*GE Medical Systems*

# Technical Publications

## Direction 2168924

**Revision 1**

# GEMS WirelessLAN Service Manual



**Operating Documentation**

# CONTENTS

# REVISION HISTORY

**1December, 1997Final draft.**

LIST OF EFFECTIVE PAGES

| PAGE NUMBER | REVISION NUMBER | PAGE NUMBER | REVISION NUMBER | PAGE NUMBER | REVISION NUMBER |
|---|---|---|---|---|---|
| Cover | 0 | 6-1 | 0 | C-1 to C-2 | 0 |
| Inside Cover | 0 | 6-2 | blank | D-1 to D-5 | 0 |
| i to v | 0 | 7-1 to 7-2 | 0 | D-6 | blank |
| 1-1 to 1-4 | 0 | 8-1 to 8-2 | 0 | Glossary-1 to Glossary-3 | 0 |
| 2-1 to 2-2 | 0 | A-1 | 0 | Glossary-4 | blank |
| 3-1 to 3-4 | 0 | A-2 | blank | Index-1 to Index-3 | 0 |
| 4-1 to 4-8 | 0 | B-1 | 0 | Index-4 | blank |
| 5-1 to 5-12 | 0 | B-2 | 0 | | |
| | | | | | |
| Cover | 1 | 7-1 to 7-16 | 1 | B-2 | blank |
| Inside Cover | 1 | 8-1 to 8-2 | 1 | C-1 to C-2 | 1 |
| i to v | 1 | 9-1 to 9-4 | 1 | D-1 to D-4 | 1 |
| 1-1 to 1-4 | 1 | 10-1 to 10-4 | 1 | Glossary-1 to Glossary 3 | 1 |
| 2-1 to 2-4 | 1 | 11-1 to 11-2 | 1 | Glossary 4 | blank |
| 3-1 to 3-4 | 1 | 12-1 to 12-4 | 1 | Index-1 to Index-3 | 1 |
| 4-1 to 4-10 | 1 | A-1 | 1 | Index-4 | blank |
| 5-1 to 5-8 | 1 | A-2 | blank | | |
| 6-1 to 6-12 | 1 | B-1 | 1 | | |

# Chapter 1
# Preface

## Section 1
## Quick Help

| If you need help... | See... |
|---|---|
| Installation | “Quick Reference” on page 2-1. |
| Network design | “Wireless Networking Tutorial” on page 7-1. |
| On-line help | “2-3 Technical Support” on page 1-2. |
| Technical support | “2-3 Technical Support” on page 1-2. |
| Quick reference | “Quick Reference” on page 2-1. |

## Section 2
## General Information

### 2.1 Trademarks

**Windows NT**, **Windows 95** and **Windows for Workgroups** are trademarks of Microsoft Corporation. **NetWare** is a trademark of Novell, Inc. **GE MEDICAL SYSTEMS** and all other trademarks are the property of their respective owners.

### 2.2 Limited Warranty, Disclaimer, Limitation of Liability

For a period of one (1) year from the date of purchase by the retail customer, GE Medical Systems warrants the WirelessLAN against defects in materials and workmanship. GE Medical Systems will not honor this warranty if there has been any attempt to tamper with the unit.

This warranty does not cover and GE Medical Systems will not be liable for any damage or failure caused by misuse, abuse, acts of God, accidents, or other causes beyond GE Medical Systems control, or claim by other than the original purchaser.

In no event shall GE Medical Systems be responsible or liable for direct, indirect, special, incidental or consequential damages including, but not limited to those arising:

- From the use of the product.

From the loss of use, revenue or profit of the product.

-or-

- As a result of any event, circumstance, action, or abuse beyond the control of GE Medical Systems.

**GE Medical Systems makes no warranty, express, implied (including but not limited to warranties of merchantability and fitness for intended purposes), or statutory, other than the foregoing express warranty.**

- Wireless bridges with long cable patch antenna

Failure to submit a claim under this warranty within ten (10) days following the expiration of the one-year (1) warranty shall be conclusive proof that the product is in every respect as warranted and shall release GE Medical Systems from any and all claims for damages. In the event you submit a timely claim and GE Medical Systems finds that the product is defective, please note that your sole and exclusive remedy shall be the repair or replacement of the product.

## 2.3 Technical Support

If you are having a problem using the WirelessLAN and cannot resolve it with the information in this manual, gather the following information and contact the GE Medical Systems Online Center:

- What kind of network are you using?
- What were you doing when the error occurred?
- What error message did you see?
- Can you reproduce the problem?
- What version of the device are you using?

To reach GE Medical Systems Online Center, call **1-800-522-6752**.

## 2.4 FCC Disclaimer

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.


**Any changes or modifications to the Wireless Bridges device or the antenna not expressly approved by GE Medical Systems will void the user's authority to operate the equipment.**

# Section 3
# Documentation Overview

The user's manual contains:

- An installation guide – See "Quick Reference" on page 2-1.
- Quick start up instructions – See "Quick Start" on page 2-1.
- Wireless tutorials – See "Wireless Networking Tutorial" on page 7-1.

## 3.1 Conventions Used in the Manual

The names of forms and menu items in the user's manual are in italics. Commands which you enter display in `monospace font (Courier new)`. Most activities in GE Medical Systems Wireless products can be performed with the mouse as well as with the keyboard.

## 3.2 Tips on Using Help

To "**save your place**" at various help topics to which you refer often, **place a bookmark** at that location to make it more easily and quickly accessible in the future. To do so, choose *Define* from the *Bookmark* menu on the *Help* window. You are then prompted to give it a name. You are free to choose any name or click *OK* to accept the default name (the topic title) that appears in the dialog box. The name you choose is added to the *Bookmark* menu in *Help*; select it from the menu at any time to display that particular *Help* screen.

To "**add notes to yourself**" in conjunction with a particular *Help* screen, choose *Annotate* from the *Edit* menu. Enter your text in the box that appears and then select *Save.* A paper clip icon appears at the beginning of the *Help* topic. To view your annotation, click on the paper clip icon (or press <Tab> to highlight the paper clip icon and then press <Enter>). When you finish viewing your annotation, select the *Cancel* button.

To "**keep the *Help* screen visibl**e" while you are working on a procedure, choose *Always on Top* from the *Help* menu. This keeps the *Help* window visible until you "put it away" by choosing *Close* from the *Help* screen *File* menu.

For more information on using *Help*, choose "*How to Use Help*" from the *Help* menu.

THIS PAGE INTENTIONALLY LEFT BLANK

# Chapter 2
# Quick Reference

## Section 1
## Quick Start

This section of the manual is for the experienced user who needs minimal help getting a basic wireless system to function.

### 1.1 System Environment Requirements

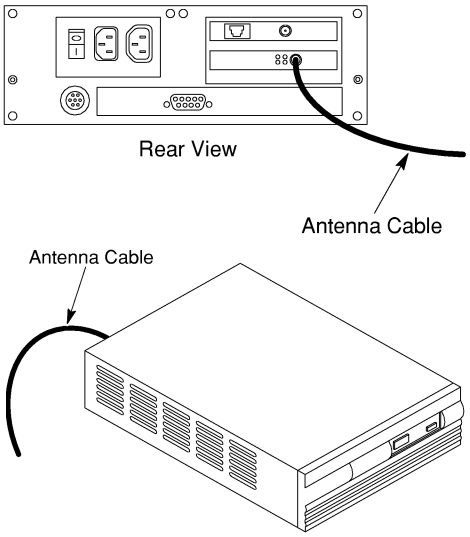
- Two Ethernet cable drops on different LAN segments (either 10BASET or 10BASE2).
- One AC power outlet for each wireless bridge.

## Section 2
## What WirelessLAN Is

The WirelessLAN is a wireless access point for network backbones. It has several members for hospital to mobile van LAN connectivity:

- WirelessLAN bridge for installation in hospital and mobile van.
- Long cable for antenna.
- Patch antenna for range to 1000 feet
- Transition and network cables.

# Section 3
# Wireless Point-to-Point Bridge Product Package




Hospital Subsystem

- Wireless Bridge
- Transition Cable
- Antenna Cable
- Patch Antenna
- 75 Foot Shielded Antenna Cable

Mobile Van Subsystem

- Wireless Bridge
- Transition Cable
- Antenna Cable (20 ft.)
- Patch Antenna
- UTP Crossover Cable
- UTP Transceiver

Optional Antenna Kit Subsystem

- Antenna Cable
- Patch Antenna
- T-Connector

Miscellaneous

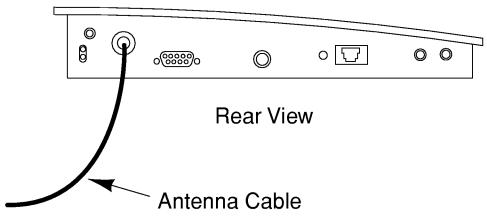
- Two 3.5" disk containing software labeled “Wireless Master”
- Two 3.5" disk containing software labeled “Wireless Station”
- Two 3.5" disk containing configuration software labeled “Configuration Tool”
- Two floppy disk drive covers
- Two patch antennas
- Two WirelessLAN user’s manual
- Two transition cables for bridge units
- One 10 BaseT Category 5 crossover network cable.
- One 10 BaseT-AUI transceiver
- One on-line help diskette
- Two power cords which are intended for use in the United States of America. For continued compliance with harmonized standards, an appropriate approved HAR power cord should be used with the device in countries other than the United States of America.
- Two BNC “T” adapters

If any of these items are missing or damaged, please contact your reseller or GE Medical Systems Online Center.

# Section 4
# Wireless Access Point Product Package

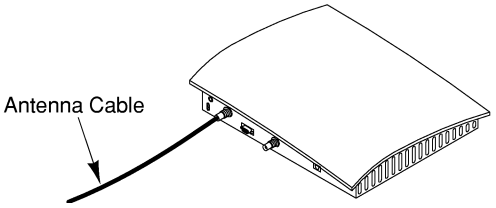
Hospital Bridge

- Antenna Cable
- Patch Antenna
- 75 Foot Shielded Antenna Cable




Mobile Van Subsystem

- Wireless Bridge
- Antenna Cable (20 ft.)
- Patch Antenna
- UTP Crossover Cable
- UTP Transceiver




Optional Antenna Kit Subsystem

- Antenna Cable
- Patch Antenna
- T-Connector

Miscellaneous

- Two Wireless Access Point User's Manuals
- Two 12 Volt DC Power Supplies
- Two BNC "T" adapters

THIS PAGE INTENTIONALLY LEFT BLANK

# Chapter 3
# Wireless Point-to-Point Bridge Quick Installation

## Section 1
## Introduction to Installation

You may use the quick installation steps if the following conditions are true:

- There is only one pair of the device operating in the same area.
- You use *all* the software default values (*MASTER, domain 0*).
- You do not have IP traffic on the network requiring you to change the IP addresses of the wireless bridge.

If your installation meets the preceding criteria, continue the installation by doing the following:

1. Insert the diskette labeled “Wireless Master” into the front of the device you have selected as the Master, and “Wireless Station” into the front of the device you have selected as the station.
2. Firmly screw the end of the antenna cable onto the antenna connector at the back of each device clockwise.

*Note* *FCC regulations mandate that the wireless bridge antenna not be alterable. Therefore, GE Medical Systems uses a custom antenna connector. Do not attempt to use a different antenna or you may damage the connector and the wireless unit.*

3. Attach an Ethernet cable to the Ethernet port on the back of each wireless device.
4. Plug the power cable into the back of each wireless device and into an AC power outlet.
5. Turn the wireless bridge on. The power switch is found on the back of the bridge.
6. Watch the floppy drive LED to see that the disk is being accessed when power is applied.
7. Install the floppy drive cover.

# Section 2
# Antenna Mounting

WirelessLAN products are available with various antenna types. Refer to the instructions included in each antenna kit for details on mounting the antenna.

For optimum performance, locate the antennas as close to a clear line of sight as possible. Make sure there are no large obstructions such as hills or buildings between the antennas.

*Note* *The range is greatly affected by the quality and length of the antenna cable. For optimum performance, use the shortest antenna cable lengths possible and extend the Ethernet cable to the wireless device whenever possible.*

For indoor installations, it is best to point the antennas at each other through a window. Make sure the windows do not have a metallic coating, because this can significantly reduce the range.

For outdoor installation it is best to mount the antennas on an antenna mast or on an outside wall. Be sure to ground the antennas and antenna masts on all rooftop installations.

*Note* *It is **strongly recommended** that a licensed electrician install all outdoor antennas to insure compliance with U.S. Consumer Product Safety Commission standards and National Electrical codes. Refer to "Appendix C" on page C-1 for more information on safety.*

You may also choose to bypass the setup program and follow the instructions in the following section to install the wireless device software for your network operating system.

Refer to GEMS WirelessLAN Pre-Installation manual (Direction 2168925).

# Job Card 001 WIRELESS ANTENNA INSTALLATION ON MOBILES 1 of 1

The wireless system antenna will be installed at the factory by the van manufacturer on a new van. Field installations can be done by either calling the van manufacturer service department for an installation cost or having the GE field engineer install it by the following procedure:

1. Find a good location for the antenna lead to pass through the wall at the highest most forward position on the door side of the mobile van. Make sure that it clears the van ducts and GE equipment. Also check to see if there are any electrical outlets below the hole. There should be none to avoid any possibility of drilling into van wiring.


**DISCONNECT ALL POWER BEFORE DRILLING!**

2. Drill a 3/16" diameter hole saw to drill through. (You should now see an outside aluminum skin and an inside aluminum skin separated by a foam core.)
3. Move to the outside and push the antenna lead through the hole. Position the antenna in the desired location and mark the four antenna mounting hole locations. It should be centered above the new 3/4" hole.
4. Drill four 3/16" diameter holes through the outside skin of the van as marked.
5. Mount the antenna with four 3/16" diameter x 1/4" long aluminum “Pop Rivets”.
6. Mark the position of the outside and inside van surface on the antenna cable. Wrap the area between these marks with black plastic electricians tape until the outside diameter fits snugly into the 3/4" hole.
7. Position the tape until the outside of the van wall and the outside of the tape are flush. Apply a coating of white silicon RTV to the outside of the tape, cable, and the edge of the aluminum skin.

You may now follow the system connection directions to complete the installation.

A second optional antenna may be installed on the opposite side of the van when required for sites that have opposite side base stations.

List of materials and tools required for the installation:

1. (8) 3/16" diameter aluminum “Pop Rivets” (4 spares)
2. (1) 3/16" diameter drill bit
3. (1) Roll black plastic electricians tape
4. (1) 3/4" diameter hole saw
5. (1) Tube white silicon RTV
6. “Pop Rivet” installation tool

# Job Card 002 — WIRELESS POINT-TO-POINT BRIDGE INSTALL — 1 of 1

1. Insert the disk labeled “Wireless Master” into the disk drive of the device which is to be the master and the disk labeled “Wireless Station” into the disk drive of the device which is to be the station.
2. Attach the antenna, power cord and Ethernet cable to the back of each device.
3. Plug the power cord into an outlet and turn the wireless bridges on. The power switch is located on the back of the bridge.
4. Copy the configuration software to your computer.
5. Attach a null modem cable from the serial port of the computer to the Local Management Port located on the back of the wireless unit.
6. When the wireless unit has finished booting up, exit to DOS and change to the directory in which the configuration software is located. Edit the SLIP.BAT file, replacing the *<INT>* and *<I/O>* values with those that correspond to the COM port on the computer being used to configure the wireless unit.

The batch file is formatted as follows:

`-SLIP8250 0X60 SLIP` **<INT> <I/O>** `9600`

| Port | **<INT>** | **<I/O>** |
|---|---|---|
| COM1 | 4 | 0x3F8 |
| COM2 | 3 | 0x2F8 |
| COM3 | 4 | 0x3E8 |
| COM4 | 3 | 0x2E8 |

7. Run the SLIP.BAT file and then the CFG.EXE file.
8. When the *RangeLINK Configuration Tool* screen appears, press <ENTER>.
9. Enter the *Configure RangeLINK* sub-menu and set the following parameters:
   - Station type: Master or Station
   - Domain: 5
   - Set security ID: test
10. Enter the *Configure TCP/IP* menu and set the following parameters:
    - IP Address: the IP address assigned to the Wireless unit
    - Subnet Mask: the subnet mask of the Wireless unit
11. Reset the RangeLINK.
12. Exit the configuration utility.

