally, change to the desired transmit key number if necessary and save again. (If "****" remains in the key field, the previously programmed key will not be changed when changes are applied.)

### 4.3.4 MAC filter

This configuration page opens when you click the Edit Filter button on the Radio Configuration form.



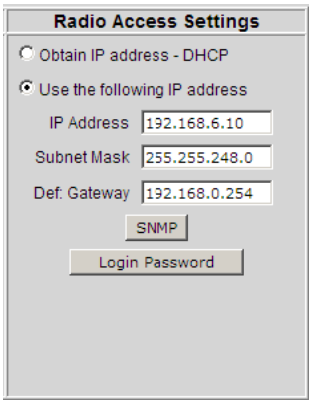

| Field | Description |
|---|---|
| Add MAC | Enter the MAC address to add. The address will appear in the list after you click the Add MAC button. |
| Delete | Click this button to delete the selected MAC address from the list. |
| Address | This list contains all the MAC addresses you have added. |
| Top | Click the Top button to see the top of the list. |
| Next / Prev | Click the Next and Prev buttons to move up and down through the address list. |
| Upload File | To assign the same list of MAC addresses to several radios conveniently, open a text editor such as Notepad.exe. Enter addresses in hexadecimal format, one MAC address per line, including periods. When you finish, save the document. In the MAC Filter window, click Browse to select the text file, then click Upload File to upload the list of MAC addresses. |
| Browse | Click Browse to navigate to a prepared text file of MAC addresses on the appropriate drive and folder, and click the Upload File button. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

### 4.3.5 Hide Network SSID

If you want your radio network to be hidden from other 802.11 users, click the Hide Network SSID check box in each radio you want hidden. With the SSID hidden, your network does not show up when other clients scan for an access point. You can still connect clients to the "hidden" network by typing the Network SSID.

## 4.4 Radio access settings

The following fields appear in the Security Settings area on the right side of the Radio Configuration window.




Note: Different versions of the RLXIB Radios support different functionality. You may see more or fewer options on this page, depending on the version of the radio you purchased.

In order to configure or diagnose a radio using its built-in Web server or SNMP agent, both your computer and the radio must have IP addresses, and these IP addresses must be on the same subnetwork. An IP address is only needed so you can configure the radio and view its diagnostic settings. Otherwise, the address is unnecessary.

| Field | Description |
|---|---|
| Obtain IP address - DHCP | Select this option to allow the radio to obtain its IP address from a DHCP server. |
| Use the following IP address | Select this option to specify a Static IP address to the radio. Enter the IP address information in the following fields. |
| IP Address | Enter an IP address that will not interfere with any other devices on the network. Request a block of IP addresses you can use from your Network Administrator. |
| Subnet Mask | Enter the Subnet Mask provided by your Network Administrator. |
| Default Gateway | Enter the Default Gateway address provided by your Network Administrator. |
| Primary DNS | Enter the Primary DNS address provided by your Network Administrator. |
| Secondary DNS | Enter the Secondary DNS address provided by your Network Administrator. |

| Field | Description |
|---|---|
| SNMP button | Click this button to open the SNMP (Simple Network Management Protocol) Agent settings form. Use this form to configure access to radio network settings through an SNMP agent. |
| Login Password button | Click this button to change the Login Password for the radio. The default password is "password". You should change this password, and keep a record of it in a safe place, to protect the radio from being reconfigured by unauthorized users. |

DHCP (Dynamic Host Control Protocol) is a service provided by a server (typically a router or a firewall) on a local area network. Devices on a network that supports DHCP can request and receive an IP address from the DHCP server. RLXIB radios support DHCP; by default, they attempt to obtain an IP address from a DHCP server.

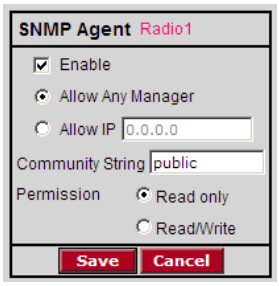
If a DHCP server is not available, the radio will not be able to acquire an IP address automatically, therefore you must assign an IP address, subnet mask and default gateway to the radio so that it can communicate on the network.

You can also assign a Static (fixed or permanent) IP address to the radio to make it easier to identify and configure the radio. Static IP addresses are particularly useful when configuring radios to serve as Access Points, or for radios that must be accessible through a firewall.

A detailed discussion of TCP/IP networking is beyond the scope of this manual. Refer to the following Microsoft knowledgebase article for more information: http://support.microsoft.com/kb/164015

### *4.4.1 SNMP Agent settings*

This configuration page opens when you click the SNMP button on the Radio Configuration form.




SNMP is a network management protocol that is often used with TCP/IP and Ethernet. As an alternative to using the Radio Configuration / Diagnostic Utility, you can change radio settings and view diagnostics in an SNMP manager application, if necessary.

| Field | Description |
|---|---|
| Enable | Click this button to enable the following SNMP Agent settings. |
| Allow Any Manager | Select this option to allow any user to change the radio settings from any computer using SNMP. |

| Field | Description |
|---|---|
| Allow IP | Select this setting to restrict access to an SNMP manager with a particular IP address, then enter the IP address in the Allow IP field. |
| Community String | Enter a "community string" (essentially a password) that a manager must use to access the radio's SNMP agent. |
| Permission | Select the permission level to assign to this radio. |
| Read only | An SNMP Agent can view but cannot modify radio settings. |
| Read/Write | An SNMP Agent can view and modify radio settings. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

The RLXIB SNMP agent supports SNMP protocol version 1.4 and 2 MIBs:

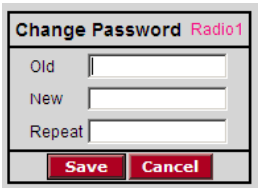
RFC12133-MIB (partial; internet.mgmt.MIB-2.system, .interfaces, .snmp)

ROMAP-MIB (included on the CD; internet.private.enterprises.romap)

It also supports a selection of standard SNMP traps, including Cold Start, which is sent when the radio initializes.

### 4.4.2 Change password

This configuration page opens when you click the Login Password button on the Radio Configuration form.



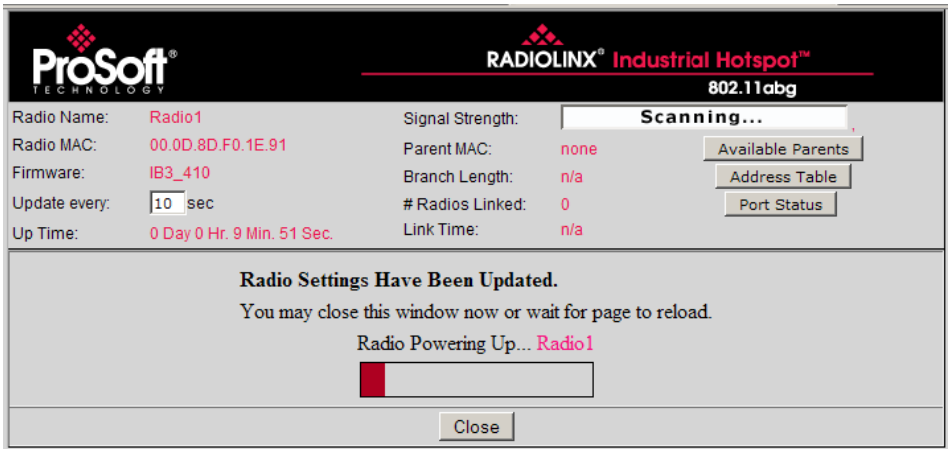

| Field | Description |
|---|---|
| Old | Enter the current password in this field. The default password is "password" (lower case, no quotes). This entry must exactly match the current password, otherwise the change will be rejected. |
| New | Enter the new password in this field. Passwords are case sensitive. |
| Repeat | Confirm the new password in this field. This entry must exactly match the password you entered in the "New" field, otherwise the change will be rejected. |
| Save | Saves your changes and updates the radio configuration. |
| Cancel | Discards your changes without updating the radio configuration. |

You can enter any alphanumeric value between one and 31 characters. The password is case-sensitive.

If you forget your password, you will be unable to change the radio settings. To get the default password again, see Troubleshooting.

## 4.5 Apply Changes

Click the Apply Changes button to save your changes after editing radio configuration in order for those changes to take effect. When you apply changes, the radio will shut down and restart using the new settings. The following illustration shows the Radio Configuration / Diagnostic Utility as the radio restarts.




## 4.6 Cancel Changes

Click Cancel Changes to discard any settings you made during this session.

Note: This button only applies to changes made in the Radio Configuration / Diagnostic window. Changes made to individual configuration forms (for example, Spanning Tree, Parent Link, and SNMP Agent settings) take effect when you click the Save button on each of those forms.

## 4.7 Factory Defaults

Click the Factory Defaults button to reset the radio to the default settings.

Important: This action discards all your radio configuration settings.

You will be prompted to confirm this action before it takes effect.

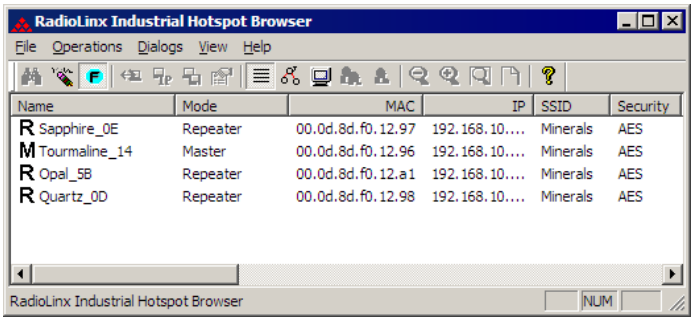
# 5 RadioLinx Industrial Hotspot Browser

*In This Chapter*



The RLX-IH Browser allows you to find any radios connected to your network, see some of their basic settings, and change the IP address so you can access the radio's Web page. For more information, see Primary radio functions (page 60).

When you run the program, the List view (shown in the illustration) appears with a list of any radios on the same network as the computer running the RLX-IH Browser. If you do not see a radio you expect to see, click the Scan (page 61) button in the tool bar or select Scan from the File menu.



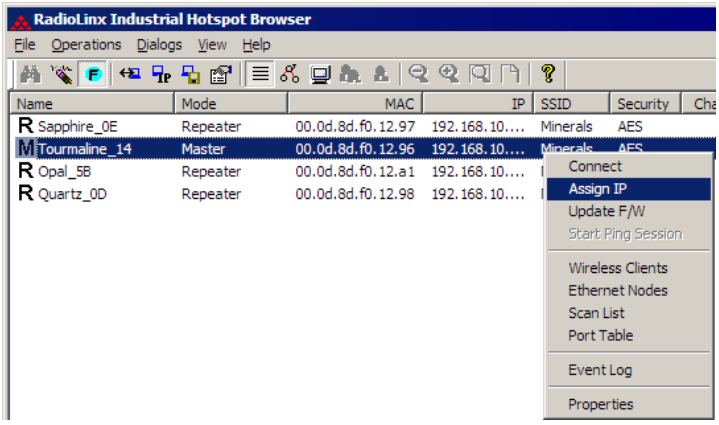

The preceding illustration shows the List View. Refer to Topology view to see alternate views.