# Chapter 4
# Wireless Access Point 2 Quick Installation

# Job Card 001 WIRELESS ANTENNA INSTALLATION ON MOBILES 1 of 1

The wireless system antenna will be installed at the factory by the van manufacturer on a new van. Field installations can be done by either calling the van manufacturer service department for an installation cost or having the GE field engineer install it by the following procedure:

1. Find a good location for the antenna lead to pass through the wall at the highest most forward position on the door side of the mobile van. Make sure that it clears the van ducts and GE equipment. Also check to see if there are any electrical outlets below the hole. There should be none to avoid any possibility of drilling into van wiring.


**DISCONNECT ALL POWER BEFORE DRILLING!**

2. Drill a 3/16" diameter hole saw to drill through. (You should now see an outside aluminum skin and an inside aluminum skin separated by a foam core.)
3. Move to the outside and push the antenna lead through the hole. Position the antenna in the desired location and mark the four antenna mounting hole locations. It should be centered above the new 3/4" hole.
4. Drill four 3/16" diameter holes through the outside skin of the van as marked.
5. Mount the antenna with four 3/16" diameter x 1/4" long aluminum “Pop Rivets”.
6. Mark the position of the outside and inside van surface on the antenna cable. Wrap the area between these marks with black plastic electricians tape until the outside diameter fits snugly into the 3/4" hole.
7. Position the tape until the outside of the van wall and the outside of the tape are flush. Apply a coating of white silicon RTV to the outside of the tape, cable, and the edge of the aluminum skin.

You may now follow the system connection directions to complete the installation.

A second optional antenna may be installed on the opposite side of the van when required for sites that have opposite side base stations.

List of materials and tools required for the installation:

1. (8) 3/16" diameter aluminum “Pop Rivets” (4 spares)
2. (1) 3/16" diameter drill bit
3. (1) Roll black plastic electricians tape
4. (1) 3/4" diameter hole saw
5. (1) Tube white silicon RTV
6. “Pop Rivet” installation tool

# Job Card 003 WIRELESS ACCESS POINT 2 INSTALL 1 of 2

## Master Configuration

1. Mount the access point at a suitable location.
2. Attach the antenna to the back of the wireless device.
3. Connect the access point to your Ethernet LAN using either the 10BaseT or 10Base2 connector.
4. Connect the 12-volt DC power supply to the access point. The top LED on the front of the access point will glow orange to indicate the unit is powered.
5. Attach a null modem cable from the serial port of the computer to the Serial Port on the back of the Access Point 2.
6. When the wireless unit has finished booting up, open a terminal session on the computer using the instructions on page 4-5 for Windows 3.1 or on page 4-7 for Windows 95.
7. In the terminal program, press <ENTER>. You should see the following menu:

| Main Menu | |
|---|---|
| Selection | Description |
| 1 | Configuration Menu |
| 2 | Statistics Menu |
| 3 | Status Menu |
| 4 | Download Menu |
| 5 | Diagnostics Menu |
| 6 | Reset Access Point |
| Enter a selection or <ESC> for previous menu - > | |

*AMP Wireless Access Point 2 Main Menu.*

8. Type 1 for the configuration menu and press <ENTER>.
9. Type 1 for the TCP/IP menu and press <ENTER>.
10. For the Unit on the LAN side (referred to as the MASTER), enter a valid IP Address, a valid Subnet Mask, a valid Default Gateway Address, and change Send BOOTP at boot time to false.
11. Press <ESC> to go to the Configuration Menu.
12. Type 2 to go to the Filter Menu.
13. Change selections 1–11 to not filtering.
14. Press <ESC> to go back to the Configuration Menu.
15. Press 4 to go to the Radio Configuration Menu.
16. Change the Configured Domain to 5.
17. Type 14 to Reset the Radio.
18. Repeatedly press <ESC> until you are back at the Main Menu.
19. Select 6 to Reset the Access Point.

# Job Card 003 — WIRELESS ACCESS POINT 2 INSTALL — 2 of 2

## Station Configuration

1. Mount the access point at a suitable location.
2. Attach the antenna to the back of the wireless device.
3. Connect the access point to your Ethernet LAN using either the 10BaseT or 10Base2 connector.
4. Connect the 12-volt DC power supply to the access point. The top LED on the front of the access point will glow orange to indicate the unit is powered.
5. Attach a null modem cable from the serial port of the computer to the Serial Port on the back of the Access Point 2.
6. When the wireless unit has finished booting up, open a terminal session on the computer using the instructions on page 4-5 for Windows 3.1 or on page 4-7 for Windows95.
7. In the terminal program, press <ENTER>. You should see the following menu:

| Main Menu | |
|---|---|
| Selection | Description |
| 1 | Configuration Menu |
| 2 | Statistics Menu |
| 3 | Status Menu |
| 4 | Download Menu |
| 5 | Diagnostics Menu |
| 6 | Reset Access Point |
| Enter a selection or <ESC> for previous menu - > | |

*AMP Wireless Point Main Menu*

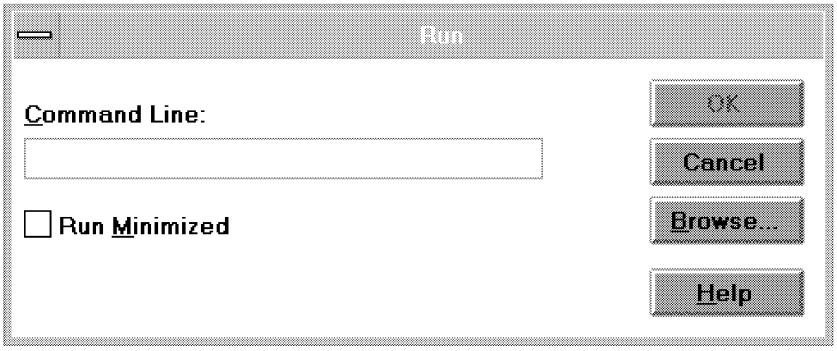
8. Type 1 for the Configuration Menu and press <ENTER>.
9. Type 1 for the TCP/IP menu and press <ENTER>.
10. Enter a valid IP Address, a valid Subnet Mask, a valid Default Gateway Address, and change Send BOOTP at boot time to false.
11. Press <ESC> to go to the Configuration Menu.
12. Type 2 to go to the Filter Menu.
13. Change selections 1–11 to not filtering.
14. Press <ESC> to go back to the Configuration Menu.
15. Press 4 to go to the Radio Configuration Menu.
16. Type 5 to change the Configured Station Type to Station.
17. Change the Configured Domain to 5.
18. Type 11 to Reset the Radio.
19. Repeatedly press <ESC> until you are back at the Main Menu.
20. Select 6 to Reset the Access Point.

# Section 1
# Using Windows 3.1 Terminal

The following instructions describe how to launch the communication package with Windows 3.1 Terminal.

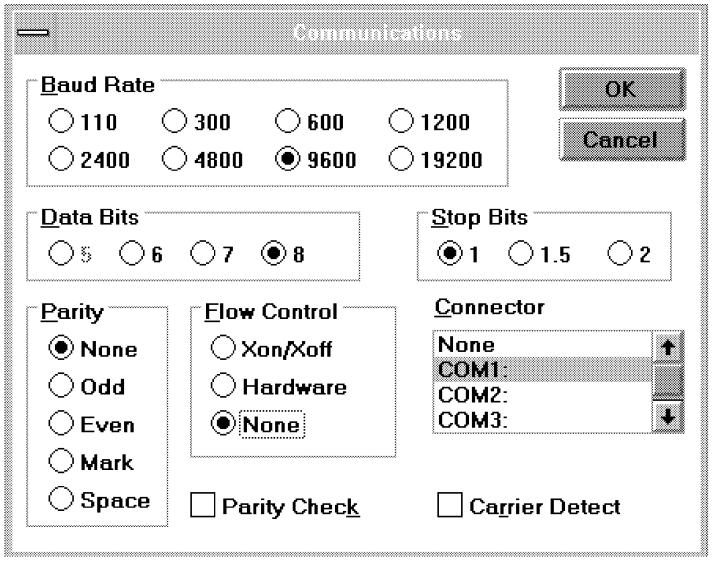
1. Make sure that your computer is connected to the Wireless Access Point Terminal port. Refer to page 6–2.
2. In the *Program Manager*, select *File*/*Run*. The *Run* window is displayed.

Illustration 4-1
Run Window



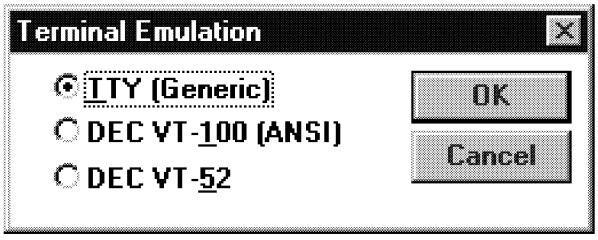

3. Type **`terminal`** in the *Command Line*.
4. Click the `OK` button. The *Terminal* screen is displayed.
5. From the *Terminal* menus, select *Settings*/*Communications*. The *Communications* window is displayed.

Illustration 4-2
Default Communications window



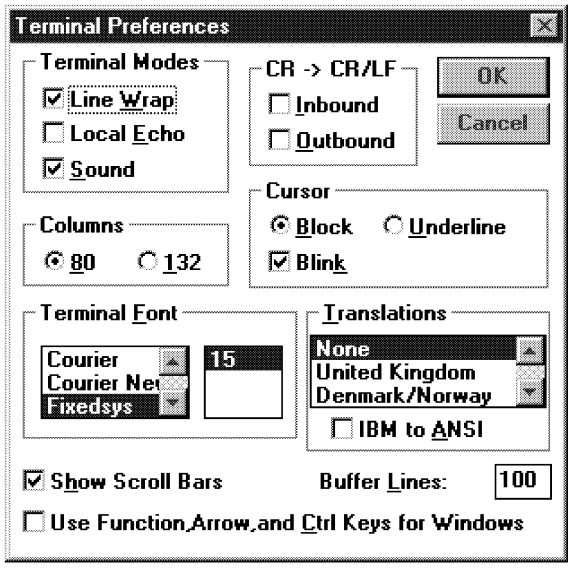
6. Select:
   9600 bits per second
   8 data bits
   1 stop bit
   No parity
   No flow control
   the appropriate connector (usually COM1 or COM2)
7. Click the OK button.
8. Select *Settings/Terminal Emulation*. The *Terminal Emulation* window is displayed.

Illustration 4-3
Default Terminal Emulation window




9. Click the circle next to TTY (Generic)
10. Click the OK button.
11. Select *Setting/Terminal* Preferences. The Terminal Preferences window appears.

Illustration 4-4
Terminal Preferences window




12. Verify the Use Function, Arrow, and Ctrl Keys for Windows box is **NOT** checked.
13. Click the OK button.

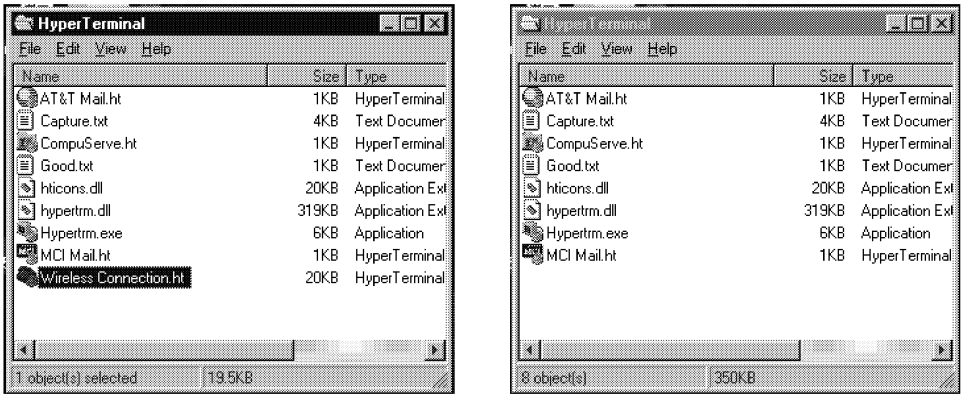
Verify that the Access Point has power and press <ENTER>. The Main Menu should appear. If it doesn't, wait 1–2 minutes for the Access Point to finish booting, and then press <ENTER>.

# Section 2
# Using Windows 95 HyperTerminal

The following instructions describe how to launch the communication package with Windows 95 HyperTerminal.

1. Make sure your computer is connected to the Terminal port.
2. Click *Start/Programs/Accessories/HyperTerminal*. A *HyperTerminal* window appears.

Illustration 4-5
HyperTerminal window



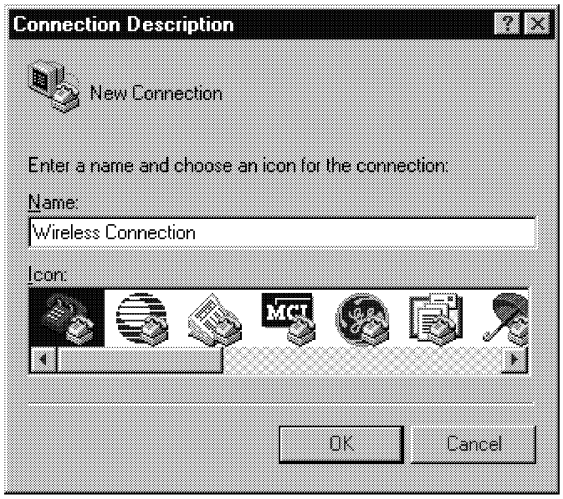

Wireless Connection Icon | No Wireless Connection Icon

3. If a Wireless Connection icon appears, double click it.

   **OR**

   If a Wireless Connection icon does NOT appear, double click *HyperTerm.exe* and go to step 4.
4. In the *Name* field, type **`Wireless Connection`**.
5. In the *Icon* field, click any icon.

Illustration 4-6
Sample Connection Description Window

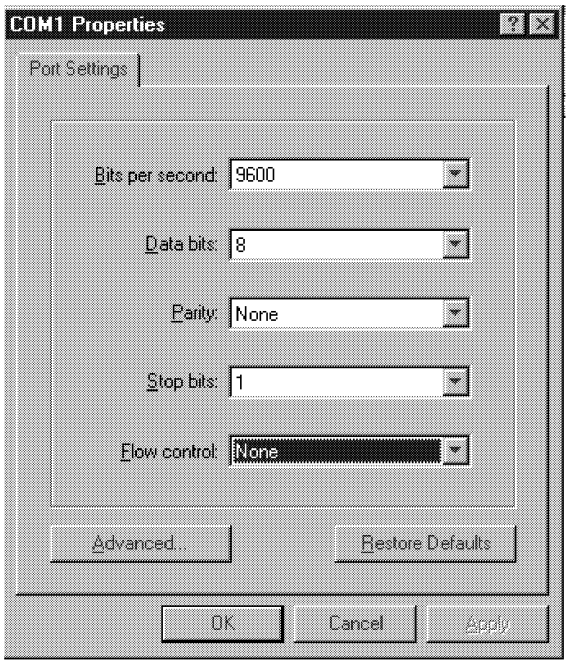



6. Click the **OK** button. The Phone Number window appears.

Illustration 4-7
Phone Number window

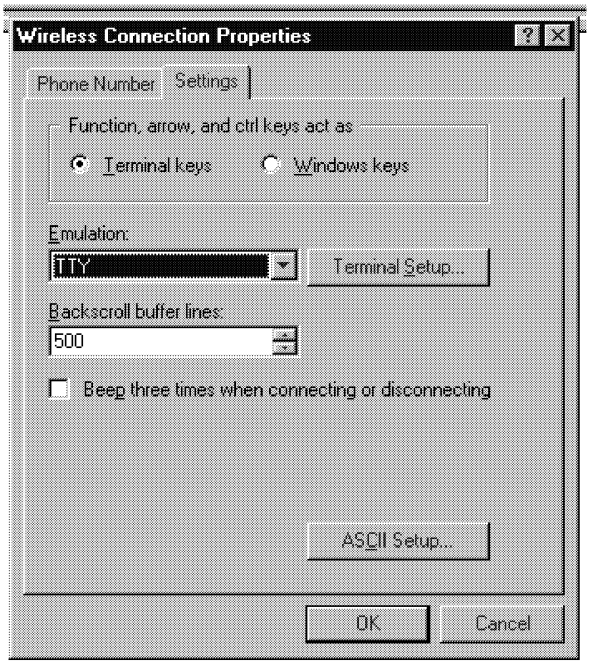

7. In the *Connect Using* field, select the appropriate communications port (usually COM1 or COM2).
8. Click the **OK** button. The *Comm Properties* window appears.