To clear all the radios from the list, click the Erase button in the tool bar or select Clear from the File menu. You can then refresh the list by clicking Scan.

If you have trouble viewing radios in the RLX-IH Browser, see Troubleshoot missing radios (page 29).

## 5.1 Primary radio functions

You can perform the following primary functions on any radio in the list by right-clicking the radio name.




Connect (page 63): Log in to the Radio Configuration / Diagnostic Utility to configure a radio or check diagnostics.

Assign IP (page 16): Assign a temporary IP address to a radio.

Update Firmware (page 64): Update the version of firmware the radio uses.

Start Ping Session (page 65):

Wireless Clients (page 67): View a list of client radios

Ethernet Nodes (page 68): View a list of wired Ethernet nodes connected to the network

Scan List (page 69): View a list of all the radios detected on the network (including those from other vendors)

Port Table (page 70):

Event Log (page 70):

Properties (page 71): View the selected radio's properties.

In addition, there are more options in the File menu.

- You can print either a list of the radios' properties or a topology view.
- Change how the RLX-IH Browser scans for radios.

## 5.2 File Menu

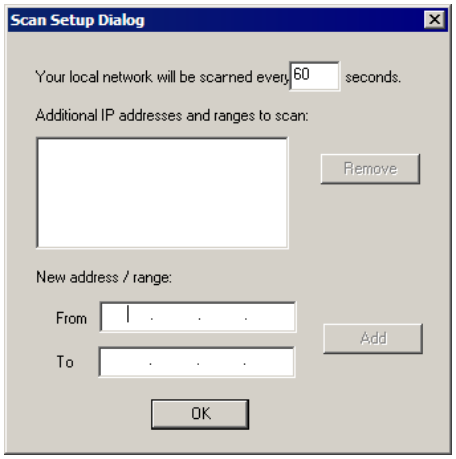
The following commands are available on the File menu:

- Scan Setup (page 61)
- Scan (page 61)
- Clear (page 62)
- Import (page 62)
- Export (page 62)
- Freeze (page 62)
- Print (page 62)
- Print Preview (page 62)
- Print Setup (page 62)
- Exit (page 62)


### 5.2.1 Scan Setup

The Scan Setup command allows you to change some settings that govern how the RLX-IH Browser scans for radios. In the top field of the Scan Setup dialog box, you can adjust how often the program automatically scans for radios. Enter a value (in seconds) to have the RLX-IH Browser scan at that rate.

In the New address/range fields, you can adjust how the program scans for radios. By default, the program sends a broadcast message to all the radios at the same time, looking for a response. Broadcasts are limited to a local network, and will not be passed through a router. If there is a router between the PC running the RLX-IH Browser and the radio to be scanned, the IP address of the radio or a range of addresses can be added to the scan list. At each interval determined by the scan rate, each IP address is individually queried.




### 5.2.2 Scan

The RLX-IH Browser automatically scans for all active radios on the network at a regular interval, but you can use the Scan command in the File menu to look for active radios at any time.

### 5.2.3 Clear

This command clears (deletes) all entries from the IH Browser window.

### 5.2.4 Import

This command imports an XML file created by the Export command in the RadioLinx IH Browser.

### 5.2.5 Export

This command creates and saves an XML file containing the current configuration and status of all radios discovered by the RadioLinx IH Browser. Use this command under the direction of ProSoft Technical Services, for troubleshooting purposes.

### 5.2.6 Freeze

Use this command to temporarily stop the display from updating. This command is useful for studying network topology and performance without the distraction of radios and other devices appearing and disappearing from the screen.

### 5.2.7 Print

Use this command to print the contents of the RadioLinx IH Browser window. Depending on the view you selected, you can print either a list of the radios' properties, or a topology view.

### 5.2.8 Print Preview

Displays a preview of the contents of the RadioLinx IH Browser window. You can use this to adjust the placement of elements so that they do not span page boundaries.

### 5.2.9 Print Setup

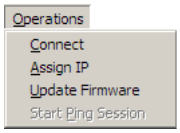
Displays the standard Window Print Setup dialog box.

### 5.2.10 Exit

Closes RadioLinx IH Browser.

## 5.3 Operations Menu

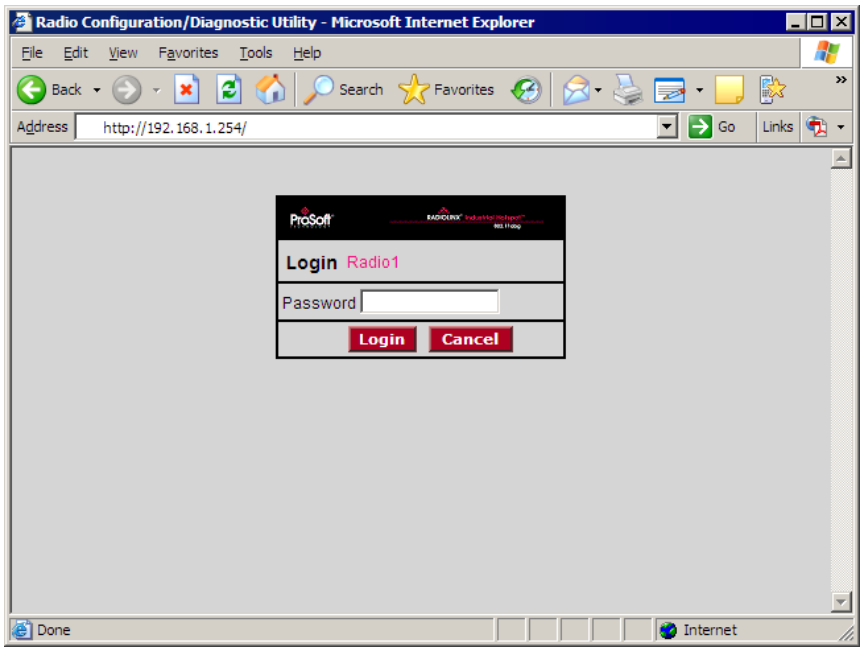
The following commands are available on the Operations Menu:



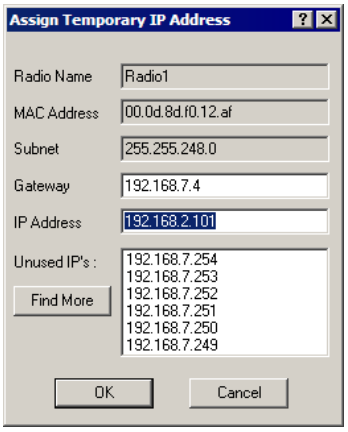

- Connect (page 63)
- Assign IP (page 16)
- Update Firmware (page 64)
- Start Ping Session (page 65)

### *5.3.1 Connect*

To connect to the Radio Configuration / Diagnostic Utility and change radio settings, double-click the radio listing in the RLX-IH Browser after it has been assigned an IP address (either manually or with DHCP). Alternatively, you can select the Connect option in the AP Operations menu. Enter your password to log in to the radio.



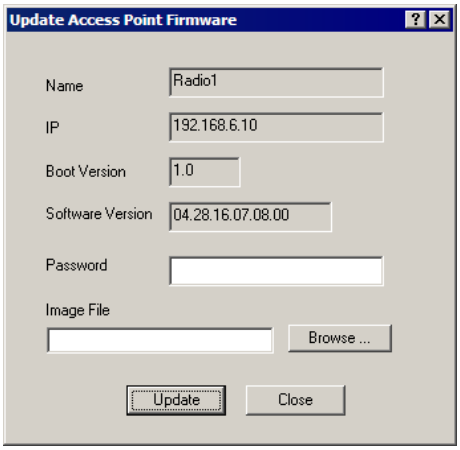
### 5.3.2 Assign IP




If the radio is connected to a network with a DHCP server, the radio may already have an IP address assigned to it. If no address appears, double-click the radio listing in the RLX-IH Browser or select Assign IP in the AP Operations menu. In the next window, click OK to accept the temporary IP address, subnet mask, and default gateway. If necessary, you can enter a particular IP address (see Radio Access settings (page 55)). After an IP address is assigned, you can configure radios through the Radio Configuration / Diagnostic Utility (page 31).

### 5.3.3 Update Firmware

"Firmware" is the program that runs in the Industrial Hotspot that allows it to communicate and exchange data between devices, using the radio as a network connection. Different versions of the firmware communicate with other radios in different ways, and provide different levels of functionality.




In order for your RadioLinx Industrial Hotspot radio to communicate with other RLXIB devices, all radios on the network must use the same firmware version.

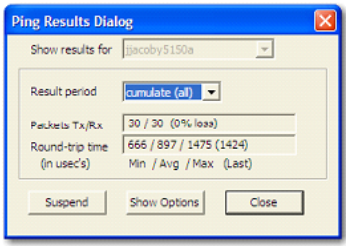
*To change the firmware version of the radio:*

1. Start RadioLinx Industrial Hotspot Browser.
2. Open the Operations menu, and then choose Update Firmware.
3. Enter the password for the radio. This is the same password you use to log into the radio from the Radio Configuration / Diagnostic Utility (page 31).
4. Click the Browse button to locate the Image File (firmware version) to update. Both versions of firmware are available both on the CD that came with in the box with the radio, and at our web site at http://www.prosoft-technology.com
5. Click Update to begin copying the new firmware to the radio. Do not disconnect the cable or turn off power to the radio during this operation.

### 5.3.4 Start Ping Session

A Ping Session allows you to run traffic over the radio network between any two computers running the IH Browser. With it the user can monitor their network over time.

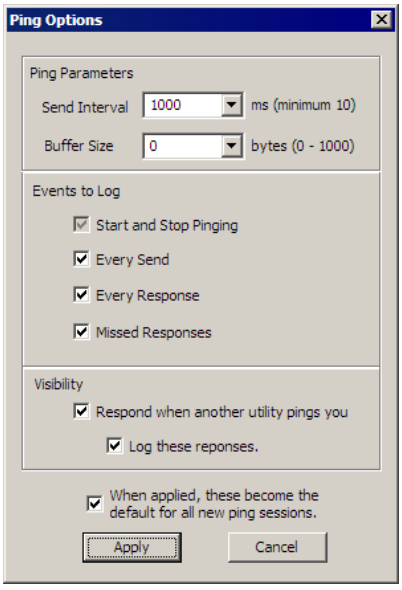
To start the ping session, enable "Show Ping Stations" on the View menu, and then highlight one of the other computers visible in the IH Browser. The session then starts automatically and the Ping Results dialog box opens.




This dialog box displays statistics on the minimum, maximum and average latency between two points on the network.