Illustration 4-8
Sample COM 1 Properties Window




9. Select the following settings:
   `9600` for *Bits per second*
   `8` for *Data bits*
   `None` for *Parity*
   `1` for *Stop bits*
   `None` for *Flow control*
10. Click the **OK** button. The *HyperTerminal* screen appears.
11. Select *File*/*Properties*. The *Wireless Connection Properties* window appears.

Illustration 4-9
Wireless Connection Properties Window




12. Verify: `TTY` is selected in the *Emulation* field.
13. In the *Function, arrow, ctrl keys act* field, select *Terminal Keys*.
14. Click the **OK** button.
    - Select the File/Save As
    - Click the Save button to save the Wireless Connection HyperTerminal Setup.
    - Verify that the Access Point has power and press <ENTER>.
    - The Main Menu should appear. If it doesn't, wait 1 – 2 minutes for the Access Point to finishing booting, and then press <ENTER>.

# Chapter 5
# Wireless Point-to-Point Bridge Configuration

## Section 1
## Overview of Wireless Bridges

Wireless radios use a radio technology called frequency hopping spread spectrum. This means that the radio signal is constantly moving from one frequency to another while sending packets of data. This hopping technique allows for multiple hopping patterns to be used in the same area and minimizes interference.

At any point in the configuration software, you can use either a mouse or keyboard to make selections. If you use a keyboard, press <ALT> followed by the highlighted letter to make a selection. Press the <TAB> key to cycle through the buttons displayed. Select *Help* to display information about the parameters you are setting.

## Section 2
## Configuring the Device

You may use the CFG program to either locally or remotely manage the device. If you are managing locally, choose *Local Wireless* after opening CFG. If managing remotely, choose the correct device once in CFG.

You configure the bridge if:

- There is more than one pair of bridges on this network, for example, in a roaming environment.
- You need to change the software default values, including IP addresses.
- You want to set security IDs on your network.

There are three ways to configure the bridge:

1. Locally via a null modem cable and the software, or
2. Remotely across the network using the software, or
3. Using an SNMP management package

## Section 3
## Locally (Out of Band)

You may use the DB-9 Local Management Port on the back of the unit to configure the wireless bridge. To configure locally, you need a female to female null modem RS-232 cable and a DOS-based PC with an available serial port.

1. Connect the null modem RS-232 cable between the Local Management Port and a free serial port on your PC.
2. If you are running the CFG tool from a DOS prompt in **Windows**, load WINPKT.COM before you enter **Windows** using the command:

   ```
   C:\> WINPKT 0X61
   ```

3. Copy the software from the "Configuration Tool" diskette to a directory on your PC's hard disk.

   ```
   C:\RLINK> COPY A:*.*(or B:)
   ```

4. One of the files you copied is a batch file called SLIP.BAT. This file may be edited with a text editor like MS-DOS's Edit. If you use a serial port on your PC other than COM2 (I/O 2F8, INT 3) to configure the unit, change the SLIP.BAT file to reflect the I/O Port Address and Interrupt settings of your COM port.
   - The batch file is formatted as follows:

     ```
     SLIP8250 0x60 SLIP <INT> <I/O> 9600
     ```

where **<INT>** and **<I/O>** refer to the Interrupt and I/O Port Address of the COM port:

| Port | <INT> | <I/O> |
|---|---|---|
| COM1 | 4 | 0x3F8 |
| COM2 | 3 | 0x2F8 |
| COM3 | 4 | 0x3E8 |
| COM4 | 3 | 0x2E8 |

For example, if your PC's available serial port is COM1, the batch file looks like this:

```
SLIP8250 0x60 SLIP 4 0x3F8 9600
```

5. Move to the directory which contains the batch file and the Configuration Software and run the batch file:

   ```
   C:\> CD\RLINK

   C:\RLINK> SLIP
   ```

6. Start the configuration software:

   ```
   C:\RLINK> CFG
   ```

7. Choose *Local Wireless* and chose *Select*. Proceed through the configuration boxes.

# Section 4
# Remotely (In Band)

The second configuration option is remotely across the wired network:

1. Install an Ethernet card in the PC you intend to use for configuration of your wireless device. This machine sends and receives IP packets during the configuration process.
2. If you run the CFG tool from a DOS prompt in **Windows**, load WINPKT.COM before entering **Windows** and use the command:

   ```
   C:\> WINPKT 0X61
   ```
3. Copy the software from the "Configuration Tool" diskette to a directory on your PC's hard disk:

   ```
   C:\RLINK> COPY A:*.*(or B:)
   ```
4. Edit the CFG.CFG file. This file assigns an IP address to the machine being used to configure the unit. It can be edited with a text editor like MS-DOS's Edit. If this is the first time you are configuring, leave the default setting in CFG.CFG. Once the unit has been assigned an IP address, re-edit the CFG.CFG file so that the configuration PC and the wireless device have unique IP addresses, but are on the same IP network. A sample CFG.CFG file looks like this:

   ```
   ip_address 192.0.1.14
   ```
5. Load a packet driver for your Ethernet card. A packet driver usually has parameters that are set on the driver load line. It does not require LSL or a NET.CFG configuration file like an ODI driver does. Skip to step 8.

Alternatively, you may use the Ethernet card's ODI driver rather than a packet driver. In this case, proceed with step 6.

6. To use the Ethernet card's ODI driver, copy this driver into the same directory as the Configuration Software.
7. Edit the NET.CFG file for this ODI driver using a text editor like MS-DOS's Edit and add the following information:

   ```
   LINK SUPPORT

   BUFFERS 6 1600
   ```
8. Add the following line as the **first frame type** in the Link Driver Section:

   ```
   FRAME ETHERNET_II
   ```
9. Load the ODI driver and the ODIPKT program. The ODI driver, the NET.CFG file, and the LSL.COM file ***must*** be in the same directory. For example, if the ODI driver is called ETHDRVR.COM, you load the following:

   ```
   C:\RLINK> LSL

   C:\RLINK> ETHDRVR

   C:\RLINK> ODIPKT
   ```
10. Start the configuration software:

    ```
    C:\RLINK> CFG
    ```

11. Choose *Default* from the list of wireless devices if this is an initial configuration and chose *Select*. If an IP address has already been assigned to the unit, select *Add* to add the unit to the list of Access Points with its IP address. Proceed through the configuration boxes.

*Note* *You may not run IP protocol stacks while the CFG program is loaded. You may run non-IP protocol stacks while the configuration software program is loaded. In order to do this, create entries for those stacks in the NET.CFG file and bind to the proper frame type.*

# Section 5
# Using an SNMP Management Package

You may choose to manage the bridge by any SNMP management package. The bridge supports the following managed objects:

- MIB-II (RFC 1213)
- IEEE 802.1d Bridge MIB (RFC 1493)
- Proxim Enterprise MIB

The Proxim Enterprise MIB is supplied in ASN.1 format on the diskette. The filename is PROXIM.MIB. Follow the instructions in your SNMP management package to incorporate enterprise-specific MIBs. Refer to the following table for user-configurable SNMP objects:

| | |
|---|---|
| Reset device | prAPReset |
| IP Address | prAPIPAddress |
| Channel | prRlCfgChannel |
| Subchannel | prRlCfgSubchannel |
| Domain | prRlCfgDomain |
| Security ID | prRlCfgSecurityID |
| Station Type | prRlCfgStationType |
| Master Name | prRlCfgMasterName |
| Spanning Tree Priority | dot1dStpPriority |
| Bridge Max Age | dot1dStpBridgeMaxAge |
| Bridge Hello Timer | dot1dStpBridgeHelloTime |
| Bridge Forward Delay | dot1dStpBridgeForwardDelay |
| Port Priority | dot1dStpPortPriority |
| Port Enabled | dot1dStpPortEnable |
| Port Path Cost | dot1dStpPortPathCost |
| Ethernet Port Priority | dot1dStpPortPriority |
| Ethernet Port Enabled | dot1dStpPortEnable |
| Ethernet Port Path Cost | dot1dStpPortPathCost |
| Aging Time | dot1dTpAgingTime |

The bridge currently supports two SNMP community strings: “Public”, which has “read-only” permission; and “Private”, which has full “read-write” permission.

*Note* *In order to use SNMP management, you first need to supply the unit with an IP address.*

# Section 6
# Using Configuration Software

The *Configure Wireless* button allows you to change all radio options including Station_type, Master_name, channel, subchannel, security ID, etc.

You also have the option to enable or disable "repeating". When repeating is enabled and the unit is configured as a Master, it repeats any signal coming from one station and destined for another station, if the two stations are both within range of the Master but not within range of one another. The advantage of repeating is the ability to double the effective range of the network. However, be aware that by enabling the repeating feature, the network performance dropped by as much as half the speed while repeating occurs.

Use the *Configure Bridge* button if you have other kinds of bridges on your network and you rely on the Spanning Tree algorithm. In general, the default parameters work, and modification is not necessary. For more information on the Spanning Tree Protocol, see "Wireless Networking Tutorial" on page 7-1.

You also have the option to enable or disable spanning tree support. If you have no other bridges on the network, or you have some method other than the IEEE 802.1d Spanning Tree Protocol to prevent loops on the network, you can choose to disable this feature.

# Section 7
# Configuring SNMP

Use the *Configure TCP/IP* button to change the IP address, Subnet Mask, and Default Gateway of the device.

If you configure the unit remotely and change the IP address, you may also need to change the CFG.CFG file on the configuring PC. The IP address of the unit and that of the configuring PC must be part of the same IP network.

IP Address indicates the IP address that will be assigned to the unit. It must be a unique number on the network.

*Subnet Mask* indicates the mask that is used to determine what network the unit is on.

If a packet is destined for an IP host or node that needs to cross a router, the unit looks for the *Default Gateway* to indicate where a router is that can send the packet to its proper destination.

In the following example, there is a wireless device, a router, and an Ethernet node. Your network administrator can help you fill in these fields:

- The IP Address of the Ethernet node is 192.0.2.7.
- The router is configured with two IP Addresses of 192.0.1.6 and 192.0.2.6.
- The wireless device is configured with an IP Address of 192.0.1.5, a Subnet Mask of 255.255.255.0 and a Default Gateway of 192.0.1.6.

# Section 8
# Configuring Filters

The filter configuration allows you to customize the type of traffic which is forwarded from the Ethernet network to the wireless network. When a box is checked, this indicates traffic that meets the corresponding filter characteristic (e.g., Protocol Type) are filtered OUT, and are not forwarded.

The **NON-WIRELESS ADDRESS FILTER**, when checked, prevents traffic which is destined to a non-broadcast, non-multicast, non-wireless address from being forwarded from Ethernet to wireless.

Do not use this filter for wireless bridges.

The **NOVELL IPX BROADCAST FILTERS** prevent IPX broadcasts of the specified types from being forwarded from Ethernet to the wireless device. Since RIP, SAP, and LSP broadcasts are of interest to routers and not end stations, these filters typically can be turned off.

The **PROTOCOL TYPE FILTERS** prevent traffic of a particular protocol type from being forwarded from Ethernet to the wireless device. When Other Types is checked, all types other than those listed are filtered out. Do not filter out the types of packets you know nodes need to receive. For example, if you use TCP/IP as a protocol on your network, do not filter IP/ARP traffic.

The **ARP FILTERARP** enables IP ARP broadcast filtering. When this filter is enabled, ARP broadcasts are forwarded from Ethernet to the wireless device only if the destination IP address is on the IP network defined by the IP Network Address and Subnet Mask fields.

**BROADCAST BANDWIDTH ALLOCATION** allows you to specify the maximum percentage of broadcast packets that are sent from the Ethernet network through the wireless bridges. There may be cases when you want to limit broadcast traffic. For example, if you know there are more broadcast packets than the 1.6 Mbps speed of the wireless device interface can handle, you might want to limit the broadcasts. As another example, to prioritize directed packets, you might want to free some of the buffers used for broadcast packets by setting this limit.

# Section 9
# Software Parameters

WirelessLAN adapters easily integrate into your existing network operating system. Each client on your network operates the same as any wired client PC except for the fact that wireless units share the same media or air space. The following wireless software parameters allow the wireless adapters to effectively share the same air space.

## 9.1 Station_Type (default=2)

In order for this system to work, in each subnetwork there must be one unit that coordinates the hops. This station is called the Master. It might help you to think of the Master as the conductor of a frequency hopping orchestra. The Master keeps time so all units know when to hop and what frequency to hop to.

Units classified as stations synchronize to the Master and follow its signal to learn what frequency in the pattern the Master is currently using.

An acting "Master" can be configured either as a Master or Alternate Master. Alternate Masters act either as a Master or a station. If an Alternate Master unit is unable to locate any other Master within range, it acts as a Master. If a Master is already present, then the Alternate Master acts as a station. When there are multiple Alternate Masters, they coordinate amongst themselves to determine who becomes the Master.

The Station_type settings are as follows:

Master= 2

Alternate Master= 1

Station= 0

The default setting is recommended for optimum performance.

## 9.2 Domain (default=0)

In order to establish communications, both units require the same domain number. Radios on different domains cannot communicate with each other. The domain is a software filter that does not affect the actual radio frequency or the frequency hop sequence.

If there are two or more WirelessLAN pairs within the same range, each pair should use a different domain. Each pair shares the 1.6 Mbps radio data rate when transmitting or receiving data.

The domain is a number between 0 and 15, with 0 being the default setting.

## 9.3 Channel (default=1)

Each Master can select one of 15 channels to establish communications with Stations. Each channel number sets a unique frequency hopping sequence allowing for multiple subnetworks with higher data rate transmission capability in the same air space. You may think of the channel as a pipe. In order to communicate, radios must be on the same channel and there must be one (and only one) Master that provides the timing for that channel.

There are 15 independent channels designated 1 through 15, with 1 being the default setting. This means that there are 15 different sequences of frequency hops. Each channel is at a different frequency at a different time. If there are two or more wireless device pairs within the same range, each pair should use a different channel. All stations use the same channel as the Master to which they are synchronized.

You need only set the channel on a Master or Alternate Master. Stations ignore the parameter if it is set.

## 9.4 Subchannel (default=1)

The subchannel is just a software code that is appended to each radio packet. It does not affect the frequency hopping sequence like a channel does. Use a subchannel if you need more than 15 Masters in the same coverage area and, therefore, all the channels are used.

For example, you can use channel 1, subchannel 1 for network A and channel 1, subchannel 2 for network B. The two networks will not communicate with one another; however, they still share the 1.6 Mbps pipe since they are both using channel 1.

The subchannels are designated 1 through 15, with 1 being the default setting.

You need only set the subchannel on a Master or Alternate Master. Stations ignore the parameter if it is set.

## 9.5 Master_name (optional)

This optional parameter of up to 11 characters specifies an alphanumeric name to simplify the identification of each Master in your network. You may not use spaces in the name.

You need only set the Master_name on a Master or Alternate Master. Stations ignore the parameter if it is set.

## 9.6 Security ID

To further improve the security of a wireless subnetwork, all units must have the same security ID, which is a specific number of alphanumeric characters. The security ID is used on all wireless products and all Station_types. This ID is encrypted and stored on the Proxim 7100 card itself, not in software. It cannot be accessed, but you may change it. If you do change it, however, you need to change the security ID on all other radios with which this one was communicating.

There are 1,048,576 unique choices for the security ID.

To change the security ID, use the CFG program. To set the security ID, refer to “Security” on page 8-1.

# Chapter 6
# Wireless Access Point 2 Configuration

## Section 1
## Overview to Configuration

Many of the operating parameters of the AMP Wireless Access Point 2 can be changed to optimize network performance. This process, called configuration, is described in this section.

The AMP Wireless Access Point 2 uses an internal flash memory that allows it to boot up as soon as power is applied. A default configuration is also contained in the flash memory, allowing the access point to operate immediately, assuming that any client terminals equipped with AMP Wireless adapters are also using their default parameters.

For some operating parameters, each access point on the network must have a unique setting. Therefore, because AMP Wireless Access Points are shipped identically configured, as soon as two or more access points are installed some configuration will be necessary.

There are four distinct ways to configure the AMP Wireless Access Point 2. One of these ways uses a “local” technique. That is, it allows you to configure the access point on the desktop (or wherever it is to be permanently mounted). The other three ways use a “remote” technique. That is, the access point is configured over your existing network.

**Local** – the local technique involves using a null modem cable to physically attach the access point to a PC running a terminal emulation package.

**Remote** – the remote techniques involve configuring the access point using either:

- A telnet session.
- An SNMP management package.
- A dial-up modem.

Generally, these remote techniques would be used for access points already installed in the network.

These four techniques are described below. Later sections describe the AMP Wireless Access Point 2 configuration menus and the software parameters that can be changed using these configuration techniques.

# Section 2
# Configuring the Access Point 2 Locally from a PC

You may use the DB-9 Local Management Port (Serial Port) on the back of the access point to configure the unit. To locally configure the AMP Wireless Access Point 2 you need a null modem RS-232 cable with a nine pin female connector on the access point side and a terminal or PC with an available serial port running a terminal application package.

*Note* *If you use a terminal application that has the option to check for the Carrier Detect signal before establishing a connection, configure the software to ignore Carrier Detect. Alternatively, verify that your null modem cable is a full handshake cable and pulls Carrier Detect high.*

1. Connect the null modem RS-232 cable between the access point Serial Port and a free serial port on your terminal or PC.
2. Configure the terminal or terminal emulation package following the directions from Chapter 4.
3. Apply power to the access point. During the boot process messages will be displayed on the terminal screen. When they are completed and you see the "Initialization Complete" message, press <ENTER> to enter the software *Main Menu* (see graphic below). If the unit was already turned on, you can press **<ENTER>** to display the *Main Menu*.

| Main Menu | |
|---|---|
| Selection | Description |
| 1 | Configuration Menu |
| 2 | Statistics Menu |
| 3 | Status Menu |
| 4 | Download Menu |
| 5 | Diagnostic Menu |
| 6 | Reset Access Point |
| Enter a selection or <ESC> for previous menu - > | |

*AMP Wireless Access Point 2 Main Menu*

*Note* *Depending on the access point's current settings, the order of the options in the menu tree may change slightly.*

# Section 3
# Configuring the Access Point 2 Remotely Using a Telnet Session

The second configuration option is remote configuration access the wired network.

*Note* *The AMP Wireless Access Point 2 is not manufactured with a default IP address. In order to telnet to the access point, you must first assign it a valid IP address for your network using a null modem cable configuration or a BOOTP server.*

1. From a wired client on your network, open a telnet session to the access point.

2. You will be prompted for a password if you previously enabled this option through the *TCP/IP Configuration Menu*.
3. You will enter the *Main Menu* (see graphic above).

# Section 4
# Configuring the Access Point 2 Remotely by SNMP (SNMP Model Only)

You may configure the AMP Wireless Access Point 2 using an SNMP management package. The access point supports the following MIBs:

- MIB-II (RFC 1213)
- IEEE 802.1d Bridge MIB (RFC 1493)
- Extended Ethernet MIB (RFC 1643)
- Proxim Enterprise MIB

Follow the instructions in your SNMP management package for incorporating enterprise-specific MIBs. The Proxim Enterprise MIB is supplied in ASN.1 format. It is available from the AMP web site: www.amp.com/networking.

# Section 5
# Configuring the Access Point 2 Remotely Using a Modem (SNMP Model Only)

The AMP Wireless Access Point 2 may be remotely configured via a dial-up modem. To allow for this type of configuration:

1. Configure the modem from a terminal or terminal emulation program at 9600 bps.
2. Issue the following commands to the modem:

| | |
|---|---|
| ATSO=1 | (Auto-answer after 1 ring) |
| AT&D0 | (Ignore DTR) |
| ATE0 | (No local echo) |
| ATQ1 | (Suppress results codes) |
| AT&W0 | (Store configuration in non-volatile memory |

1. Attach a modem via a straight-through cable to the access point.
2. From a remote modem, dial the phone number of the modem connected to the access point.
3. After the access point's modem has answered the phone, press <ENTER> on the terminal connected to the remote modem until you see the *Main Menu* tree (see graphic above).

# Section 6
# Configuration Menu

To configure the AMP Wireless Access Point 2, pick the *Configuration Menu* Option from the *Main Menu*.

| Configuration Menu | |
|---|---|
| Selection | Description |
| 1 | TCP/IP Configuration Menu |
| 2 | Filter Configuration Menu |
| 3 | Bridge Configuration Menu |
| 4 | Ethernet Configuration Menu |
| 5 | Radio Configuration Menu |
| 6 | Authorization Table Configuration Menu |
| 7 | SNMP Configuration Menu |
| 8 | Reset Access Point to Factory Defaults |
| 9 | Dump Configuration To Screen |
| Enter a selection or <ESC> for previous menu - > | |

*AMP Wireless Access Point 2 Configuration Menu*

# Section 7
# TCP/IP Configuration Menu

Use this option to change the TCP/IP parameters of the AMP Wireless Access Point 2. The *TCP/IP Configuration Menu* is shown below.

| TCP/IP Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | IP Address | 0.0.0.0 |
| 2 | Subnet Mask | 0.0.0.0 |
| 3 | Default Gateway Address | 0.0.0.0 |
| 4 | Send BOOTP at Boot Time | 0.0.0.0 |
| 5 | BOOTP Server (0.0.0.0 for Broadcast) | true |
| 6 | Telnet Access | 0.0.0.0 |
| 7 | Telnet Password | enabled |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Configuration Menu*

**IP Address** indicates the IP address that will be assigned to the AMP Wireless Access Point 2. It must be a unique number on the network. This parameter will not change until the access point is reset.

**Subnet Mask** indicates the mask that will be used to determine what network the AMP Wireless Access Point 2 is on. This parameter will not change until the access point is reset.

If a packet is destined for an IP host or node belonging to a different IP subnet, the AMP Wireless Access Point 2 will send IP packets to the **Default Gateway** (usually a router) for the packets to be routed to the proper destination. This parameter will not change until the access point is reset.

You can enable or disable the access point's ability to request its IP address from a BOOTP server at boot time (**Send BOOTP at BOOTP Time**), and you can supply IP address of that server (**BOOTP Server Address**).

You can enable or disable the ability to open a telnet session to the AMP Wireless Access Point 2 (**Telnet Access**) and set a password to control telnet access (**Telnet Password**).

# Section 8
# Filter Configuration Menu

Filter configuration allows you to customize the type of traffic forwarded from the Ethernet network to the AMP wireless network. None of these filters affect traffic flowing from the wireless clients to the wired backbone.

| Filter Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Filter Fixed nodes | filtering |
| 2 | Filter IP Packets | not filtering |
| 3 | Filter IPX Packets | not filtering |
| 4 | Filter NetBEUI Packets | not filtering |
| 5 | Filter AppleTalk Packets | filtering |
| 6 | Filter DECNet Packets | not filtering |
| 7 | Filter Other Packets | not filtering |
| 8 | Filter IPX RIP Broadcast Packets | filtering |
| 9 | Filter IPX SAP Broadcast Packets | filtering |
| 10 | Filter IPX LSP Broadcast Packets | filtering |
| 11 | Filter ARP Broadcast Packets | not filtering |
| 12 | ARP Filter Network Address | 0.0.0.0 |
| 13 | ARP Filter Subnet Mask | 0.0.0.0 |
| 14 | Broadcast Bandwidth Allocation % | 80 |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Filter Configuration Menu*

**Filter Fixed Notes** will prevent traffic which is destined for a non-broadcast, non-multicast, non-AMP wireless address from being forwarded from Ethernet to wireless. **Do not** use this filter when using the node address overwrite feature on AMP wireless stations.

The protocol type filters prevent traffic of a particular protocol type from being forwarded from Ethernet to AMP wireless. When "Other Types" is enabled, all types other than those listed will be filtered out. **Do not** filter out the types of packets you know AMP wireless nodes will need to receive. For example, if you use TCP/IP as a protocol on your wireless nodes, do not filter IP traffic. If you have Macintosh computers on your Ethernet network that send AppleTalk traffic only to each other, you may want to filter those packets from AMP wireless stations. The protocol type filters include **IP, IPX, NetBEUI, AppleTalk, DECNet**, and **Other** (none of the above).

The IPX broadcast filters (**RIP, SAL, LSP**, and **ARP**) prevent IPX broadcasts of the specified types from being forwarded from Ethernet to AMP wireless. Since RIP, SAP, and LSP broadcasts are of interest to routers and not end stations, these filters can typically be turned on, saving valuable bandwidth.

The **ARP Filter Network Address** and **ARP Filter Subnet Mask** enable IP ARP broadcast filtering. When these filters are configured, ARP broadcasts will be forwarded from Ethernet to AMP wireless only if the destination IP address is on the IP network defined by the ARP Filter Network Address and ARP Filter Subnet Mask fields.

**Broadcast Bandwidth Allocation** allows you to specify the maximum percentage of AMP wireless bandwidth that may be allocated for broadcast traffic. There may be cases when you want to limit broadcast traffic. As an example, to prioritize directed packets, you might want to reserve radio bandwidth for directed packets by setting this limit to less than 100%.

# Section 9
# Bridge Configuration Menu

The *Bridge Configuration Menu* is shown below.

| Bridge Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Aging Period (seconds) | 300 |
| 2 | Forwarding DB Usage Trap Threshold % | 100 |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Bridge Configuration Menu*

The **Aging Period** parameter specifies the time after which the learned physical address of the network node, which is stored in the Forwarding Database, is discarded. This address is dynamically acquired by the AMP Wireless Access Point 2 so that it can forward packets properly.

The **Forwarding DB Usage Trap Threshold** parameter specifies the percentage of learned database entries after which an SNMP trap will be sent. This parameter is only supported on the AMP Wireless Access Point 2 with SNMP, which has the capability of holding 2048 entries.

# Section 10
# Ethernet Configuration Menu

The *Ethernet Configuration Menu* is shown below.

| Ethernet Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Ethernet Port Administrative Status | enabled |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Ethernet Configuration Menu*

The only option in this menu, **Ethernet Port Administrative Status**, is only visible on the AMP Wireless Access Point 2 with SNMP. It corresponds to the SNMP MIB-II Administrative status parameter and can be used to bring the Ethernet interface back up after it has been disabled by an SNMP manager.

# Section 11
# Radio Configuration Menu

The *Radio Configuration Menu* is shown below.

| Radio Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Radio Port Administrative Status | enabled |
| 2 | Configured Channel | 1 |
| 3 | Configured Subchannel | 1 |
| 4 | Configured Domain | 0 |
| 5 | Configured Master Name | MASTER |
| 6 | Repeating Enabled | false |
| 7 | Delay Radio Reconfigure | false |
| 8 | MAC Optimize | auto |
| 9 | No Traffic Trap Threshold (seconds) | 0 |
| 10 | Radio Traffic Trap Threshold (%) | 100 |
| 11 | Radio Broadcast Trap Threshold (%) | 100 |
| 12 | Set Security ID | |
| 13 | Reset Radio | |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Radio Configuration Menu*

The **Radio Port Administrative Status** allows the various wireless parameters to be changed.

Each Master can select one of 15 **Channels** to establish communications with Stations. Each Channel number sets a unique frequency hopping sequence, allowing for multiple subnetworks with higher data rate transmission capability in the same air space. You may think of the Channel as a pipe. In order to communicate, radios must be on the same Channel and there must be one (and only one) Master that provides the timing for that Channel.

There are 15 independent Channels. This means that there are 15 different sequences of frequency hops. Each Channel is at a different frequency at a different time. For networks with multiple Masters (such as in a roaming environment), set each Master to a different channel. All Stations will determine their channel by the Master to which they are synchronized.

The **Subchannel** is a software code that is appended to each radio packet. It does not affect the frequency hopping sequence like a Channel does. Use a Subchannel if you need more than 15 Masters in the same coverage area and, therefore, all the Channels are used.

For example, you can use Channel 1, Subchannel 1 for Network A and Channel 1, Subchannel 2 for Network B. The two networks will not communicate with one another. They are, however, still sharing the 1.6 Mbps “pipe” since they are both using Channel 1.

In order to establish communications, all communicating stations must be configured with the same **Domain** number. Radios on different Domains cannot communicate with each other. The Domain is a software filter that does not affect the actual radio frequency or the frequency or the frequency hop sequence.

You may want to set everyone on your network to the same Domain. For larger wireless networks, use the Domain to establish roaming subnetworks throughout your building. For example, the Engineering Department may use Domain 2 and the Sales Department may use Domain 5. Then engineers can only roam within the geographical area mapped out by AMP Wireless Access Points with a Domain setting of 2.

The optional **Master Name** parameter specifies an alphanumeric name to simplify the identification of each Master in your network.

You may enable or disable the ability for the AMP Wireless Access Point 2 to repeat signals coming from one Station and destined for another Station. These two Stations must be out of range of one another but both in range of the access point for repeating to occur.

The **Delay Radio Reconfigure** parameter allows you to delay radio parameter changes from taking effect. You might want to enable this feature if you are wirelessly configuring the AMP Wireless Access Point 2, so that you do not lose communication when the parameters change.

For example, suppose you were changing an access point’s Domain from 0 to 1. If you did not use the Delay Radio Reconfigure parameter, when the Domain changed, the wireless client would no longer be able to communicate with the access point.

The **MAC Optimize** parameter can help improve throughput for small networks. The default setting of Auto causes the AMP Wireless Access Point 2 to determine the number of units synchronized to it and adjust this parameter accordingly. If you have 0 or 1 wireless node communicating with an access point, set this parameter to Very Light. If you have between 2 and 7 wireless nodes communicating with an access point at the same time, set this parameter to Light. In networks with more than 7 concurrent wireless users, set the parameter to Normal.

The **No Traffic Trap Period** specifies the number of seconds after which a No Traffic trap is sent via SNMP. This parameter is only available on the AMP Wireless Access Point 2 with SNMP.

The **Radio Traffic Trap Threshold** specifies a percentage of radio traffic after which a Radio High Usage trap is sent via SNMP. This parameter is only available on the AMP Wireless Access Point 2 with SNMP.

The **Radio Broadcast Trap Threshold** specifies a percentage of radio broadcast traffic after which a Radio High Usage trap is sent via SNMP. This parameter is only available on the AMP Wireless Access Point 2 with SNMP.

To further improve the security of a wireless subnetwork, each unit requires the same **Security ID** to establish communication. The Security ID is used on all AMP wireless products and all Station Types. This ID is encrypted and stored in the AMP Wireless Access Point 2 itself, not in software. It cannot be accessed but you may change it. If you do change it, however, you will need to change the Security ID on all other radios with which this one was communicating. The Security ID parameter can be up to 20 characters and is an empty string by default.

**Reset Radio** allows you to reset the radio contained in the AMP Wireless Access Point 2 without resetting the entire unit. This will cause any changes to the radio parameters which haven't yet taken effect (because the Delay Radio Reconfigure parameter is set) to take effect.

# Section 12
# Authorization Table Configuration Menu

The *Authorization Table Configuration Menu* is shown below.

| Authorization Table Configuration Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Authorization Table | |
| 2 | Authorization Table Usage Option | unused |
| 3 | Enable/Disable Unauthorized Addr. Trap | disabled |
| 4 | AP Authorization Config. Download Table | |
| 5 | Update Authorization Config. of all APs | |
| Enter a selection or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Authorization Table Configuration Menu*

For added security, you can use the **Authorization Table** to hold the MAC addresses of the wireless nodes that will be allowed or disallowed to connect to the Ethernet LAN through the AMP Wireless Access Point 2 with SNMP. These addresses are manually added and deleted. This is in addition to the Security ID already supported by the AMP wireless hardware. For example, if an AMP wireless client card is stolen, you can specifically disallow it access to the network.

The **Authorization Table Usage Option** determines if this table will include or exclude wireless users and if the table will be used at all. If you have not recently updated the table, you may want to disable usage until you can add all the proper entries. By default, it is disabled. The table can hold a maximum of 256 nodes.

You can also enable or disable an SNMP trap that will tell the SNMP manager an unauthorized user has tried to use the AMP Wireless Point 2.

The **Update Authorization Config. of All APs** parameter distributes the Authorization Table from this access point to all other access points on the network. This feature is useful in that you do not have to set the Authorization Table individually on all access points in the same network. Choose the AP Authorization Config. Download Table to watch progress of the distribution. In most cases, the distribution will take place so quickly that you will only see the final status of the distribution.

# Section 13
# SNMP Configuration Menu

The *SNMP Configuration Menu* is shown below.

SNMP Configuration Menu

| Selection | Description | Current Value |
|---|---|---|
| 1 | Enable/Disable SNMP | enabled |
| 2 | Read-Only SNMP Community | public |
| 3 | Read-Only SNMP Manager IP Address | 0.0.0.0 |
| 4 | Read/Write SNMP Community | private |
| 5 | Read/Write SNMP Manager IP Address | 0.0.0.0 |
| 6 | SNMP Trap Community | AccessPointTrap |
| 7 | Trap Target Address | 0.0.0.0 |
| 8 | Enable/Disable Authentication Traps | enabled |

Enter a selection or <ESC> for previous menu - >

*AMP Wireless Access Point 2 SNMP Configuration Menu*

You may configure and monitor the AMP Wireless Access Point 2 with SNMP using an SNMP management package.