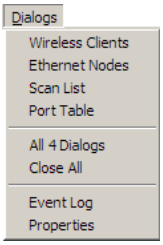
*Ping Options dialog box*

The Ping Options dialog box opens when you click the Show Options button on the Ping Results (page 65) dialog box. Use this dialog box to choose ping parameters, logging options, and response to other stations.




## 5.4 Dialogs Menu

The Dialogs menu contains the following commands:

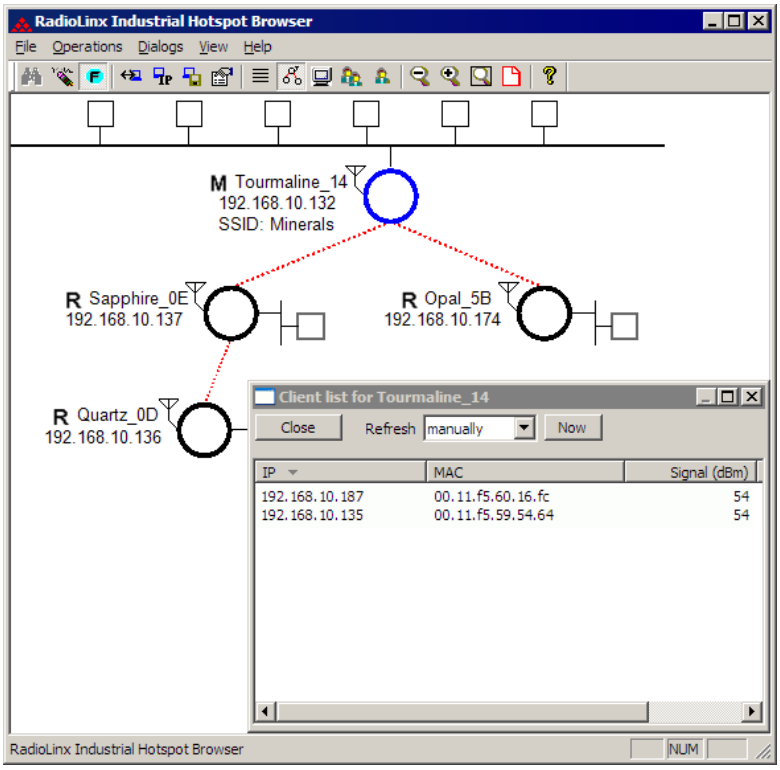



- Wireless Clients (page 67)
- Ethernet Nodes (page 68)
- Scan List (page 69)
- Port Table (page 70)
- Event Log (page 70)
- Properties (page 71)

### 5.4.1 Wireless Clients

This dialog box opens when you open the AP Dialogs menu and choose Wireless Clients.

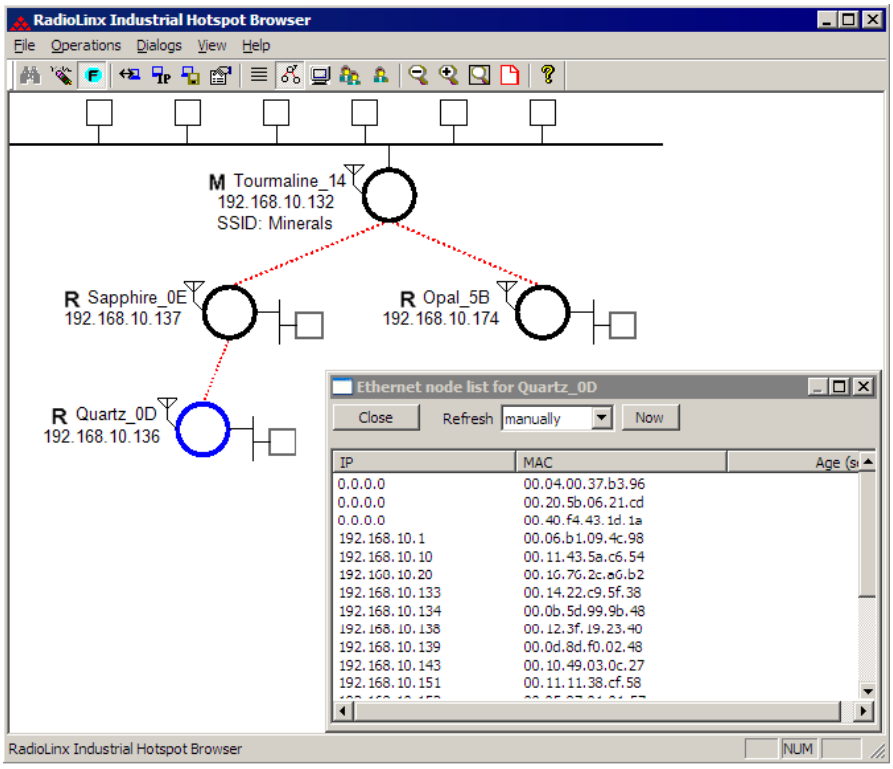
Use this dialog box to see information about wireless clients attached to the radio.



### 5.4.2 Ethernet Nodes

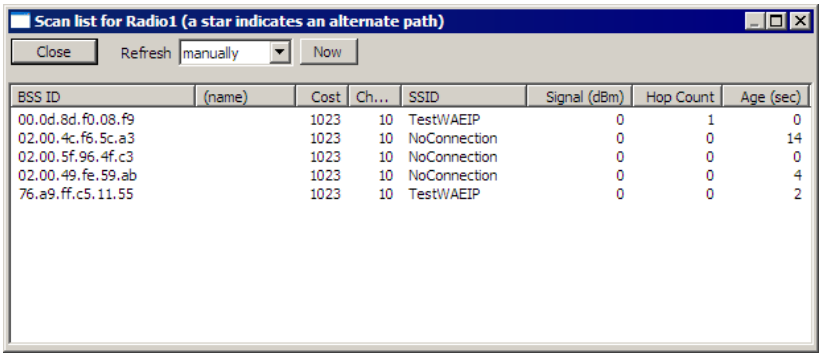
This dialog box opens when you open the AP Dialogs menu and choose Ethernet Nodes.

Use this dialog box to see information about Ethernet devices attached to the radios. The following illustration shows a list of Ethernet devices (by IP address and MAC ID) attached to the Ethernet port of Tourmaline_14. In addition to the IP and MAC ID it gives an age for each entry, which is the amount of time since a packet has been heard from that device.



### 5.4.3 Scan List

This dialog box opens when you open the AP Dialogs menu and choose Scan List.




The scan list is a list of all the radios that this particular radio "hears" on this channel (via beacons) even if it is not linked to it (different SSID or encryption). This list shows the same information as the Available Parents list in the Radio Configuration / Diagnostic Utility.

List entries marked with a "*" indicate the entry is an alternate path, which can also be seen if the 'parents' button is selected in the menu bar (blue lines will link the radio to its alternate parents).

*802.11 Access Point Detector*

The RLXIB Radio can be used as an installation tool to analyze the 802.11 environment and provide the user with information on choosing antenna location and channel selection.

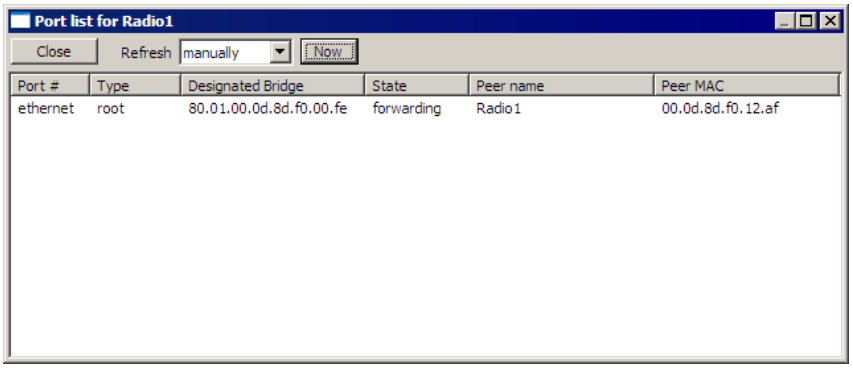
By using the table in the radio, you can mount an RLXIB Radio with its actual antenna and use it to report information on every active 802.11 radio in the area. It will report

- Each 802.11 AP heard including SSID
- Actual RSSI from each given in dBm
- Channel of each radio

Use this information to help choose a channel that is least utilized, or to select appropriate antenna types and alignments to minimize interference.

### 5.4.4 Port Table

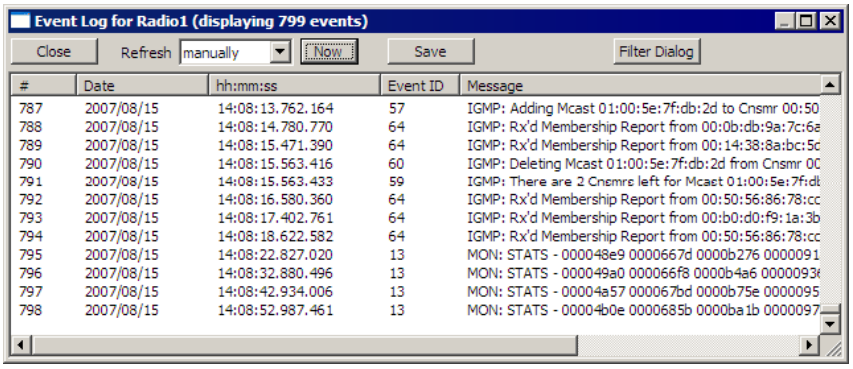
This dialog box opens when you open the AP Dialogs menu and choose Port Table.




The port table is a list of all the active ports on the radio. This list shows the same information as the Port status (page 38) list in the Radio Configuration / Diagnostic Utility. Each radio can have up to 34 active ports—one Ethernet cable, one parent RF link, and up to 32 child RF links.

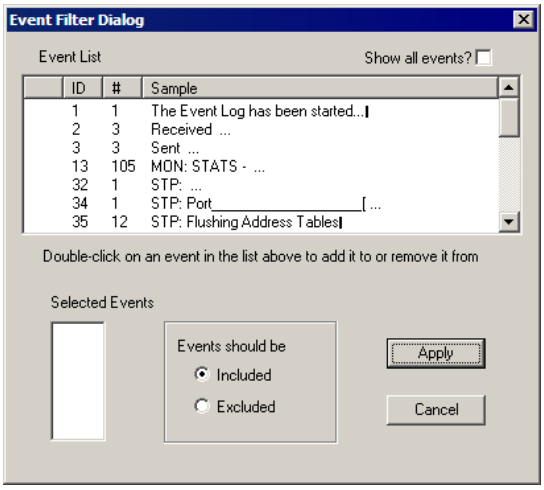
### 5.4.5 Event Log

The event log allows you to extract a log from the selected radio. The log shows a history of the radio. You can save the event log to a file for troubleshooting purposes.