This access point supports the following MIBs:

- MIB-II (RFC 1213)
- IEEE 802.1d Bridge MIB (RFC 1493)
- Extended Ethernet MIB (RFC 1643)
- Proxim Enterprise MIB

Follow the instructions in your SNMP management package for incorporating enterprise-specific MIBs. The Proxim Enterprise MIB is available at the AMP web site: www.amp.com/networking.

*Note* *The AMP Wireless Access Point 2 is not manufactured with a default IP address. In order to SMNP manage the access point, you must first assign it a valid IP address for your network using a null modem cable configuration or a BOOTP server.*

You may choose to configure the AMP Wireless Access Point 2 through the menu trees (local or remote) to set SNMP parameters before using an SNMP manager.

**Enable/Disable SNMP** allows you to enable or disable SNMP management of the access point.

The **Read-Only SNMP Community** parameter specifies a community supported by the AMP Wireless Access Point 2. Actions permitted by this community are "read-only" (GET and GET-NEXT). SET attempts using this community will result in rejection of the attempt with a general error response and the generation of an authentication trap (if so enabled).

The **Read-Only SNMP Manager IP Address** specifies the IP address of the SNMP manager which is permitted to use the Read-Only SNMP Community. An address of 0.0.0.0 indicates any manager may use this community.

The **Read-Write SNMP Community** parameter specifies a community supported by the AMP Wireless Access Point 2. Actions permitted by this community are "read-write" (GET, GET-NEXT and SET).

The **Read-Write SNMP Manager IP Address** specifies the IP address of the SNMP manager which is permitted to use the Read-Write SNMP Community. An address of 0.0.0.0 indicates any manager may use the community.

The **SNMP Trap Community** parameter specifies the community that will be used by the AMP Wireless Access Point 2 when generating TRAP Protocol Data Units to remote managers.

The **Trap Target Address** specifies the IP address of the device to which generated TRAP Protocol Data Units will be sent. A value of 0.0.0.0 disables trap generation.

**Authentication Traps** are sent to the Trap Target Address whenever anyone attempts to SNMP manage the AMP Wireless Access Point 2 with an invalid community or from an invalid community. You may enable or disable the sending of these traps.

# Section 14
# SNMP Supported Traps

The following traps are supported by the AMP Wireless Access Point 2 with SNMP and are sent to the SNMP manager defined by the Trap Target Address when they occur.

MIB II Traps

**Cold Start** – Sent when the access point powers on or reboots.

**Link Up** – Sent by each interface at start-up or after coming back up.

**Link Down** – Sent when the access point software cannot initialize or communicate with either interface.

**Authorization** – Sent to the network manager when someone tries to manage an access point with an invalid community.

Enterprise Specific Traps

**No Traffic** – Sent when set to a non-zero value and when the access point does not receive any traffic from other radios for the configured period of time. The time may be configured in the *Radio Configuration Menu.*

**Broadcast Threshold** – Sent if the radio broadcast traffic exceeds the limit set by the Radio Configuration parameter called Radio Broadcast Trap Threshold.

**Cache Table High Usage** – Sent when the cache table usage percentage has exceeded the limit set by the *Bridge Configuration Menu* parameter Forwarding DB Usage Trap Threshold. For example, if this limit were set to 50%, when the AMP Wireless Access Point 2 with SNMP knows 1024 (out of the 2048 possible) entries, it will send this trap message. Similarly, 512 entries would cause an AMP Wireless Access Point 2 Basic mode to send this trap.

**Radio High Usage** – Sent if the radio traffic has crossed the limit set by the Radio Configuration parameter called Radio Traffic Threshold.

**Serial Port Down** – Sent when the serial port of the access point is not working. The status of this port is check only at boot time.

**Unauthorized Usage Trap** – Sent when an unauthorized wireless user tries to attach to the network through the access point.

## Section 15
## Reset Access Point to Factory Defaults

Use this option to reset all the parameters to default values.

## Section 16
## Dump Configuration to Screen

This parameter displays the current configuration of the AMP Wireless Access Point 2 to the screen. You can save these settings using a screen snapshot program. If you contact the AMP Wireless Help Desk for assistance you may be asked to print this screen for troubleshooting purposes.

# Chapter 7
# Wireless Networking Tutorial

## Section 1
## Tutorial Introduction

The purpose of this section is to provide an overview of wireless networking technology, terminology and concepts so you can effectively design and implement wireless networks. This section is written for network designers and system administrators not familiar with wireless networking.

## Section 2
## Tutorial Organization

The following topics are reviewed:

- Radio Technology – The radio techniques that make wireless networking feasible.
- Wireless Range – Considerations for network design based on building design and construction.
- Site Surveys – Determining the impact of building design on network performance.
- Benchmarking – Techniques for assessing application performance.
- Roaming – Techniques for improving the range of desktop and portable computers.
- Licensed versus Unlicensed Operation.
- Network System Considerations – Using wireless technology with the variety of NOS available.
- Master/Alternate Master Configurations – Determining the best configuration to meet your application need.
- Network Architectures:
  - Simple Network.
  - Moderately Complex Network.
  - Peer-to-Peer.
- Spanning Tree Protocol Support.

# Section 3
# Radio Technology

The GE Medical Systems Wireless products family uses radio frequency (RF) signals to carry LAN data. You do not need to be an RF engineer to install, use or maintain wireless networks. It is helpful if you understand some of the basic concepts employed in wireless systems.

## 3.1 Straight Line Signals

Signals travel in a straight line, but bounce off metal objects. Thus, signals may take several "bounces" before they arrive at their destinations.

## 3.2 Penetration

The GE Medical Systems WirelessLAN operates at 2.4 GHz. Signals at these frequencies pass through most non-metallic objects such as walls, ceilings and floors. Metal objects such as heating and air conditioning ducts interfere with line of sight transmissions at these frequencies and can provide "dead" spots in the reception of signals. Thick concrete structures reduce signal strength.

## 3.3 Safety

GE Medical Systems WirelessLAN produce a donut-shaped radio pattern around the antenna in all three planes. The power level is 0.1 watt. (The typical coverage is several hundred feet in all directions.) A microwave oven operates in the same frequency range with approximately 1,000 watts in a confined area.

## 3.4 Coverage

Radio signals radiate from wireless products in a three-dimensional circular pattern. The pattern resembles a donut with the antenna at the center. Because of this pattern, these products work as well between floors of buildings as within floors, as long as there is no shielding by building components.

## 3.5 Polarization

Signals at very high frequencies must be polarized. The transmit and receive planes must be the same or signals become severely reduced. Generally, antennas are vertically polarized. They either point straight up or straight down. All units should be similarly polarized.

## 3.6 Frequency Hopping

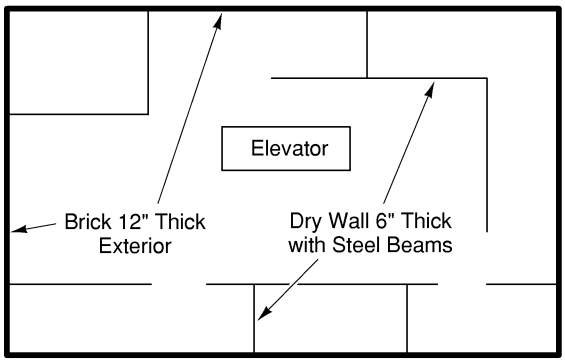
Rather than transmit on a single frequency that could be tuned in as you do with your FM radio, wireless products transmit and receive on many frequencies using spread spectrum techniques. Spread spectrum techniques are employed because of the following features:

- Interference reduction – A unit transmits on one frequency at a time and then moves to another frequency. If interference exists, it can only disrupt communications temporarily.
- Detection of signals is very difficult because the frequency is always changing.
- Federal government agencies do not require site licensing for low power, 2.4 GHz spread spectrum transmissions.

# Section 4
# Wireless Range

The range and throughput of WirelessLANs are affected by the composition of material in the floors, walls and ceiling of buildings. It is best to draw a map of your proposed site, then test the throughput and performance of the WirelessLAN system. It is beneficial to complete a site survey of your entire building before you select the final locations for GE Medical Systems Wireless Access Points:

*Illustration 7-1*
*Sample Building Map*




# Section 5
# Site Survey

A site survey software tool is provided with wireless ISA and PCMCIA LAN adapters. This tool helps determine the placement of antennas and Access Points to provide the best coverage for your wireless network. The tool measures both the link quality and received signal strength of all radios within the same domain.

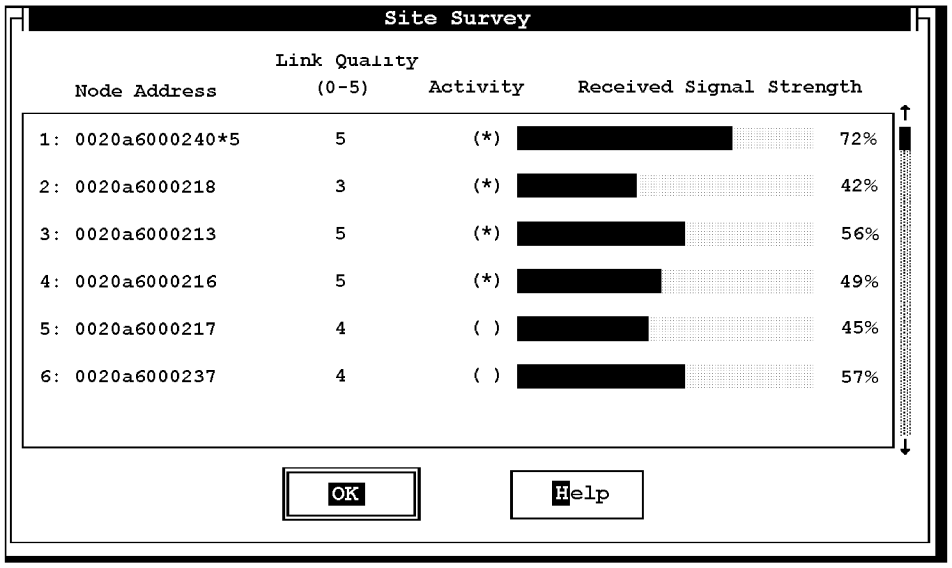
The link quality is measured over a range of zero (0) to five (5). The value measures the number of packets sent out by the site survey tool that are received by the adapters within range. A reading of five means that most of the packets are being received, while a reading of zero means that only a few packets are received. The received signal strength parameter measures the radio signal strength between the remote computers and the site survey computer. The link quality and received signal strength parameters are not necessarily reflective of each other. For example, the received signal strength might be fifty percent (50%), but the link quality could still be five. This indicates you are operating near the fringe of the range, but signals are strong enough to maintain high connectivity.

To run the site survey tool, make sure all Access Points are turned on, and that all client computers have either the ODI or NDIS driver loaded. Select one separate computer to run the site survey tool. The site survey tool operates on either a network with active connections or one where the NDIS or ODI drivers are running on each PC.

## 5.1 Running the Site Survey Tool

### 5.1.1 Wireless Point-To-Point Bridge

Illustration 7-2
Site Survey Screen Accessed Through the Test/Utilities Window



Turn on the Access Point and load an ODI or NDIS driver on a PC. Load the site survey tool on a PC, and note the link quality and received signal strength measurements at your location on the building map. Move the PC with the site survey software to various locations in your building, and record the respective link quality and received signal strength measurements. To optimize placement of your Access Point, move the unit to different places, or try different antenna placement options to see if it affects your measurements. Place the Access Point in the best location that produces the highest overall numbers for the area you want to cover.

### 5.1.2 Wireless Access Point 2

A variety of AMP Wireless Access Point 2 diagnostics can be performed from the *Diagnostics Menu* shown below.

| Diagnostics Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Radio Diagnostics Menu | |
| 2 | Technical Support Parameters | disabled |
| 3 | BOOT ROM Version | 1.1-B17 |
| 4 | Flash Code Version | FF 1.1-B20 |
| 5 | Ping IP Host | |
| 6 | Discover APs | |
| Enter a selection number or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Diagnostics Menu*

### 5.1.3 Radio Diagnostics Menu

The AMP Wireless Access Point 2 has a site survey function that displays the quality of the wireless link between the access points and wireless clients. A network administrator might want to perform a site survey when diagnosing user performance problems. A network installer might perform a site survey to help determine access point placement and wireless client antennas placement. The site survey functions may also be used to diagnose some access point problems (see “Troubleshooting” sections, pages 9-1 and 10-1).

The site survey is accessible from the *Radio Diagnostics Menu* shown below.

| Radio Diagnostics Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Run Broadcast Site Survey | |
| 2 | Run Directional Site Survey | |
| 3 | Radio ROM Version | V1.578 |
| Enter a selection number or <ESC> for previous menu - > | | |

*AMP Wireless Access Point 2 Radio Diagnostics Menu*

To perform a site survey, first choose the **Run Broadcast Site Survey** option and let the AMP Wireless Access Point 2 sit for a period of time you specify (the site survey period). Then look at the list of MAC addresses found, the Link Quality, and the Received Signal Strength Indicator (RSSI) data. The results will show an average value for each parameter over the time period for which the site survey was run. If you check the data before the full time has elapsed, you will see values that are an average of the time thus far elapsed. An example of a broadcast site survey is shown below:

| Site Survey Table | | |
|---|---|---|
| Address | Link Quality (1=poor, 5=strong) | RSSI |
| 00:20:a6:10:2d:68 | 5 | 158 |
| 00:20:a6:10:24:99 | 5 | 150 |
| 00:20:a6:10:26:89 | 4 | 127 |
| Hit any key to continue . . . | | |

*AMP Wireless Access Point 2 Broadcast Site Survey Table*

The higher the Link Quality number from a particular node, the better the link. A Link Quality number of 0 indicates the node is no longer responding. This is the most important parameter to watch to verify that you will be able to maintain a reliable wireless connection. The Link Quality number of AMP Wireless adapters may be low if those adapters are in their doze mode when being surveyed. As these adapters wake up, the Link Quality number may change.

Received signal strength (RSSI) indicates how strong a signal was received from a particular mode.

After using the Broadcast Site Survey, you can choose the **Run Directed Site Survey** from the Radio Diagnostics Menu to check the packets per second and bytes per second measurements between the AMP Wireless Access Point 2 and the node you select. An example of a directed site survey is shown below.

| Site Survey Table | | | |
|---|---|---|---|
| Index | Address | Link Quality (1=poor, 5=strong) | RSSI |
| 1 | 00:20:a6:10:2d:68 | 5 | 158 |
| Hit any key to continue. . . | | | |

*AMP Wireless Access Point Directed Site Survey Table*

### 5.1.4 Other Diagnostic Menu Options

The Diagnostics menu has a number of other submenu options which can be useful if you contact AMP to diagnose access print problems. **Technical Support Parameters** is a way to remotely diagnose access point problems over a modem. **Boot ROM Version** and **Flash Code Version** simply show the version number used in your access point. **Ping IP Host** is another way to verify host communication. **Discover APs** is a way to identify other access points on the wireless network. These *Diagnostic Menu* parameters are not discussed further in this manual.

## 5.2 Range

Before you determine the range of products, you must first define what is meant by being in “range”. One option is to pick a percentage of the throughput that you receive when the units are close to each other (five to ten feet). For example, say that your throughput is 100 bytes per second and you pick less than five percent (5%) throughput as out of range. You would continue to walk away from the other wireless unit until the throughput reached five (5) bytes per second. It is helpful to map an entire circle of range and see how different materials affect the throughput.

When making range measurements, it is important to eliminate as many variables as possible so that you can easily repeat your tests. For example, if you know of any products that directly interfere in a particular frequency range, then it is best that you conduct tests with the units always on or off.

*Note* *Do not run the site survey tool during your throughput testing. The tool communications with all units within range decreases the overall performance of the WirelessLAN.*

# Section 6
# Hardware and Software Installation

## 6.1 PCMCIA Adapter Set-Up

You must attach the GE Medical Systems Wireless PCMCIA Adapter to the portable computer you will use for the site survey, and load the PCMCIA software. Refer to the hardware installation and software loading instructions in the GE Medical Systems Wireless PCMCIA Adapter user’s guide.

## 6.2 Access Point Set-Up

Follow the instructions in the GE Medical Systems Wireless Access Point user’s guide to set up the access point. Use the default or “out-of-box” configuration. If you are using a U.S./Canada access point, the DC power supply must be plugged into an AC outlet and the DC cable must be connected to the access point. If you are using an international access point, the unit must be plugged into an AC outlet and the antenna must be attached. When conducting the site survey the access point must not be connected to a computer network.

When you are performing the site survey you will be mounting the access point at various temporary locations while you make measurements. The access point should be positioned in a manner similar to its permanent mounting position. U.S./Canada access points, for example, are usually mounted above a false ceiling with the antenna pointing down. International access points are usually placed on a high shelf or other platform, with the antenna pointing up. You may wish to construct a mounting pole or modify a tall ladder to position the U.S./Canada access point in its temporary locations, as shown in the figure below. For the international access point, a shorter ladder or other platform may be suitable, as shown in the figure. Be sure to use a mounting system that is stable and will prevent the access point from falling. Avoid creating or using a temporary mounting system made largely of metal, due to the potential for radio frequency interference. The GE Medical Systems access point stand provides a convenient temporary mounting platform.

## 6.3 Confirming Access Point and PCMCIA Compatibility

GE Medical Systems wireless devices have many software parameters that can be adjusted to various setting. Adjusting these software parameters (termed “configuration”) for the different devices installed in a wireless network allows the devices to share the same air space with minimum interference. During the site survey, two parameters must be set correctly so that the access point and the portable computer can communicate. These two parameters are the Station Type and the Domain. When performing the site survey, the Domain of both the access point and the PCMCIA adapter (attached to your portable computer) must be set to the same value (a numerical value between 0 and 15). The Station Type for the access point must be set to MASTER, while the Station Type for the PCMCIA adapter must be set to STATION. The access point and the PCMCIA adapter supplied in your site survey kit are set at the factory with default settings that allow them to work correctly together. (Domains are both set to 0 (zero), and Station Types are set as indicated above.) If the access point and PCMCIA adapter you are using are not configured correctly, follow the procedure below to set the Station Type and Domain. Additional information on this process is contained in the GE Medical Systems Wireless Access Point user’s guide “Configuration” chapter.

To change the Station Type or Domain of the PCMCIA adapter, or to verify that they are set correctly, use the software program called RL2Setup. This program comes with the PCMCIA adapter on the diskette labeled “Network Drivers/RL2Setup”. Perform the following steps to set these PCMCIA card software parameters.

1. If not already installed in your portable computer, install RL2Setup by following the instructions in the GE Medical Systems Wireless PCMCIA Adapter’s user’s guide.
2. Run RL2Setup. You will see the *WirelessLAN/PCMCIA Setup* main menu screen (shown below).
   To run the RL2Setup program you must first boot or reboot the computer without loading any network drivers or entering the Windows operating system. (For Windows 95 you must exit and restart in MS-DOS mode.) Go to the directory specified during the installation process; the default setting is C:/NDIS. Type RL2Setup and press <ENTER>.
3. <TAB> to Configure and press <ENTER>. You will see the *Configuration* screen.
4. Set Station Type to Station using the <TAB> Key and <↑> and <↓> arrow keys.
   If you know the access point Domain setting proceed to step 5. If you don’t know this access point setting <TAB> to OK and press <ENTER>, repeating this until you return to the *WirelessLAN/PCMCIA Setup* main menu screen. Proceed to Step 8.
5. <TAB> to Advance and press <ENTER>. You will see the *Advanced Configuration* Screen.
6. <TAB> to Network Domain to set the PCMCIA card’s Domain. Use either the <↑> and <↓> arrows or enter the Domain number directly. Set the Domain to the same value as the access point’s Domain.
7. <TAB> to OK and press <ENTER> to return to the previous screen. Repeat this process to return to the *WirelessLAN/PCMCIA Setup* main menu screen. Your PCMCIA adapter is now set to work properly with the access point. Skip the remaining steps.
8. <TAB> to Test/Utilities and press <ENTER>. <TAB> to Masters and press <ENTER>. The access point’s Domain (along with other information) will be displayed on the screen. If more than one access point is listed, locate the one(s) not being used and turn them off.

9. <TAB> to the Address location to select the access point. Then <TAB> to Use Domain and press <ENTER> (you will see a confirmation screen, confirm the change). <TAB> to *Done on the Utilities* screen and press <ENTER>. Your PCMCIA adapter Domain is now set to the Domain of the access point and you are returned to the *WirelessLAN/ PCMCIA Setup* main menu screen.

# Section 7
# Measuring WirelessLAN Performance

## 7.1 Measures of Transmission Quality

The site survey software provides three parameters that indicate signal strength or throughput.

- Link Quality
  Link quality is a 0 – 5 scale with 5 being the best. A reading of 0 indicates you are out of range.
- Received Signal Strength
  Received signal strength is a percentile scale, with 100% being the best and 0% the worst.
- Packets Per Second
  This is the recommended parameter for site survey measurements. Packets per second (also called throughput) indicates the number of data packets being successfully transmitted and received per second. The minimum acceptable packets per second for your system will depend on the applications you are running on your network. Under ideal circumstances (the portable computer near the access point with no obstructions between them) the throughput should be over 55 packets per second (when the packet size is the default value of 1500 bytes). Transmission rates of 20 packets per second or higher are generally considered acceptable, even for network intensive applications. Applications that do not challenge the network, such as e-mail, may work fine with transmission rates as low as 5 – 10 packets per second. (Remember, an unsuccessfully transmitted packet is retransmitted until it is successfully received. It is not skipped or lost.)
  The software can also measure throughput in bytes per second. This is simply the packets per second value multiplied by the packet size in bytes.

## 7.2 How to Measure Throughput (Packets per Second)

For the site survey, we recommend using packets per second as the measure of transmission throughput for determining access point locations. Packets per second are measured using the procedure below. This procedure will be used throughout the site survey.

### 7.2.1 Wireless Point-to-Point Bridge

1. Run RL2Setup. You will se the *WirelessLAN/PCMCIA Setup* main menu screen (shown below).
   To run the RL2Setup program you must first boot or reboot the computer without loading any network drivers or entering the Windows operating system. (For Windows 95 you must exit and restart in MS-DOS mode.) Go to the directory specified during the installation process; the default setting is C:NDIS. Type RL2Setup and press <ENTER>.
2. <TAB> to Test/Utilities and press <ENTER>. You will see the *Utilities* screen.
3. <TAB> to Site Survey and press <ENTER>. You will see the *Site Survey* screen. Note the Roaming Enabled box at the lower left. If there is an "X" in the box, <TAB> to the box and hit the <Spacebar> to remover the "X" and disable this function. If the access point is operating and the two units are set to the same Domain, you will see displayed the Node Address, Link Quality, Activity, and Received Signal Strength for the access point. If more than one access point is listed, locate the one(s) not being used and turn them off.
4. <TAB> to highlight the Node Address of the access point and press the <spacebar>, or click on the access point's address. You will see the *Directed Link* screen with the transmission rate in packets per second. You will also see the throughput in bytes per second and the packet size, in bytes. We recommend that you use the default packet size of 1500 bytes. The transmission rate (throughput) will fluctuate. When conducting a site survey you will need to mentally average this fluctuation value in order to determine the approximate throughput.
5. <TAB> to Done and press <ENTER> to return to the previous screen. Repeat this process to return to the *WirelessLAN/PCMCIA Setup* menu screen.

### 7.2.2 Wireless Access Point 2

1. Open up a terminal session using the instructions from Section 2 starting on page 6-2.
2. From the *Main Menu*, select the *Diagnostics Menu*. The Diagnostics Menu will appear.

Model 7520, FF 1.2-B31

| Diagnostics Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Radio Diagnostics Menu | |
| 2 | Technical Support Parameters | disabled |
| 3 | Boot ROM Version | 1.1-B17 |
| 4 | Flash Code Version | FF 1.2-B31 |
| 5 | Ping IP Host | |
| 6 | Discover APs | |

*Main Menu*

Enter a selection number or <ESC> for previous menu ->

Select the *Radio Diagnostics Menu*. The radio *Diagnostics Menu* will appear.

| Diagnostics Menu | | |
|---|---|---|
| Selection | Description | Current Value |
| 1 | Run Broadcast Site Survey | |
| 2 | Run Directed Site Survey | |
| 3 | Run Antenna Pointing Tool | |
| 4 | Radio ROM Version | V1.57B |

*Radio Diagnostics Menu*

Enter a selection number or <ESC> for previous menu ->

To perform a survey, first choose the **Run Broadcast Site Survey** option and let the AMP Wireless Bridge sit for a period of time you specify (the site survey period). Then look at the list of MAC addresses found, the Link Quality, and the Received Signal Strength Indicator (RSSI) data. The results will show an average value for each parameter over the time period for which the site survey was run. If you check the data before the full time has elapsed, you will see values that are an average of the time thus far elapsed. An example of a broadcast site survey is shown below.

| Site Survey Table | | |
|---|---|---|
| Address | Link Quality (1=poor, 5=strong) | RSSI |
| 00:20:a6:10:2d:68 | 5 | 158 |
| 00:20:a6:10:24:99 | 5 | 150 |
| 00:20:a6:10:26:89 | 4 | 127 |
| | | |
| Hit any key to continue . . . | | |

The higher the Link Quality number from a particular node, the better the link. A Link Quality number of 0 indicates the node is no longer responding. This is the most important parameter to watch to verify that you will be able to maintain a reliable wireless connection. The Link Quality number of AMP Wireless adapters may be low if those adapters are in their doze mode when being surveyed. As these adapters wake up, the Link Quality number may change.

Received signal strength (RSSI) indicates how strong a signal was received from a particular node.

After using the **Broadcast Site Survey**, you can choose the **Run Directed Site Survey** from the *Radio Diagnostics Menu* to check the packets per second and bytes per second measurements between the AMP Wireless Bridge and the node you select.

Select the node on which to perform the directed site survey. If only one node is shown press <ENTER>. Press <ENTER> to choose the default packet size of 1500 bytes. Press <ENTER> to set the default duration of 10 seconds. The results of the directed site survey will be displayed as shown below.

| | |
|---|---|
| Site Survey Completed | |
| Node Address | 00:20:ab:10:23:33 |
| Packets Per Second | 32 |
| Bytes Per Second | 48000 |
| Average RSSI | 170 |
| Average Latency (mS) | 26 |
| Maximum Latency (mS) | 59 |
| Standard Deviation of Latency (mS) | 8 |
| | |
| Hit any key to continue. . . | |

As you aim the antenna, you will run the antenna pointing tool (selection 3 of the *Radio Diagnostics Menu*) to achieve optimum performance. From selection 3 press <ENTER> to get the Target Node Address. Verify the displayed Mac ID address corresponds to the bridge unit to which you are aiming, press <ENTER>. The default Packet Size (1500 bytes) will be displayed, press <ENTER>. Sample Interval Periods will be displayed. Select one and press <ENTER>. As you aim the antennas, monitor the displayed values until maximum throughput is achieved.

# Section 8
# Benchmarking

There are many ways to benchmark WirelessLAN performance. A few of them are:

- File transfer
- Printing
- Loading applications over the network
- Running client/server applications

## 8.1 Single Client to an Access Point

- Measure throughput with the units at close range of five to ten feet with line of sight between the antennas.
- Measure the throughput by moving the client to various points within the network, using the locations on your building map.
- Measure the throughput at locations near the fringe.

## 8.2 Multiple Clients to a Single Access Point

- Measure throughput with one client at close range of five to ten feet with line of sight between the antennas. Add additional clients and measure the change in overall throughput and the throughput for each client.
- Repeat the same test with the clients spaced at various locations on your building map.

## 8.3 Multiple Clients to Multiple Access Points

- Install multiple Access Points all within the same range. Space them roughly ten feet away, and configure each to communicate on a different channel with the same domain number.
- Have the client computers attach to the network. They will randomly attach to one of the multiple Access Points. Place the units at close range or within five to ten feet with line of sight with the Access Points. Compare the throughput numbers to the previous tests.

Repeat the same test with the clients spaced out at different locations on your building map.

# Section 9
# Licensed Versus Unlicensed Operation

Wireless products operate in the 2.4 GHz frequency range which is the same frequency as many microwave ovens and some licensed radio transmitters. The FCC does not require licensing for operators of microwave ovens because the transmissions are limited to the microwave oven enclosure. GE Medical System's wireless devices are not site licensed because transmissions are limited to short distances and the signals are very low power, approximately 0.1 watt compared to the 1000 watt microwave oven or a typical FM transmitter that operates at thousands of watts.

# Section 10
# Network Operating System Considerations

Wireless Access Point meets the IEEE 802.2 frame type specification. Most bridges, gateway software, and other products you use on your network will interoperate with Access Point just like any other network card. For example, you may have both Novell and TCP/IP attached through a gateway. Your workstations and servers using wireless adapters can access the **UNIX** portion of the network in the same way other wired workstations do.

Access Point is shipped with ODI and NDIS compliant drivers that function with operating systems that use Network Interface Cards (NIC) with ODI or NDIS drivers.

# Section 11
# Master/Alternate Master Configurations

GE Medical Systems devices use a spread spectrum frequency hopping technique. The radio signal is constantly moving from one frequency to another in a pre-defined sequence. In order for several radios to communicate, they must be at the same frequency at the same time.

The Master sets the pace for the other radios. All stations look to the Master to determine where and when to hop. If there is no Master present, a station configured as an Alternate Master becomes the Master.

The system administrator has the task of configuring each wireless node on the network as Master, Alternate Master or a station. In most cases, the default configurations for each device is adequate. To improve performance in some applications, you should consider:

- In a roaming environment, all Access Points must be set as Masters on the same domain with unique channel/subchannel combinations.
- ISA and PCMCIA workstations are all set as stations on the same domain as that of the Access Points.
- If an Access Point is part of your wireless network, it must be the Master or Alt Master node.
- For most wireless networks, only one node should be the Master. If you need to set up additional Masters, they should be configured as Alternate Masters.
- The Master must be within range of the other wireless stations on the network. The typical range for a wireless PC radio is a radius of 100 to 150 feet from the Access Point in office environments, and up to 1,000 feet in open areas.
- The Master should not be a station which will be moved or turned off like a notebook computer or a user's personal machine.
- If you are using an ISA card in a Novell file server, it must be configured as the Master.
- On a peer-to-peer based network, it is a good idea to designate at least one computer as an Alternate Master in the event that the Master is unavailable, or accidentally is turned off.
- On a network with all notebook or pen-based computers, make all the units Alternate Masters.
- Performance improves as you limit the number of Alternate Masters.

# Section 12
# Network Architectures

The GE Medical Systems wireless products family can exist on your LAN as a standalone network or as an additional subnetwork, and operate with a variety of network operating system environments.

# Section 13
# Spanning Tree Protocol Support

The WirelessLAN meets the IEEE 802.1d Spanning Tree Protocol specification. This protocol was designed to handle cases in a complex bridged network (multiple bridges) where loops are created either unintentionally or to provide redundancy in the network. The bridges configure themselves into a spanning tree topology and remove any loops within the network. If you are administering a network with more than one bridge (wireless or otherwise), you may need to have some understanding of this protocol so that you can configure your bridges for optimum performance.

One of the bridges becomes the root of the spanning tree. This root is determined by the bridge with the lowest spanning tree priority on the network. This bridge determines when all the bridges broadcast their priorities, physical addresses, activity states, etc. This communication is sent in what are called hello packets, and the root bridge determines the interval between these packets called the hello time.

Once a root to the tree has been established, all other bridges on the network become the branches. The order of the branches is determined by the spanning tree priority, path cost number of jumps away from the root), and port priority for each bridge and each port on each bridge.

In the case where there are redundant bridges causing loops in the network, these loops are resolved by one of the bridges becoming inactive. This means the bridge no longer forwards packets of data that are sent to it. If the loops were not resolved, the same packet of data might travel around the network ad infinitum.

The network's bridges determine who should become inactive based on several parameters which you may configure on the wireless device using the configuration program CFG.EXE or a network management station which supports the IEEE 802.1d Bridge MIB (RFC 1493).

## 13.1 Spanning Tree Priority

This parameter sets the priority of the wireless device in the spanning tree created on the network. It is used to determine the root node and the branches of the tree as well as resolving conflicts to decide which bridge on a network becomes inactive when there is a loop. In the event that two bridges have the same priority, the unique physical address breaks the tie. The lower value has the higher priority. You may choose a value of 0 to 65535 with the wireless device default being set to 32,768.

## 13.2 Bridge Max Age

When the wireless device acts as the root, it uses this parameter to determine the maximum amount of time before discarding hello packet data for all bridges on the network. This parameter is specified in seconds between 6 and 40, with a default value of 20.

## 13.3 Bridge Hello Timer

When the wireless device acts as the root, it uses this parameter to determine the interval of time between hello packets. If this parameter is set too high, the network does not quickly resolve contention problems. However, if the parameter is set too low, the network will be crowded with hello packet traffic. This parameter is specified in seconds between 1 and 10, with a default value of 2.