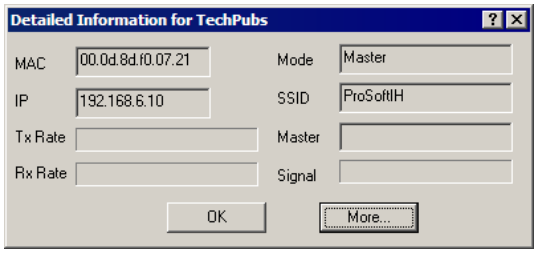
*Event Filter*

The Event Filter dialog box allows you to include or exclude specific event types from the event log.

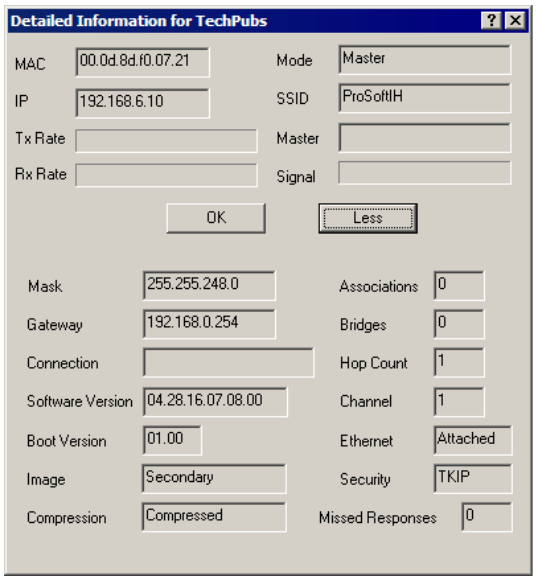



### 5.4.6 Properties

This dialog box opens when you select a radio, and then open the AP Dialogs menu and choose Properties.



To see additional properties, click the More button.

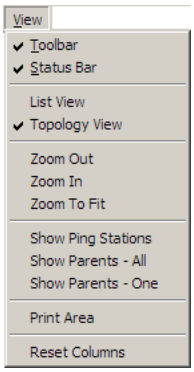



| Field | Description |
|---|---|
| Radio Name | The name of the selected radio. |
| MAC | The physical media access control address for the network interface. |
| IP, Mask, and Gateway | The radio's IP address, subnet mask, and default gateway. For information, see Radio Access settings (page 55). |
| IP State | Indicates whether a radio's IP address has been set—"Uninit(ialized)" or "OK". |
| SSID | A name that identifies a wireless network. You assign this name when you configure the radio. The SSID must be the same for all radios on the same network. |
| Mode | Indicates whether you designated the radio as a master, repeater, or client. |
| Connection | The status of the wireless connection. |
| Signal | The signal strength, which in this field is a number from 0 to 15. |
| Hops | The number of wireless connections a radio is from the closest master radio. |
| Master | The MAC address of the selected radio's master radio. |
| Associations | The number of network elements to which a radio has a wireless connection. |
| Bridges | The number of repeaters to which a radio has a wireless connection. |
| Tx and Rx | The transmission throughput rate and the received throughput rate. Both rates are measured in kilobytes per second (KB/s). |
| Software Version and Boot Version | The versions of the radio's firmware and its boot code. |
| Image | The image type can be Primary or Secondary. |
| Compression | Indicates whether the radio's firmware images are compressed or not. |
| Ethernet | The Ethernet connection status, either Attached or Detached. |

| Field | Description |
|---|---|
| Channel | The channel that the radio is using, if connected. The channel list indicates the channel number as well as the frequency (2.4 gHz or 5 gHz).<br><br>**Important:** The RLXIB radio is supplied with a dual-band antenna that supports both frequency ranges. If you use a different antenna with the RLXIB radio, you must choose a channel and frequency range supported by the antenna. |
| Security | Indicates the encryption setting on the radio. See Security settings (page 52) for information. |

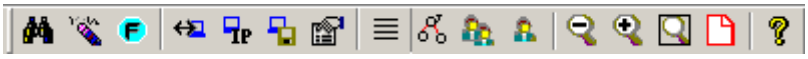
## 5.5 View Menu

The View menu contains the following commands:




- Tool Bar (page 73)
- Status Bar (page 74)
- List View (page 74)
- Topology View (page 75)
- Zoom In (page 76)
- Zoom Out (page 77)
- Zoom to Fit (page 77)
- Show Ping Stations (page 78)
- Show Parents (page 78)
- Print Area (page 79)
- Reset Columns (page 79)

### *5.5.1 Tool Bar*

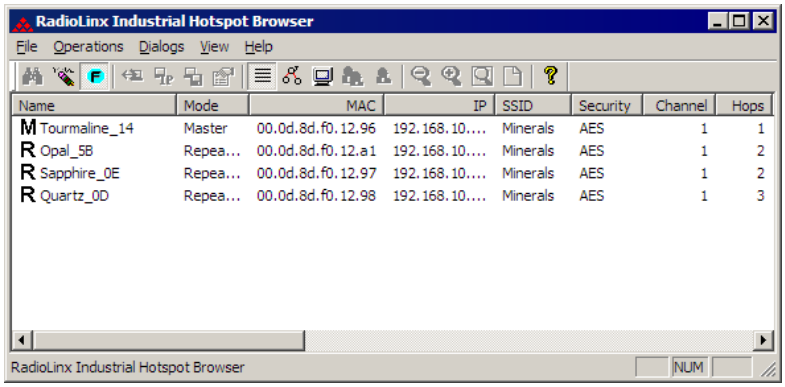


The Tool Bar near the top of the IH Browser window contains buttons to access frequently used commands. Hold the mouse button over each button to view a brief "Tool Tip" explaining the button's use.

### 5.5.2 Status Bar


The Status Bar at the bottom of the RLX IH Browser displays additional information about the currently selected menu command or tool bar button. On the right side of the Status Bar, you can see the status of the Caps Lock and Num Lock keys on your computer keyboard. Use the corner of the status bar to drag and resize the RLX-IH Browser window.

### 5.5.3 List View



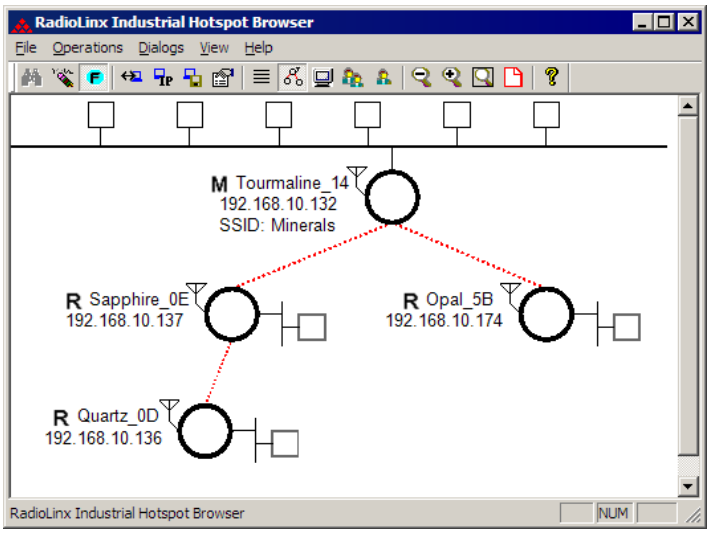

List View shows a list of all the connected radios in a grid, arranged similarly to data in a spreadsheet. Resize the window or scroll across to see all of the available columns. Click between column headers and drag to the left or right to resize columns. Click on column headers and drag to the left or right to re-order columns.

Tip: Use the Reset Columns command to restore the column size and order to their default values.

### 5.5.4 Topology View

To see how radios are connected together in the network, select Topology View from the View menu. The Topology view shows a diagram of the network's wireless connections. If a radio does not appear in the view, it is not connected to the network. To change the way a radio is linked to the network, connect to it and make changes through its Web page. For information on these settings, see Parent Link settings (page 42).

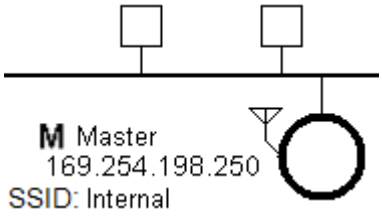
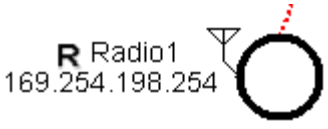
In the topology view, you can double-click a radio to log in to the Radio Configuration / Diagnostic Utility and change the radio's settings. To view a radio's properties, right-click on a radio representation in the topology view and then select Properties from the resulting menu.

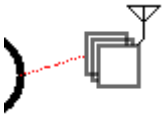



Refer to Topology View key (page 75) for an explanation of the symbols that appear in this view.

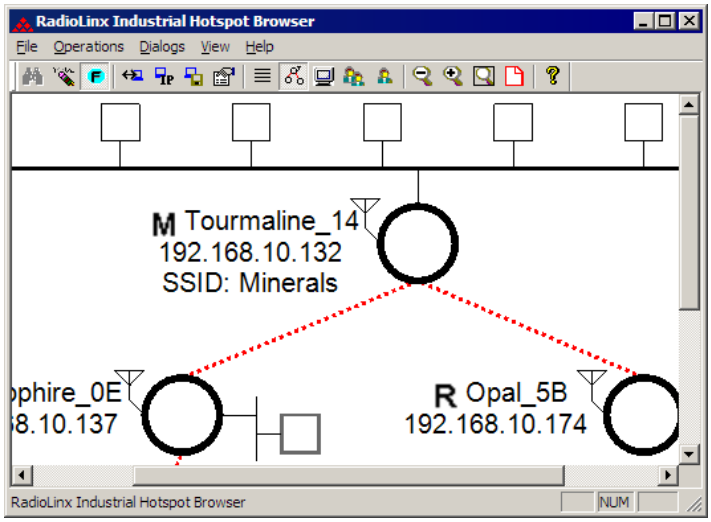
*Topology View key*

For information on other options that appear when you right-click a radio representation, see RLX-IH Browser options (page 59).

| | |
|---|---|
|  | Master; always shown at the top |
|  | Radio linked to the network |

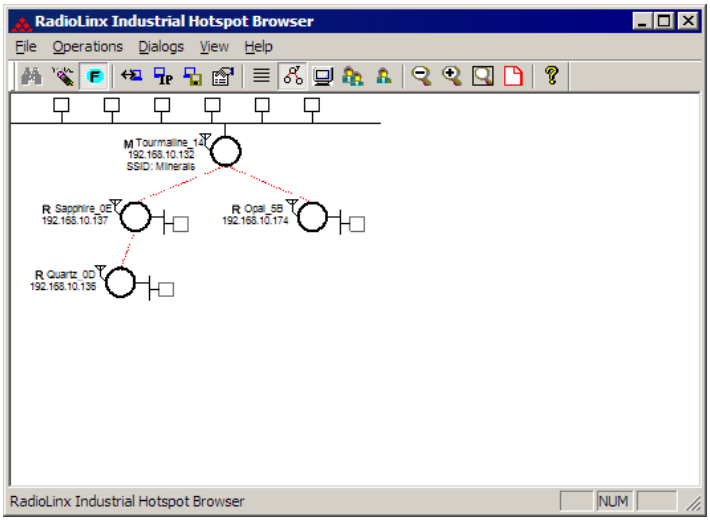
| | |
|---|---|
|  | Radio not linked; no parent |
|  | An Ethernet connection exists to the radio; does not indicate the number of devices on the connection |
|  | Wireless clients (PCMCIA cards) are linked to this radio; the number of clients linked is indicated by the number of boxes |
|  | Signal strength; the width of the line is not calibrated |
|  | Alternate parents. |

### 5.5.5 Zoom In



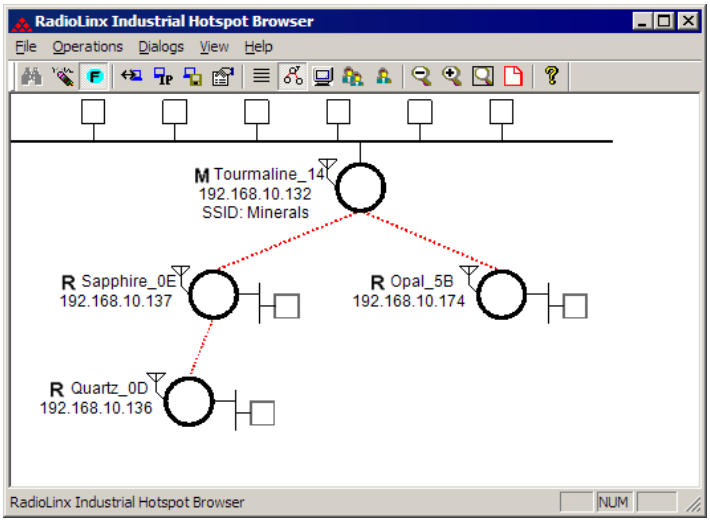

Use the **ZOOM IN** command in Topology View to enlarge the size of the items in the RadioLinx IH Browser window.

### 5.5.6 Zoom Out




Use the **ZOOM OUT** command in Topology View to to reduce the size of the items in the RadioLinx IH-Browser window.

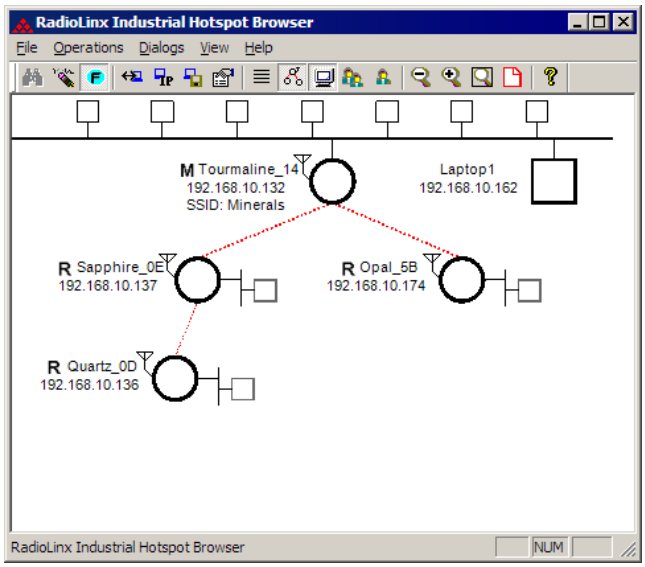
### 5.5.7 Zoom to Fit




Use the **ZOOM TO FIT** command in Topology View to change the size of the items so that the entire network fits within the RadioLinx IH-Browser window.

### 5.5.8 Show Ping Stations

Ping Stations are other computers running an instance of RadioLinx IH Browser. To test latency between points on the network, select a ping station, open the Operations menu, and then choose Start Ping Session.

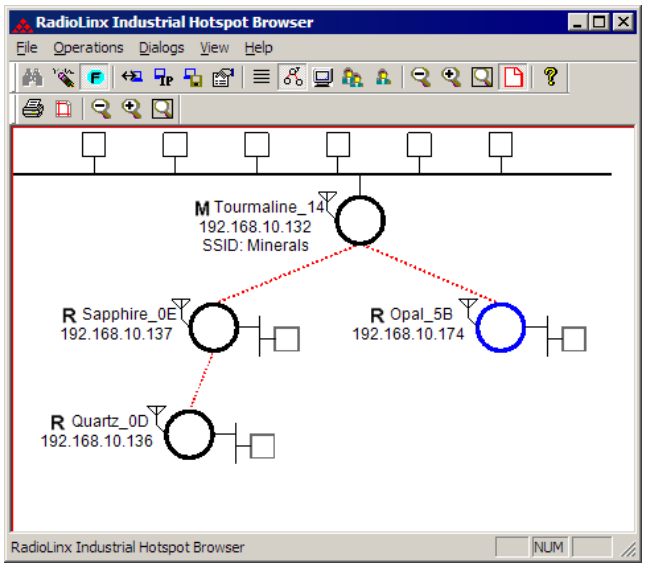



### 5.5.9 Show Parents

The show parents function allows you to display the possible alternate parents for a repeater graphically in the topology view. The link from the repeater to its current parent will be shown in red. If the repeater can hear other radios in the network, links to those radios will be shown in blue. This gives a graphical representation of the number of alternate paths available to a radio should its parent link go down. A detailed list of each of the alternates can be seen by right-clicking and selecting ‘Scan List'. This list, though, shows not only radios in the same network but also 802.11 radios on other networks.

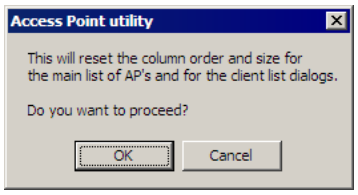
By selecting All, alternate paths for all repeaters in the network will be shown. By selecting One, alternate paths will be shown only for the one repeater that is currently selected.

### 5.5.10 Print Area




Use the Print Area command to show the border around the area of the IH Browser window that you can print using the Print command on the File menu.

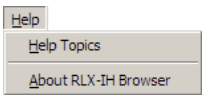
### 5.5.11 Reset Columns




Use the Reset Columns command to restore the column size and order to their default values. You will be prompted to confirm this action.

## 5.6 Help Menu

The Help menu contains the following commands:




- Help Topics (page 79)
- Help Index
- About RLX-IH Browser (page 80)

### 5.6.1 Help Topics

Most of the information needed to help you use the RadioLinx IH Browser is provided in an online help system that is always available whenever you are running the application.

To view the online help, start the RadioLinx IH Browser, open the Help menu, and then choose Help Topics.

*The RadioLinx IH Browser Help System*

The RadioLinx IH Browser has an online help system that works like a web browser. Each dialog box has its own page in the help system, which explains each item on the dialog box.

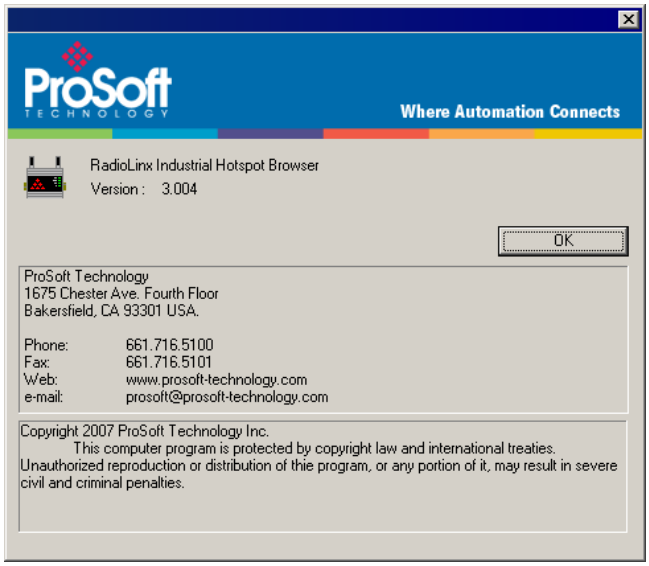
To view the online help, open the Help menu and choose Help Topics.

Many help pages have **links** that lead you to more information if you need it. Links are always **underlined**. Use your mouse to click the underlined text to "follow a link" and open a help page with more information.

You can use the Search tab to search for words or phrases inside a help file. The help system shows you a list of help topics that contain the words you typed in the Search field. Click a topic from the list to view the help page.

You can also use the Index button to see an index of keywords. You can type the first few letters of a keyword to jump directly to the part of the index you would like to view. Each keyword is linked to one or more help topics. Click a keyword to see a list of topics, and then click a topic from the list to view the help page.

### *5.6.2 About RLX-IH Browser*




Use this command to view version information about the RadioLinx IH Browser. You may be asked to provide this information if you contact ProSoft Technical Services.

# 6 Reference

*In This Chapter*



## 6.1 Product Overview

The RLXIB-IHW-66 is an industrial high-speed Ethernet radio. You can use it in place of Ethernet cables to save money, extend range, and make connections that may not otherwise be feasible. The radio operates as a wireless Ethernet switch, so any data that you can send over a wired network can also be sent over the radio.

The RLXIB-IHW-66 is certified for unlicensed operation in the United States, Canada and Europe at 2.4 and 5 GHz. With an output power of a 50mW (typical) approved high-gain antennas, the radios can achieve distances of 5 miles line-of-sight between them. You can use multiple repeaters (page 38) to extend this range to far greater distances.

You can develop a highly reliable wireless network by creating redundant (page 49) wireless paths. Multiple master (page 41) radios can be installed without any special programming or control. Repeater (page 41) radios can connect to any master at anytime; if one master goes down, the repeater connects to another. Likewise, if a repeater goes down, any repeater that was connected to it can reconnect to a different repeater, keeping the network intact. You can create large, self-healing tree-like networks in this fashion. Fully redundant paths are possible because the Spanning Tree (page 49) protocol in the radios disables and enables paths as necessary to avoid Ethernet loops, which would otherwise make your network stop functioning.

In addition to acting as a switch, every master or repeater radio in an RLXIB-IHW-66 wireless network can simultaneously act as an 802.11 a, b or g access point. This allows 802.11 WiFi clients to connect and roam between radios for monitoring of the wireless network or general network access. The RLXIB-IHW-66 has a special client mode that allows connection of any Ethernet device to any existing 802.11 a, b or g access point, regardless of the brand. (An example of an 802.11 client is a laptop with a WLAN card.)

Note: WiFi is a brand name originally issued by the WiFi Alliance, used to describe the underlying technology of wireless_local area networks (WLAN) based on the IEEE 802.11 specifications.

A high level of security is inherent with AES (Advanced Encryption Standard) encryption. You also can choose TKIP (Temporal Key Integrity Protocol), and if necessary add WEP128 or WEP64 (Wired Equivalent Protocol) encryption in addition to AES or TKIP for clients that do not support AES. A simple Media Access Control (MAC) filter table restricts the radios or clients that can link to a selected radio according to the MAC IDs you enter in the table.

The radio is designed for industrial applications with a metal enclosure, DIN rail mounting, and shock and vibration tested to IEC 60068.