## 13.4 Bridge Forward Delay

This parameter specifies the amount of time it takes to transition between port states after reset of the wireless. The state transitions follow:

- Disabled
- Blocking incoming packets
- Listening for other bridges

- Learning the addresses of other bridges
- Forwarding data

It is specified in seconds between 4 and 30, with a default setting of 15.

## 13.5 Aging Time

This parameter specifies the time after which the learned physical address of the network node is discarded. This data is dynamically acquired by the wireless device so that it can forward packets properly. This parameter is set in seconds between 10 and 1,000,000 seconds with a default value of 300.

## 13.6 Wireless Port and Ethernet Port Priorities

These parameters are used in the spanning tree algorithm to determine the place of the port in the tree, as well as to resolve loop contention problems. The lower value has the higher priority. Set this parameter for both the Wireless port and the Ethernet port. These parameters range from 0 to 255, with default values of 128.

## 13.7 Wireless Port and Ethernet Port Enabled

If either port is disabled, the wireless bridge will not forward data packets to the network through this port. Since there are only two ports on the device, disabling either port makes the entire bridge inactive.

## 13.8 Wireless Port Path and Ethernet Port Path Cost

These parameters specify the cost that is added to the spanning tree for this port of the wireless device. This applies only when the device is not the root of the tree and when the port you are setting is the root port of the two wireless ports. The parameter range is 1 to 65535, with a default value of 100 for the Ethernet port, and 625 for the Wireless port.

# Chapter 8
# Security

## Section 1
## Setting Security

***Important*** ***Any wireless devices which are to communicate with each other must be set with the same Security ID.***

### 1.1 Wireless Point-to-Point Bridge

You can set a security identification (ID) for each GE Medical Systems product installed on a network. This is an added security measure. All products must have matching security IDs in order to communicate.

To set the wireless security ID, use the CFG program that is on the driver diskette:

1. Select the correct device from the list.
2. Choose the *Configure Wireless* button followed by the *Set Security ID* button to set or change the security ID on the wireless device.

### 1.2 Wireless Access Point 2

You can set a security identification (ID) for each GE Medical Systems product installed on a network. This is an added security measure. All products must have matching security IDs in order to communicate.

1. Open up a terminal session with Wireless Access Point.
2. Select 1 for the Configuration Menu.
3. Select 4 for the Radio Configuration Menu.
4. Select 10 to set the Security ID.

THIS PAGE INTENTIONALLY LEFT BLANK

# Chapter 9
# Troubleshooting Point-to-Point Bridges

## Section 1
## Overview of Troubleshooting

The WirelessLAN is easy to install, operate and troubleshoot. If you cannot resolve a problem after reviewing this section of the manual, contact GE Medical Systems Online Center. See “Technical Support” on page 1-2.

## Section 2
## Obtaining Help with LAN Installation

If you require installation assistance, contact the GE Medical Systems Online Center for the name of reseller in your area. Reseller are experts in the design, installation, and maintenance of WirelessLANs. They can examine your needs and recommend the most cost-effective solution for new LAN or expansion systems.

## Section 3
## General Problems

This section reviews some of the most common WirelessLAN problems.

No response from the device when **configuring remotely.** There are several possible solutions for this problem:

- Verify that the IP address for the configuration tool PC is set properly in the CFG.CFG file.
- Use local management to verify that the IP address for the device is set correctly.
- Verify that you are not duplicating IP addresses on your network.
- Verify the Access Point diskette is seated properly inside the wireless device.

No response from the wireless device when configuring **locally.** There are several possible solutions for this problem:

- Verify that SLIP.BAT is configured for the correct I/O port address and IRQ interrupt of the configuration PC’s COM port.
- Verify that there are no IRQ conflicts between the configuration PC’s COM port and other cards in the computer.
- Verify that you are using a null modem serial cable when attaching a configuration PC to the device.
- Verify the diskette is seated properly inside the device.

**Mismatched domains and security IDs.** If you are unable to establish communication with another machine on the network, it is possible that you do not have the same domain and security ID as that which is on the other machine.

The SNMP management system **is unable to write parameters.** Verify that you are using "Private" for the community string.

**You cannot communicate through the wireless device to the rest of the Ethernet network.** Follow these steps to diagnose the problem:

- Use remote management to access the device. If this fails, check the Ethernet cabling.
- Check the yellow Sync LED on the back of the Station device to verify you have a wireless link.
- Check the filter settings on the wireless device. Verify that you are not filtering out the kind of traffic you are trying to send. For example, on a Novell network, you do not want to check the IPX protocol box. On an IP network, you may need to set an ARP filter.
- Verify that the diskette is seated properly inside the device.

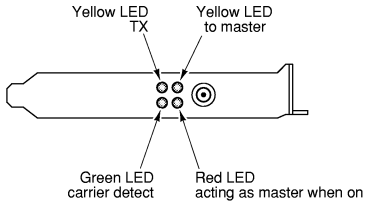
# Section 4
# Wireless LEDs

There are three LEDs on the front panel of the WirelessLAN:

- The Power LED (green) should be on whenever the wireless device is powered on.
- The LAN1 LED (amber) flashes to indicate transmissions on the network.
- The LAN2 LED (red) flashes to indicate Ethernet transmissions on the network.

There are four LEDs that are visible on the back of the wireless device:

- The red LED in the bottom right is on steady when the device acts as the Master station. There should be only one card on the subnetwork with this light on at any time.
- The yellow LED in the upper right is lit when the card is synchronized to a Master.
- The upper left yellow LED indicates the card is transmitting.
- The bottom green LED lights whenever the card detects another unit that is transmitting.



# Section 5
# Wireless Bridge Audio Aids

As the wireless device boots and initializes, you hear several tones. Soon after the machine is turned on, you hear a single beep. Later there are two separate beeps as the machine is initializing. Wait until you hear a multi-tone beep which indicates the wireless device is now in the forwarding state before you attempt to attach to a network.

# Section 6
# Other Information

If there is additional information that becomes available after the printing of this manual, there will be a README file on the GE Medical Systems diskette.

THIS PAGE INTENTIONALLY LEFT BLANK

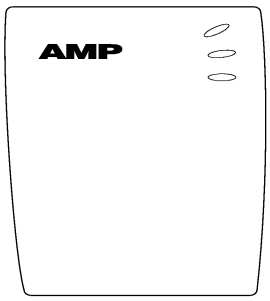
# Chapter 10
# Troubleshooting Wireless Access Point 2 Bridges

The AMP Wireless Access Point 2 is easy to install and operate. If you do experience problems, however, the information in this section will help you diagnose and solve them. If you need additional assistance contact AMP (see “Technical Support” page 1-2). The Diagnostics Menu can be helpful in diagnosing some access point problems. If you contact AMP technical support, you may be asked to run the diagnostics functions.

## Section 1
## LED Indicators

The LEDs on the top and on the back panel of the AMP Wireless Access Point 2 indicate how the unit is functioning. There are three LEDs on the top of the access point:

- The top LED, called the Status LED, changes from orange to green to indicate the access point is functional. It changes from orange to red if there is a hardware problem with the unit. If the LED turns red, contact AMP (see “Technical Support” page 1-2).
- The center orange LED, called the Radio LED, flashes when the access point transmits wirelessly.
- The bottom green LED, called the Network LED, flashes when the access point transmits over the Ethernet network.



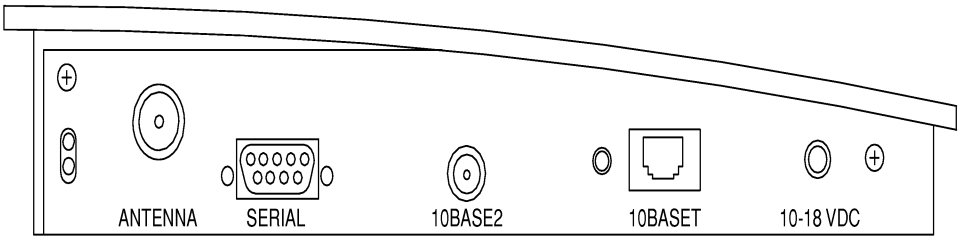

*LEDS on the TOP of the AMP Wireless Access Point 2*

The following table illustrates the state of the LEDs during power-up:

| State | Status | Radio LED | Network LED |
|---|---|---|---|
| Unit Off | Off | Off | Off |
| Power-On Diagnostics | Orange | Off | Off |
| Diagnostics Failed | Red | Off | Off |
| Normal | Green | Blinking Orange | Blinking Green |

There are three LEDs on the pack panel of the AMP Wireless Access Point 2, two on the left and one next to the 10BaseT connector.

- If the access point is configured as a Master, the top-left green LED should always be on.
- If the access point is configured as a Station, the bottom-left yellow LED should always be on.
- The green LED near the 10Base T connector is on when a functional 10BaseT cable is plugged in. It will not light if a 10 Base2 cable is being used.




*LEDs on Back Panel of the AMP Wireless Access Point 2*

# Section 2
# General Problems

**Is access point fully booted?**

This will be indicated by the Status LED changing from orange to green.

**I can't connect to the network from a wireless client.**

- Verify wireless connection using the AMP Wireless Access Point 2 site survey tools (see page 7-5).
- Check the *Ethernet Statistics Menu* to verify there is Ethernet traffic that the access point can detect. If you are using 10BaseT Ethernet cable, you can also determine that the cable is functional by verifying that the cable LED is green.
- Verify you are not filtering out the find of traffic you are trying to pass.
- Verify the two wireless devices are using the same Domain.
- Verify the two wireless devices can communicate using the **Ping IP Host** command on the Diagnostics Menu (see page 7-5) to ping between the wireless devices.

If you still can't connect, call the OLC for assistance.

**Are the wrong filters set?**

Turn on one of the filters through the *Configuration Menu*. Then check the Filter Statistics. If the count is increasing on the filter you set, that kind of traffic is on the network. If wireless clients cannot attach to the network after setting this filter, turn that filter off.

**I can't ping or telnet to my brand new AMP Wireless Access Point 2.**

- If you are using 10BaseT Ethernet cable, verify that the cable is functional by checking that the cable LED is green. (The cable LED will not light if a 10Base2 connector is being used.)
- There is no default IP address. The first time you use the access point you should set an IP address using a terminal and null modem cable or a BOOTP server.

**How can I tell which clients are synchronized to my access point?**

View the Forwarding Database in the *Status Menu*. Units on the wireless side of the access point that are synchronized to it are shown.

**I can't configure the access point locally via the serial port.**

Verify you are using a null modem cable and that the terminal is set to 9600 N81.

**I can't establish a wireless connection with the access point.**

Verify that the client is set to the same Domain and Security ID and that the client is configured as a Station.

**The throughput seems slow.**

- To achieve maximum throughput, verify your antennas are well-placed, not blocked by too many obstacles or shielded by metal. If you move the antenna closer to the client and throughput increases, you may want to consider adding a second access point and implementing roaming.
- You may be able to set filters to filter out Ethernet traffic from the wireless side of the network.

**The status LED on the access point is red.**

This indicates a hardware problem within the access point, contact AMP (see "Technical Support" page 1-2).

THIS PAGE INTENTIONALLY LEFT BLANK.

# Chapter 11
# Point-to-Point Bridges Renewal Parts

Illustration 11-1

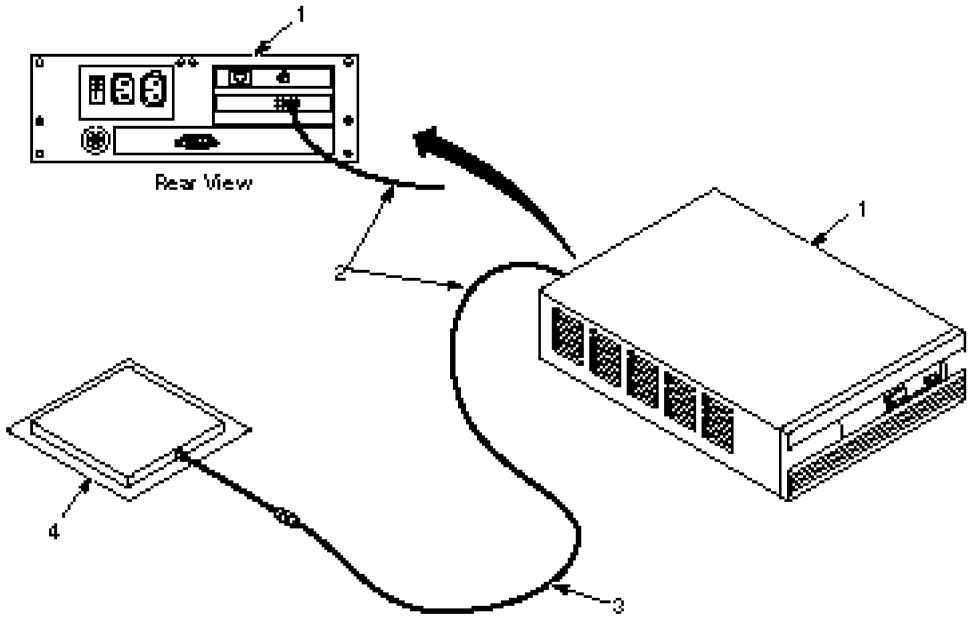



Table 11-1

**HOSPITAL SUBSYSTEM (earlier model - no longer orderable as a subsystem)**

| Description | GCP# |
|---|---|
| 1. Wireless Bridge | GCP#2168907 |
| 2. Transition Cable | GCP#2168909 |
| 3. Antenna Cable (20') | GCP#2168910 |
| 4. Patch Antenna | GCP#2168911 |
| 5. 75 foot Shielded Antenna Cable | GCP#2168914<br>(for unusual setting conditions) |

Illustration 11-2

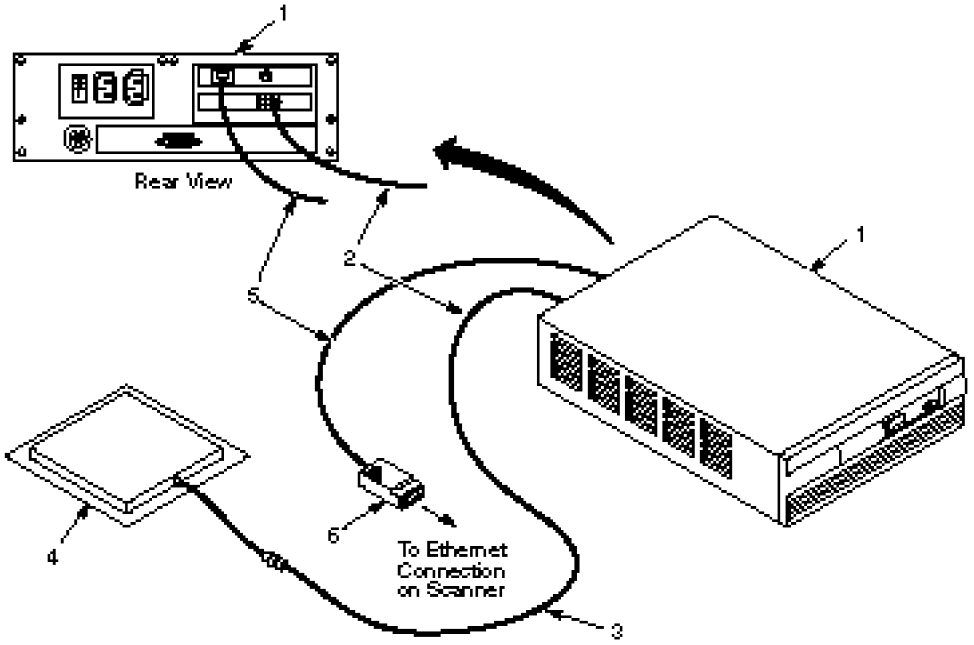



Table 11-2

**MOBILE VAN SUBSYSTEM, GCP#2169069, CATALOG #K1000MM**

| Description | GCP# |
|---|---|
| 1. Wireless Bridge | GCP#2168907 |
| 2. Transition Cable | GCP#2168909 |
| 3. Antenna Cable (20 feet) | GCP#2168910 |
| 4. Patch Antenna | GCP#2168911 |
| 5. UTP Cross-Over Cable (10 feet) | GCP#2168912 |
| 6. UTP Transceiver | GCP#2168977 |