The RLXIB-IHW-66 is easy to use. Use the Radio Configuration / Diagnostic Utility, which runs in your web browser, to configure the radio; optionally, you can use an SNMP manager for configuration. The radio comes with a Windows-based utility called RLX-IH Browser that finds all the radios on the network and lists information about them. A topology view in the RLX-IH Browser shows how the wireless network is linked together at any point in time. You can update firmware at any time from anywhere on the network, even over the wireless link or over the Internet.

ProSoft Technology radios can easily be installed into new or existing systems. The software and manuals can be downloaded from the CD or ProSoft Technology's web site at http://www.prosoft-technology.com.

## 6.2 Radio hardware

The RLXIB-IHW-66 radio consists of the following components, as illustrated and explained below:

Two antenna ports (AUX and MAIN)

LEDs that indicate the status of the radio

Ethernet port (page 83)


### *6.2.1 Radio power requirements*

The RLXIB-IHW-66 radio accepts 802.3af PoE, with an average power draw of less than 6 watts. You can also order an optional DC PoE Injector if AC is not available. The DC power wires must be less than 3 m to meet regulatory requirements.

The radio shall be installed by trained personnel only, as outlined to the installation instructions provided with each radio.

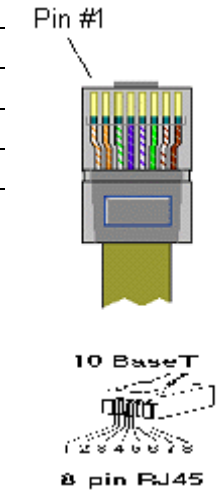
The equipment shall be installed by a qualified installer/electrician. The installer/electrician is responsible for obtaining a secured ground connection between the lug terminal on the surge protector to a verified common ground point using a minimum 18 gauge wire. This must be done when attaching power lines to the radio during installation. .

A solid ground connection should be verified using a meter prior to applying power to the radio. Failing to secure a proper ground could result in serious injury or death as a result of a lightning strike.

### 6.2.2 Ethernet Cable Configuration

Note: The standard connector view shown is color-coded for a straight-through cable.

| Crossover cable | |
|---|---|
| RJ-45 PIN | RJ-45 PIN |
| 1 Rx+ | 3 Tx+ |
| 2 Rx- | 6 Tx- |
| 3 Tx+ | 1 Rx+ |
| 6 Tx- | 2 Rx- |




| Straight- through cable | |
|---|---|
| RJ-45 PIN | RJ-45 PIN |
| 1 Rx+ | 1 Tx+ |
| 2 Rx- | 2 Tx- |
| 3 Tx+ | 3 Rx+ |
| 6 Tx- | 6 Rx- |

### 6.2.3 Ethernet Cable specifications

The recommended cable is category 5 or better. A category 5 cable has four twisted pairs of wire that are color-coded and cannot be swapped. The radio uses only two pairs. One pair uses pins 1 and 2, and the second pair uses pins 3 and 6.

Use a straight-through cable when connecting the radio to an Ethernet hub or a 10/100 Base-T Ethernet switch. Straight-through cables are used in most cases.

Use a cross-over cable when connecting the Ethernet radio directly to any device that is NOT a switch or a hub (e.g., a direct connection to a PC, PLC, or printer).

Ethernet cabling is like U.S. telephone cables, except that it has eight conductors. Some hubs have one input that can accept either a straight-through or crossover cable, depending on the switch position. In this case, you must ensure that the switch position and cable type agree.

Refer to Ethernet cable configuration (page 83) for a diagram of how to configure Ethernet cable.

# 7 Glossary of Terms

**8**

802.11

A group of wireless specifications developed by the IEEE. It details a wireless interface between devices to manage packet traffic.

802.11a

Operates in the 5 GHz frequency range with a maximum 54 Mbit/sec signaling rate.

802.11b

Operates in the 2.4 GHz Industrial, Scientific, and Measurement (ISM) band. Provides signaling rates of up to 11 Mbit/sec and is the most commonly used frequency.

802.11g

Similar to 802.11b but supports signaling rates of up to 54 Mbit/sec. Operates in the heavily used 2.4 GHz ISM band but uses a different radio technology to boost throughput.

802.11i

Sometimes Wi-Fi Protected Access 2 (WPA 2). WPA 2 supports the 128-bit and above advanced encryption Standard, along with 802.1x authentication and key management features.

802.11n

Designed to raise effective WLAN throughput to more than 100 Mbit/sec.

802.11s

Deals with mesh networking.

**A**

Access Point

A generic term for an 802.11 radio that "attaches" other 802.11 radios (clients) to a wired network. APs can also bridge to one another.

Ad hoc Mode

Wireless network framework in which devices can communicate directly with one another without using an AP or a connection to a regular network.

AES

Advanced Encryption Standard. New standard for encryption adopted by the U.S. government for secure communications.

Amplifier

A device connected to an antenna used to increase the signal strength and amplify weak incoming signals.

Antenna

A device connected to a wireless transceiver that concentrates transmitted and received radio waves to increase signal strength and thus the effective range of a wireless network.

ASCII

American Standard Code for Information Interchange. A communication mode in which each eight-bit byte in a message contains one ASCII character code. ASCII characters (or hexadecimal characters) are sometimes used as a key to encrypt data and ensure its secure transmission.

Association

Process whereby two 802.11 radios establish communications with each other. Requirements for communication include common SSID (network names) and encryption settings.

Authenticate

The process of confirming the identity of someone connecting to a network.

Authentication Server

A back-end database server that confirms the identity of a supplicant to an authenticator in an 802.1x-authenticated network.

**B**

Band

Another term for spectrum used to indicate a particular set of frequencies. Wireless networking protocols work in either the 2.4 GHz or the 5 GHz bands.

Bandwidth

(See Throughput)

Base Station

See Wireless Gateway

Baud Rate

The speed of communication between devices on the network. All devices must communicate at the same rate.

bps

Bits per Second. A measure of data transmission speed across a network or communications channel;bps is the number of bits that can be sent or received per second.

**C**

Channel

One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference.

Client

A client is software program, or the device on which that program runs, that makes requests for information from a software program, or the device on which that program runs, in a client-server relationship.

A Client on an Ethernet network is equivalent to a Master on a serial network.

Configuration PC

A Computer that contains the IH Browser Setup/Diagnostic software (for Frequency Hopping radios), or RadioLinx IH Browser Setup/Diagnostic software (for Industrial Hotspot and Industrial Broadband radios).

**D**

dBi

Decibels referenced to an "ideal" isotropic radiator in free space; frequently used to express antenna gain

dBm

Decibels referenced to one milliwatt (mW); an "absolute" unit used to measure signal power (transmit power output or received signal strength)

DCE

Data communications equipment. A modem, for example.

Decibel (dB)

A measure of the ratio between two signal levels; used to express gain (or loss) in a system.

Default Gateway

The IP address of a network router where data is sent if the destination IP address is outside the local subnet. The gateway is the device that routes the traffic from the local area network to other networks such as the Internet.

Device-to-Device Network (Peer-to-Peer Network)

Two or more devices that connect using wireless network devices without the use of a centralized wireless access point. Also known as a peer-to-peer network.

DHCP

Dynamic Host Configuration Protocol. A protocol by which a server automatically assigns IP addresses to clients so users don't have to configure them manually.

Direct Sequence Spread Spectrum

One of two approaches (with frequency hopping spread spectrum) for sorting out overlapping data signals transmitted via radio waves. 802.11b uses DSSS

Directional Antenna

Transmits and receives radio waves off the front of the antenna.

Diversity Antenna

An antenna system that uses multiple antennas to reduce interference and maximize reception and transmission quality.

DTE

Data Terminal Equipment, for example, a computer or terminal.

Dual Band

A device that is capable of operating in two frequencies. On a wireless network, dual-band devices are capable of operating in both the 2.4 GHz (802.11b/g) and 5 Hz (802.11a) bands.

**E**

EAP

Extensible Authentication Protocol. A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks.

EIRP

Equivalent isotropically radiated power (EIRP) is the amount of power that would have to be emitted by an isotropic antenna (that evenly distributes power in all directions and is a theoretical construct) to produce the peak power density observed in the direction of maximum antenna gain.

Encryption

Method of scrambling data so that only the intended viewers can decipher and understand it.

ESD

Electrostatic Discharge. Can cause internal circuit damage to the coprocessor.

ESSID

Extended Service Set Identifier. A name used to identify a wireless network.

**F**

Firmware

Firmware is the embedded software code that that runs in the module to direct module function (similar to the BIOS in a personal computer). This is distinguished from the Setup/Diagnostic Application software that is installed on the Configuration PC.

Frequency Hopping

A radio that rapidly changes its operating frequency several times per second following a pre-determined sequence of frequencies. The transmitting and receiving radios are programmed to follow the same frequency hopping sequence.

Frequency Hopping Spread Spectrum

Changes or hops frequencies in pattern known to both sender and receiver. FHSS is little influenced by radio stations, reflections, or other environmental factors. However, it is much slower than DSSS.

Fresnel Zone

An elliptical area on either side of the straight line of sight that must also be clear for a long-range wireless network to work.

Full-Duplex

A communications circuit or system designed to simultaneously transmit and receive two different streams of data. Telephones are an example of a full-duplex communication system. Both parties on a telephone conversation can talk and listen at the same time. If both talk at the same time, their two signals are not corrupted.

**G**

Gain

The amount by which an antenna concentrates signal strength in a wireless network.

Gateway

In wireless terms, a gateway is an access point with additional software capabilities such as providing NAT and DHCP.

## H

### Half-Duplex

A communications circuit or system designed to transmit and receive data, but not both simultaneously. CB or walkie-talkie radios are an example of a half-duplex communication system. Either parties on a radio conversation may talk or listen; but both cannot talk at the same time without corrupting each other's signal. If one operator is "talking", the other must be "listening" to have successful communication.

### Hz

Hertz. The international unit for measuring frequency equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigabit (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz. 802.11a devices operate in the GHz band; 802.11b and g devices operate in the 2.4 GHz band.

## I

### IEEE

Institute of Electrical and Electronics Engineers, Inc. IEEE is a professional organization with members in over 175 countries and is an authority in technical areas such as computer engineering and telecommunications. IEEE developed the 802.11 specifications.

### IP Address

An identifier for a computer or device in a TCP/IP network. Networks using the TCP/IP Protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255. For example, 192.168.0.100 could be an IP address.

## K

### Key

A set of information (often 40 to as much as 256 bits) that is used as a seed to an encryption algorithm to encrypt (scramble) data. Ideally, the key must also be known by the receiver to decrypt the data.

## L

### LAN

A system of connecting PCs and other devices within the same physical proximity for sharing resources such as internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

LED

Light-emitting diode.

Line of Sight (LoS)

A clear line from one antenna to another in a long-range wireless network.

Link point

The graphical point next to a radio icon that represents the connection point for RF communications between radios. An RF connection between two radios is called an RF Link and is represented as a graphical black line between the radio's link points.

**M**

MAC ID

Media Access Control address. Every 802.11 device has its own MAC address. This is a unique identifier used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to the network's MAC table are able to get on the network.

Master device

Device that is connected to the Master radio.

Mbps

Megabits per second, or millions of bits per second. A measure of bandwidth.

Megahertz

A measure of electromagnetic wave frequency equal to one million hertz. Often abbreviated as MHz and used to specify the radio frequency used by wireless devices.

Mesh Networking

Features free standing, non wired network nodes that communicate among one another and form self-configuring networks, with only one node required to hook into a wired LAN. The other nodes are simply plugged into an electrical outlet, so cabling is much less of an issue.

MIC

Message Integrity Check. One of the elements added to the TKIP standard. A "signature" is added by each radio on each packet it transmits. The signature is based on the data in the packet, a 64-bit value (key) and the MAC address of the sender. The MIC allows the receiving radio to verify (check) that the data is not forged.

MIMO

Multiple Input Multiple Output refers to using multiple antennas in a WiFi device to improve performance and throughput. MIMO technology takes advantage of a characteristic called multipath, which occurs when a radio transmission starts out at Point A and the reflects off or passes through surfaces or objects before arriving, via multiple paths, at Point B. MIMO technology uses multiple antennas to collect and organize signals arriving via these paths.

Modbus

The Modbus protocol provides the internal standard that the MODICON® controllers use for parsing messages. During communications on a ModBus network, the protocol determines how each controller will know its device address, recognize a message addressed to it, determine the kind of action to be taken, and extract any data or other information contained in the message. If a reply is required, the controller will construct the reply message and send it using ModBus protocol.

Modem

Stands for MODulator-DEModulator, a device that converts digital signals to analog signals and vice-versa. Analog signals can be transmitted over communications links such as telephone lines.

**N**

Network

A series of stations or nodes connected by some type of communication medium. A network may consist of a single link or multiple links.

Node

An address or software location on the network.

Null Modem Cable

A specialty cross-communication cable with female connectors on each end used for direct connection between devices when no modems are present. Commonly used as a quick and inexpensive way to transfer files between two PCs without installing a dedicated network card in each PC.

**P**

Panel Antenna

An antenna type that radiates in only a specific direction. Panel antennas are commonly used for point-to-point situations. Sometimes called Patch antennas.

Parabolic Antenna

An antenna type that radiates a very narrow beam in a specific direction. Parabolic antennas offer the highest gain for long-range point-to-point situations.

### Peer-to-Peer Network

Each radio in a Peer-to-Peer network has the ability to receive data from - and transmit data to - any other radio in the network.

### Point-Multipoint (Broadcast) Network

A network type where a single master radio sends data to every remote radio in the network. This is done repeatedly until every remote radio individually receives and acknowledges the data. Each remote radio sends pending data to the master radio that receives and acknowledges data sent from each remote. In this configuration, there are multiple remote radios referenced to a single master radio.

### Point-Multipoint (Modbus) Network

A network with a single Master radio and multiple Remote radios. The devices cabled to the radios communicate through the Modbus standard protocol. The Master radio sends data to a Remote radio based on the Modbus address of the Modbus device. The data is only sent to the single Remote device based on its address. Each Remote radio sends its data only to the Master radio. The Master and Remote radios acknowledge that data was received correctly.

### Point-to-Multipoint

A wireless network in which one point (the access point) serves multiple other points around it. Indoor wireless networks are all point-to-multipoint, and long-range wireless networks that serve multiple clients usually employ either a single omnidirectional antenna or multiple sector antennas.

### Point-to-Point Network

A network consisting of a single Master radio and a single Remote radio. All data from the Master is received and acknowledged by one Remote. All data from the single Remote is received and acknowledged by the Master radio.

### Poll

A method of electronic communication.

### Power Supply

Device that supplies electrical power to the I/O chassis containing the processor, coprocessor, or other modules.

### Protocol

The language or packaging of information that is transmitted between nodes on a network.

## Q

QoS

Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications.

## R

RADIUS

Remote Access Dial-In Service. This describes a general method for allowing remote users access to a network. It authenticates the user, specifies passwords and access rights to network resources. It also keeps track of accounting for when and how long the user is logged onto the network. It was originally used for dial-in users, accessing corporate networks via modems. It is now being specified as part of the 802.11i standard to control access of users to wireless networks. Any of several protocols can be used by the wireless client to communicate with the RADIUS server to gain access to the network resources. These protocols include EAP-TLS (Windows), LEAP (Cisco) and EAP-TTLS.

Range

The distance covered by a wireless network radio device. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to a mile.

Remote Access Point

One of a number of secondary access points in a wireless network that uses WDS to extend its range. Remote access points (sometimes called relay access points) connect to a master access point.

Remote device

Devices connected remote radios

Repeater

A Repeater is a device used to extend the range of a Wi-Fi signal. Placed at the edge of signal reception, a repeater simply receives and re-transmits the signal.

RS-232

Recommended Standard 232; the standard for serial binary signals between DTE and DCE devices.

RTU (Remote Terminal Unit)

Modbus transmission mode where each eight-bit byte in a message contains two four-bit hexadecimal characters. There are two transmission modes (ASCII or RTU). The main advantage of the RTU mode is that its greater character density allows better data throughput than ASCII mode for the same baud rate; each message is transmitted in a continuous stream. (See also ASCII, above.)

## S

Sector Antenna

An antenna type that radiates in only a specific direction. Multiple sector antennas are commonly used in point-to-multipoint situations.

Signal Diversity

A process by which two small dipole antennas are used to send and receive, combining their results for better effect.

Signal Loss

The amount of signal strength that's lost in antenna cable, connectors, and free space. Signal loss is measured in decibels. Also referred to as gain loss.

Signal Strength

The strength of the radio waves in a wireless network.

Simplex

A communications circuit or system designed to either transmit data or receive data, but not both. Broadcast television is an example of simplex communication system. A television station sends a TV signal but cannot receive responses back from the television sets to which it is transmitting. The TV sets can receive the signal from the TV station but cannot transmit back to the station.

Site Survey

A comprehensive facility study performed by network managers to ensure that planned service levels will be met when a new wireless LAN, or additional WLAN segments to an existing network are deployed. Site survey's are usually performed by a radio frequency engineer and used by systems integrators to identify the optimum placement of access points to ensure that planned levels of service are met. Site surveys are sometimes conducted following the deployment to ensure that the WLAN is achieving the necessary level of coverage. Site surveys can also be used to detect rogue access points.

Spectrum

A range of electromagnetic frequencies.

Spread Spectrum

A form of wireless communication in which a signal's frequency is deliberately varied. This increases bandwidth and lessens the chances of interruption or interception of the transmitted signal.

SSI

Service Set Identifier is a sequence of characters unique to a specific network or network segment that's used by the network and all attached devices to identify themselves and allow devices to connect to the correct network when one or more than one independent network is operating in nearby areas.

Subnet Mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: the network address, and the host (node or device) address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network (with a subnet mask of 255.255.0.0), the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

**T**

TKIP

Temporal Key Integrity Protocol. The wireless security encryption mechanism in Wi-Fi Protected Access. TKIP uses a key hierarchy and key management methodology that removes the predictability that intruders relied upon to exploit the WEP key. In increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by an authentication server, providing some 500 trillion possible keys tht can be used on a given data packet. If also includes a Message Integrity Check (MIC), designed to prevent the attacker from capturing data packets, altering them, and resending them. By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult (if not impossible) for a would-be intruder to break into a Wi-Fi network.

**U**

UART

Universal Asynchronous Receiver/Transmitter

**W**

WAP

Wireless Application Protocol. A set of standards to enable wireless devices to access internet services, such as the World Wide Web and email.

WDS

Wireless Distribution System. Enables access points to communicate with one another in order to extend the range of a wireless networks. Used in 802.11g based access points.

WEP

Wired-Equivalent Privacy protocol was specified in the IEEE 802.11 standard to provide a WLAN with a minimal level of security and privacy comparable to a typical wired LAN, using data encryption.

Wi-Fi

A certification mark managed by a trade group called the Wi-Fi Alliance. Wi-Fi certification encompasses numerous standards including 802.11a, 802.11b, 802.11g, WPA, and more. Equipment must pass compatibility testing to receive the Wi-Fi mark.

Wi-Fi CERTIFIED™

The certification standard designating IEEE 802.11-based wireless local area network (WLAN) products that have passed interoperability testing requirements developed and governed by the Wi-Fi alliance.

Wi-Fi Interoperability Certificate

A statement that a product has passed interoperability testing and will work with other Wi-Fi CERTIFIED products.

Wi-Fi Protected Setup

Wi-Fi Protected Setup™ (previously called Wi-Fi Simple Config) is an optional certification program developed by the Wi-Fi alliance designed to ease set up of security enabled Wi-Fi networks in the home and small office environment. Wi-Fi Protected Setup supports methods (pushing a button or entering a PIN into a wizard-type application) that are familiar to most consumers to configure a network and enable security.

Wireless Gateway

Term used to differentiate between an access point and a more-capable device that can share an internet connection, serve DHCP, and bridge between wired and wireless networks.

Wireless Network

Devices connected to a network using a centralized wireless access point.

WLAN

Wireless Local Area Network. A type of local area network in which data is sent and received via high-frequency radio waves rather than cables or wires.

WPA

Wi-Fi Protected Access is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. It improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.

WPA2

An enhanced version of WPA. It is the official 802.11i standard. It uses Advanced Encryption Standard instead of TKIP. AES supports 128-bit, 192-bit, and 256-bit encryption keys.

## Y

Yagi Antenna

An antenna type that radiates in only a specific direction. Yagi antennas are used in point-to-point situations.

# 8 Support, Service & Warranty

*In This Chapter*



ProSoft Technology, Inc. (ProSoft) is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

**1** Product Version Number
**2** System architecture
**3** Network details

If the issue is hardware related, we will also need information regarding:

**1** Module configuration and contents of file
   - Module Operation
   - Configuration/Debug status information
   - LED patterns

**2** Information about the processor and user data files as viewed through and LED patterns on the processor.
**3** Details about the serial devices interfaced, if any.

## 8.1 How to Contact Us: Technical Support

| | |
|---|---|
| **Internet** | Web Site: http://www.prosoft-technology.com/support |
| | E-mail address: support@prosoft-technology.com |

**Asia Pacific**

+603.7724.2080, support.asia@prosoft-technology.com
Languages spoken include: Chinese, English

**Europe (location in Toulouse, France)**

+33 (0) 5.34.36.87.20, support.EMEA@prosoft-technology.com
Languages spoken include: French, English

**North America/Latin America (excluding Brasil) (location in California)**

+1.661.716.5100, support@prosoft-technology.com
Languages spoken include: English, Spanish
*For technical support calls within the United States, an after-*hours *answering system allows pager access to one of our qualified technical and/or application support engineers at any time to answer your questions.*

**Brasil (location in Sao Paulo)**

+55-11-5084-5178, eduardo@prosoft-technology.com
Languages spoken include: Portuguese, English

## 8.2 Return Material Authorization (RMA) Policies and Conditions

The following RMA Policies and Conditions (collectively, "RMA Policies") apply to any returned Product. These RMA Policies are subject to change by ProSoft without notice. For warranty information, see "Limited Warranty". In the event of any inconsistency between the RMA Policies and the Warranty, the Warranty shall govern.

### *8.2.1 All Product Returns:*

a) In order to return a Product for repair, exchange or otherwise, the Customer must obtain a Returned Material Authorization (RMA) number from ProSoft and comply with ProSoft shipping instructions.
b) In the event that the Customer experiences a problem with the Product for any reason, Customer should contact ProSoft Technical Support at one of the telephone numbers listed above (page 99). A Technical Support Engineer will request that you perform several tests in an attempt to isolate the problem. If after completing these tests, the Product is found to be the source of the problem, we will issue an RMA.
c) All returned Products must be shipped freight prepaid, in the original shipping container or equivalent, to the location specified by ProSoft, and be accompanied by proof of purchase and receipt date. The RMA number is to be prominently marked on the outside of the shipping box. Customer agrees to insure the Product or assume the risk of loss or damage in transit. Products shipped to ProSoft using a shipment method other than that specified by ProSoft or shipped without an RMA number will be returned to the Customer, freight collect. Contact ProSoft Technical Support for further information.
d) A 10% restocking fee applies to all warranty credit returns whereby a Customer has an application change, ordered too many, does not need, etc.

### *8.2.2 Procedures for Return of Units Under Warranty:*

A Technical Support Engineer must approve the return of Product under ProSoft's Warranty:

a) A replacement module will be shipped and invoiced. A purchase order will be required.
b) Credit for a product under warranty will be issued upon receipt of authorized product by ProSoft at designated location referenced on the Return Material Authorization.

### *8.2.3 Procedures for Return of Units Out of Warranty:*

a) Customer sends unit in for evaluation
b) If no defect is found, Customer will be charged the equivalent of $100 USD, plus freight charges, duties and taxes as applicable. A new purchase order will be required.

c) If unit is repaired, charge to Customer will be 30% of current list price (USD) plus freight charges, duties and taxes as applicable. A new purchase order will be required or authorization to use the purchase order submitted for evaluation fee.

The following is a list of non-repairable units:

- 3150 - All
- 3750
- 3600 - All
- 3700
- 3170 - All
- 3250
- 1560 - Can be repaired, only if defect is the power supply
- 1550 - Can be repaired, only if defect is the power supply
- 3350
- 3300
- 1500 - All

### *8.2.4 Purchasing Warranty Extension:*

a) ProSoft's standard warranty period is three (3) years from the date of shipment as detailed in "Limited Warranty (page 101)". The Warranty Period may be extended at the time of equipment purchase for an additional charge, as follows:

- Additional 1 year = 10% of list price
- Additional 2 years = 20% of list price
- Additional 3 years = 30% of list price

## 8.3 LIMITED WARRANTY

This Limited Warranty ("Warranty") governs all sales of hardware, software and other products (collectively, "Product") manufactured and/or offered for sale by ProSoft, and all related services provided by ProSoft, including maintenance, repair, warranty exchange, and service programs (collectively, "Services"). By purchasing or using the Product or Services, the individual or entity purchasing or using the Product or Services ("Customer") agrees to all of the terms and provisions (collectively, the "Terms") of this Limited Warranty. All sales of software or other intellectual property are, in addition, subject to any license agreement accompanying such software or other intellectual property.

### 8.3.1 What Is Covered By This Warranty

a) *Warranty On New Products*: ProSoft warrants, to the original purchaser, that the Product that is the subject of the sale will (1) conform to and perform in accordance with published specifications prepared, approved and issued by ProSoft, and (2) will be free from defects in material or workmanship; provided these warranties only cover Product that is sold as new. This Warranty expires three years from the date of shipment (the "Warranty Period"). If the Customer discovers within the Warranty Period a failure of the Product to conform to specifications, or a defect in material or workmanship of the Product, the Customer must promptly notify ProSoft by fax, email or telephone. In no event may that notification be received by ProSoft later than 39 months. Within a reasonable time after notification, ProSoft will correct any failure of the Product to conform to specifications or any defect in material or workmanship of the Product, with either new or used replacement parts. Such repair, including both parts and labor, will be performed at ProSoft's expense. All warranty service will be performed at service centers designated by ProSoft.
b) *Warranty On Services*: Materials and labor performed by ProSoft to repair a verified malfunction or defect are warranteed in the terms specified above for new Product, provided said warranty will be for the period remaining on the original new equipment warranty or, if the original warranty is no longer in effect, for a period of 90 days from the date of repair.

### 8.3.2 What Is Not Covered By This Warranty

a) ProSoft makes no representation or warranty, expressed or implied, that the operation of software purchased from ProSoft will be uninterrupted or error free or that the functions contained in the software will meet or satisfy the purchaser's intended use or requirements; the Customer assumes complete responsibility for decisions made or actions taken based on information obtained using ProSoft software.
b) This Warranty does not cover the failure of the Product to perform specified functions, or any other non-conformance, defects, losses or damages caused by or attributable to any of the following: (i) shipping; (ii) improper installation or other failure of Customer to adhere to ProSoft's specifications or instructions; (iii) unauthorized repair or maintenance; (iv) attachments, equipment, options, parts, software, or user-created programming (including, but not limited to, programs developed with any IEC 61131-3, "C" or any variant of "C" programming languages) not furnished by ProSoft; (v) use of the Product for purposes other than those for which it was designed; (vi) any other abuse, misapplication, neglect or misuse by the Customer; (vii) accident, improper testing or causes external to the Product such as, but not limited to, exposure to extremes of temperature or humidity, power failure or power surges; or (viii) disasters such as fire, flood, earthquake, wind and lightning.

c) The information in this Agreement is subject to change without notice. ProSoft shall not be liable for technical or editorial errors or omissions made herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material. The user guide included with your original product purchase from ProSoft contains information protected by copyright. No part of the guide may be duplicated or reproduced in any form without prior written consent from ProSoft.

### 8.3.3 Disclaimer Regarding High Risk Activities

Product manufactured or supplied by ProSoft is not fault tolerant and is not designed, manufactured or intended for use in hazardous environments requiring fail-safe performance including and without limitation: the operation of nuclear facilities, aircraft navigation of communication systems, air traffic control, direct life support machines or weapons systems in which the failure of the product could lead directly or indirectly to death, personal injury or severe physical or environmental damage (collectively, "high risk activities"). ProSoft specifically disclaims any express or implied warranty of fitness for high risk activities.

### 8.3.4 Intellectual Property Indemnity

Buyer shall indemnify and hold harmless ProSoft and its employees from and against all liabilities, losses, claims, costs and expenses (including attorney's fees and expenses) related to any claim, investigation, litigation or proceeding (whether or not ProSoft is a party) which arises or is alleged to arise from Buyer's acts or omissions under these Terms or in any way with respect to the Products. Without limiting the foregoing, Buyer (at its own expense) shall indemnify and hold harmless ProSoft and defend or settle any action brought against such Companies to the extent based on a claim that any Product made to Buyer specifications infringed intellectual property rights of another party. ProSoft makes no warranty that the product is or will be delivered free of any person's claiming of patent, trademark, or similar infringement. The Buyer assumes all risks (including the risk of suit) that the product or any use of the product will infringe existing or subsequently issued patents, trademarks, or copyrights.

a) Any documentation included with Product purchased from ProSoft is protected by copyright and may not be duplicated or reproduced in any form without prior written consent from ProSoft.
b) ProSoft's technical specifications and documentation that are included with the Product are subject to editing and modification without notice.
c) Transfer of title shall not operate to convey to Customer any right to make, or have made, any Product supplied by ProSoft.
d) Customer is granted no right or license to use any software or other intellectual property in any manner or for any purpose not expressly permitted by any license agreement accompanying such software or other intellectual property.

e) Customer agrees that it shall not, and shall not authorize others to, copy software provided by ProSoft (except as expressly permitted in any license agreement accompanying such software); transfer software to a third party separately from the Product; modify, alter, translate, decode, decompile, disassemble, reverse-engineer or otherwise attempt to derive the source code of the software or create derivative works based on the software; export the software or underlying technology in contravention of applicable US and international export laws and regulations; or use the software other than as authorized in connection with use of Product.

f) **Additional Restrictions Relating To Software And Other Intellectual Property**

   In addition to compliance with the Terms of this Warranty, Customers purchasing software or other intellectual property shall comply with any license agreement accompanying such software or other intellectual property. Failure to do so may void this Warranty with respect to such software and/or other intellectual property.

### *8.3.5 Disclaimer of all Other Warranties*

The Warranty set forth in What Is Covered By This Warranty (page 102) are in lieu of all other warranties, express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

### *8.3.6 Limitation of Remedies ***

In no event will ProSoft or its Dealer be liable for any special, incidental or consequential damages based on breach of warranty, breach of contract, negligence, strict tort or any other legal theory. Damages that ProSoft or its Dealer will not be responsible for included, but are not limited to: Loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; loss of data; cost of capital; cost of any substitute equipment, facilities, or services; downtime; the claims of third parties including, customers of the Purchaser; and, injury to property.

** Some areas do not allow time limitations on an implied warranty, or allow the exclusion or limitation of incidental or consequential damages. In such areas, the above limitations may not apply. This Warranty gives you specific legal rights, and you may also have other rights which vary from place to place.

### *8.3.7 Time Limit for Bringing Suit*

Any action for breach of warranty must be commenced within 39 months following shipment of the Product.

### 8.3.8 No Other Warranties

Unless modified in writing and signed by both parties, this Warranty is understood to be the complete and exclusive agreement between the parties, suspending all oral or written prior agreements and all other communications between the parties relating to the subject matter of this Warranty, including statements made by salesperson. No employee of ProSoft or any other party is authorized to make any warranty in addition to those made in this Warranty. The Customer is warned, therefore, to check this Warranty carefully to see that it correctly reflects those terms that are important to the Customer.

### 8.3.9 Allocation of Risks

This Warranty allocates the risk of product failure between ProSoft and the Customer. This allocation is recognized by both parties and is reflected in the price of the goods. The Customer acknowledges that it has read this Warranty, understands it, and is bound by its Terms.

### 8.3.10 Controlling Law and Severability

This Warranty shall be governed by and construed in accordance with the laws of the United States and the domestic laws of the State of California, without reference to its conflicts of law provisions. If for any reason a court of competent jurisdiction finds any provisions of this Warranty, or a portion thereof, to be unenforceable, that provision shall be enforced to the maximum extent permissible and the remainder of this Warranty shall remain in full force and effect. Any cause of action with respect to the Product or Services must be instituted in a court of competent jurisdiction in the State of California.

# Index