Illustration 11-3

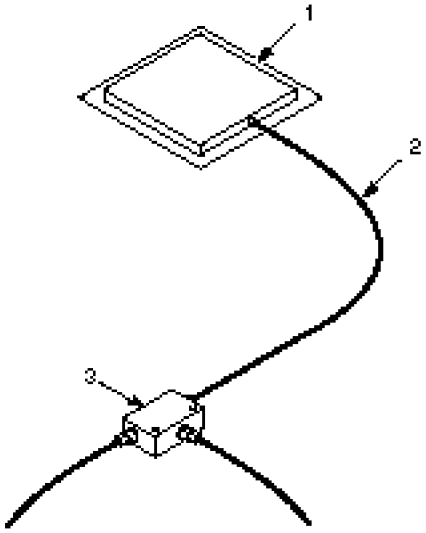



Table 11-3

**OPTIONAL ANTENNA KIT SUBSYSTEM, GCP#2187974, CATALOG #K1000MN**

| Description | GCP# |
|---|---|
| 1. Antenna Cable (20 feet) | GCP#2213234-3 |
| 2. Patch Antenna | GCP#2213231 |
| 3. Splitter | GCP#2187973 |

THIS PAGE INTENTIONALLY LEFT BLANK

# Chapter 12
# Wireless Access Point 2 Renewal Parts

Illustration 12-1

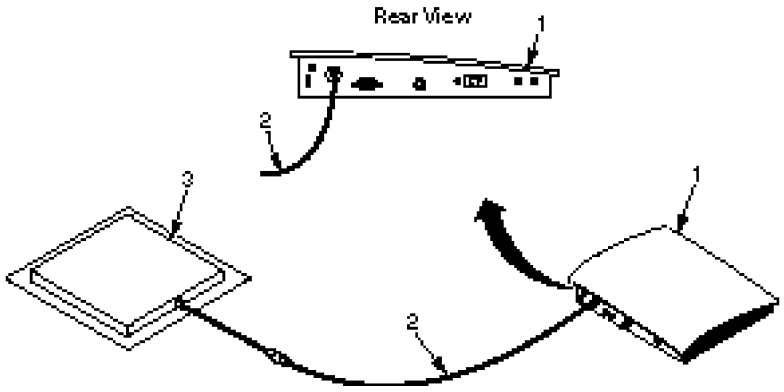



Table 12-1

**HOSPITAL SUBSYSTEM, GCP#2169070, CATALOG #K1000MH**

| Description | GCP# |
|---|---|
| 1.Wireless Bridge | GCP#2200725 |
| 2.Antenna Cable (20') | GCP#2213234-3 |
| 3.Patch Antenna | GCP#2213231 |

Illustration 12-2

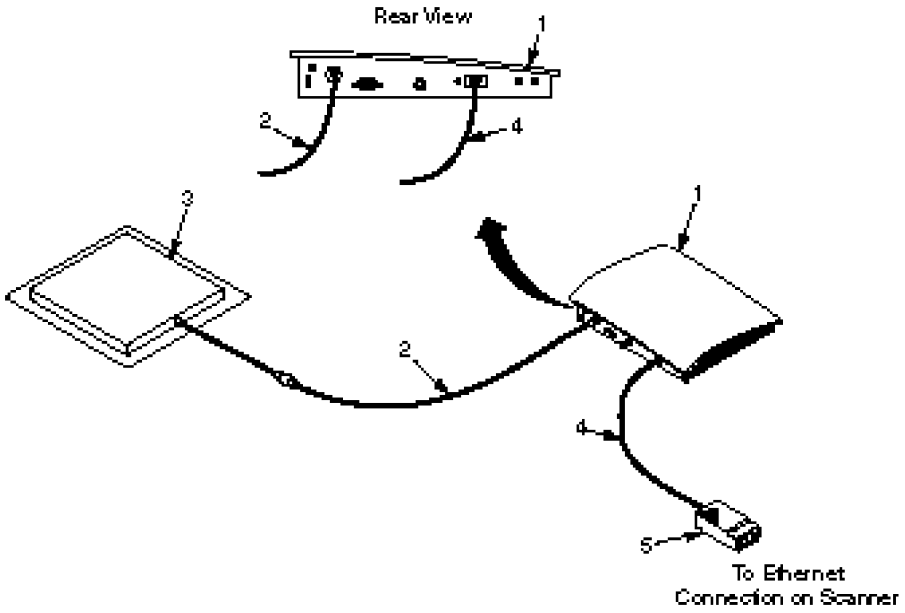



Table 12-2

**MOBILE SUBSYSTEM, GCP#2169069, CATALOG #K1000MM**

| Description | GCP# |
|---|---|
| 1.Wireless Bridge | GCP#2200952 |
| 2.Antenna Cable(20 feet) | GCP#2213234-3 |
| 3.Patch Antenna | GCP#2213231 |
| 4.UTP Cross-Over Cable (32 feet) | GCP#2168912-2 |
| 5.UTP Transceiver | GCP#2168977 |

Illustration 12-3

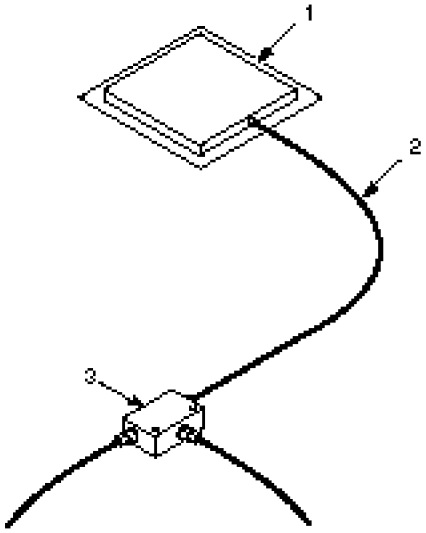



Table 12-3

**OPTIONAL ANTENNA KIT SUBSYSTEM, GCP#2187974, CATALOG #K1000MN**

| Description | GCP# |
|---|---|
| 1.Antenna Cable (20 feet) | GCP#2213234-3 |
| 2.Patch Antenna | GCP#2213231 |
| 3.Splitter | GCP#2187973 |

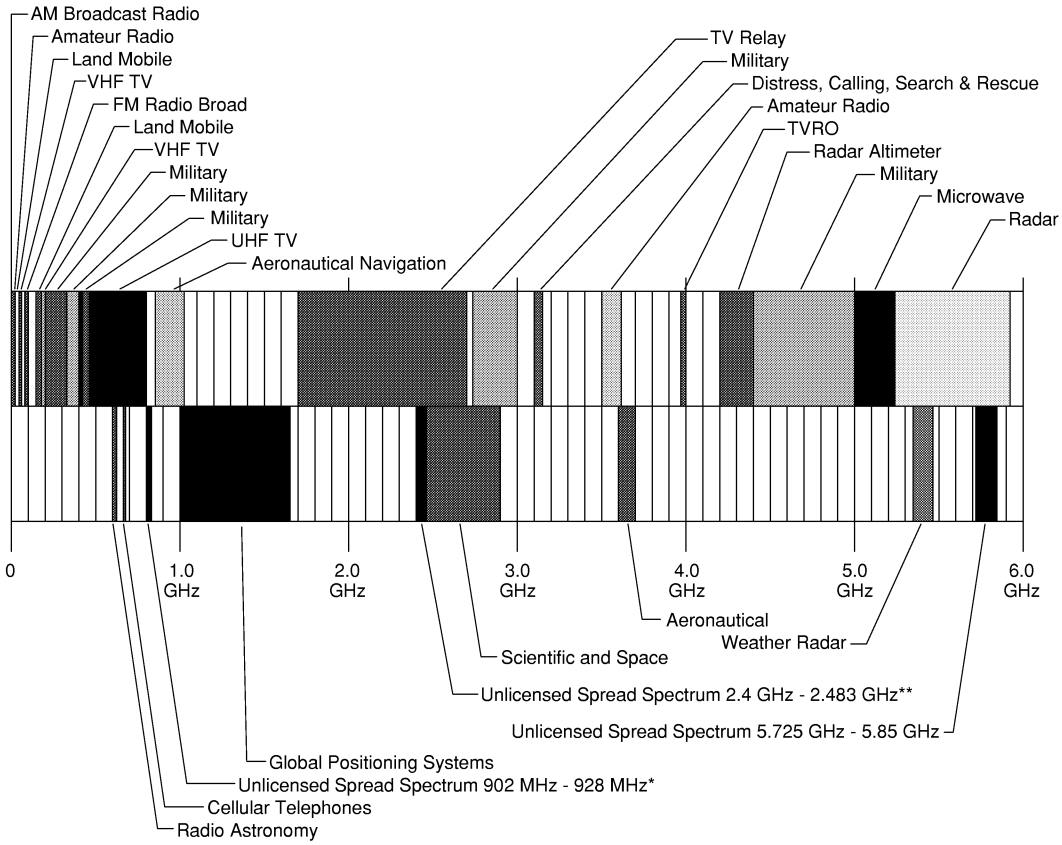
THIS PAGE INTENTIONALLY LEFT BLANK

# Appendix A

## Section 1
## Upgrading the Software

At some point in the future, you may need to upgrade the wireless software. To do this, use the CFG tool in the same way in which you would configure the wireless device. In the *Configure TCP/IP* screen, enter the name of the file you would like to be downloaded to the device in the *Download File* field. Indicate the method you are using to communicate with the device in the *BOOTP Interface* field.

After you fill in the *Download File* and *BOOTP Interface* fields, use the *Reset Wireless* button. Leave the CFG tool running. When the wireless device resets, the new software image is downloaded.



THIS PAGE INTENTIONALLY LEFT BLANK

# Appendix B

## Section 1
## U.S. Specifications

The following technical specification is for reference purposes only. Actual product performance and compliance with local telecommunications regulations may vary from country to country. GE Medical Systems only ships products that are type approved in the destination country.

| | |
|---|---|
| **Network Interfaces** | Ethernet 10BASE2 (Thin) BNC<br>Ethernet 10BASET (Twisted-Pair)<br>Ethernet 10BASE5 (Thick) 15 pin AUI (optional) |
| **Data Rate** | 1.6 Mbps—Wireless<br>10 Mbps—Ethernet |
| **Media Access Protocol** | CSMA/CA |
| **Ethernet Compatibility** | Ethernet packet types and Ethernet Addressing |
| **Frequency Band 2.4** | 2.483 GHz (spread spectrum frequency hopping) |
| **Independent Channels** | 15 |
| **Output Power** | 100 mW |

THIS PAGE INTENTIONALLY LEFT BLANK

# Appendix C

## Section 1
## Antenna Safety Standards

The following guidelines are safety recommendations for all amateur and general purpose communications antennas from the U.S. Consumer Product Safety Commission. For mast mounted antennas, be sure to review the antenna safety standards concerning grounding and mounting according to the National Electric Code.

### 1.1 You, Your Antenna, and Safety

Each year hundreds of people are killed, mutilated or receive severe permanent injuries when they attempt to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

For your safety and to help you achieve a good installation, please read and follow the safety precautions below. **THEY MAY SAVE YOUR LIFE!**

1. If you are installing an antenna for the first time, for your own safety as well as others, seek PROFESSIONAL ASSISTANCE. Consult your dealer. S/he can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind.


**Electric Power lines and phone lines look alike. For your safety, assume that any overhead lines can kill you.**

3. Call your power company. Tell them your plans and ask them to look at your proposed installation. This is a small inconvenience when you consider that your life is at stake.
4. Plan your installation procedure carefully and completely *before* you begin. The successful raising of a mast or tower is largely a matter of coordination. Assign each person who is working with you to a specific task. Each person needs to know what to do and when to do it. Place one person in charge of the operation to call out instructions and watch for signs of trouble.
5. When you install the antenna, **REMEMBER: DO NOT USE A METAL LADDER.** Do ***not*** work on a wet or windy day. Dress properly – shoes with rubber soles and heels, rubber gloves, long sleeve shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember, the antenna, mast, cable and metal guy wires are all conductors of electrical current. Even the slightest touch of any of these parts to a power line complete an electrical path through the antenna and the installer – **THAT'S YOU!**

If any part of the antenna system should come in contact with a power line – **DON'T TOUCH IT OR TRY TO REMOVE IT YOURSELF. CALL YOUR LOCAL POWER COMPANY.** The power company will remove it safely.

*Note* *If an accident should occur with the power lines, call for qualified emergency help immediately.*

# Appendix D

## Section 1
## Use of RF Devices in Hospitals and Clinics

### 1.1 Background

The rapid increase of the use of cellular phones, portable police radios, and other portable radio

Frequency devices over the last few years has focused more attention on the use of RF devices in healthcare facilities. Instances of portable RF devices interacting with electric wheel chairs, heart pacemakers, and medical monitoring devices have been documented. While these instances have been minimal, they do suggest the possible risks involved when radio waves interact with medical devices. Proxim recognizes the fact that responsible RF and medical device manufacturers and healthcare organizations must take the necessary precautions to ensure that medical devices continue to operate properly when used in conjunction with WirelessLAN products.

As of October 1996, there have been no reported instances of the WirelessLAN interfering with medical monitors and devices such as ventilators and heart monitors. Many hospitals and clinics currently use WirelessLAN equipment throughout their facilities, including ICUs (intensive care units). WirelessLAN units have not been a problem because:

- Uses a low power (0.1 watt) radio;
- Spreads its signal across 83,000 kHz, resulting in low power concentration;
- Rapidly changes its frequency every 0.2 seconds or sooner minimizing any possible interference impact at a specific frequency;
- Typically transmits less than 20% of the time which further reduces the average power concentration.

This is in contrast to walkie-talkies and portable cellular phones. The power concentration of these units is 10,000 times stronger than that of a WirelessLAN radio.

Walkie-talkies, portable cellular phones, and other wireless devices have been shown to occasionally interact with some electronic medical devices. Since WirelessLAN is a wireless device that has not interfered with medical devices, it should he examined in more detail to understand why there are no known instances of WirelessLAN interacting with electronic medical devices.

### 1.2 WirelessLAN

WirelessLAN uses a frequency hopping spread spectrum signal that operates in the 2.4 UHz ISM (industrial, scientific, medical) band and transmits at 0.1 watt of power. This low power level ensures that the WirelessLAN is capable of being used throughout the world and minimizes the possibility of any interaction with sensitive electronic equipment, including medical devices.

WirelessLAN power concentration at any point is very low. This is because the 0.1 watt of power is spread across 83,000 kHz of bandwidth. The end result is that the power concentration is very low, less than 11100 of that of portable cellular phone.

As a spread spectrum frequency hopping radio, WirelessLAN spends very little time at one spot on the 2.4 GHz ISM band; typically, less than 200 milliseconds are spent on a hop. A low power frequency hopping spread spectrum radio which changes its frequency every 0.1 to 0.2 seconds is unlikely to interfere with electronic equipment. Usually, there are certain frequencies at which electronic equipment is sensitive to electromagnetic radiation (EMR). At other frequencies, EMR has is no impact. Even on the sensitive frequencies, EMR usually has to exist for 0.5 seconds or longer to trigger a change in electronic equipment function. WirelessLAN by changing its frequency every 0.2 seconds (or sooner) is not on a frequency long enough to cause interference in other devices.

WirelessLAN has a low duty cycle and as a WirelessLAN radio, is transmitting less than 20% of the time.

The table on the next page summarizes the characteristics of WirelessLAN, portable cellular phones, and walkie-talkies.

Compared with the many RF devices used in healthcare environments today, WirelessLAN generates very low levels of RF energy for very short periods of time over a wide range of widely interference. This has been proven by the fact that WirelessLAN has been tested and used by many hospitals. A list of these hospitals is available on request.

Additional information on WirelessLAN compact used for WirelessLAN can be found on the Proxim web site:

http://www.proxim.com/

or contact Proxim on 800-229-1630 in North America or 415-960-1630 outside of North America. Proxim can also be contacted via email, sales @proxim.com.

## 1.3 A Simple “Ad Hoc” Testing Procedure

The following is a simple procedure for doing “ad hoc” testing. This procedure is meant to be a way of getting started with “ad hoc” testing. It is recommended that this procedure be replaced by the IEEE procedure for testing medical devices when IEEE releases the formal specification for “ad hoc” testing with medical devices.

This recommended procedure is intended to serve as a guide for performing radiated electromagnetic immunity testing of existing inventories of installed medical devices using WirelessLAN equipment.

This procedure is not meant to substitute for rigorous laboratory electromagnetic compatibility (EMC) testing. The objective is to provide an inexpensive, relatively reproducible test method for estimating the immunity of installed medical devices.

Test results for a medical device apply only to that unit and to the frequency, modulation, and field strength characteristics of the RF test source. The medical device may be either susceptible or immune to other frequencies, modulations, and field strengths. Results may vary from unit to unit for the same model. Results may also be different over the short term as conditions change and over time as the medical device ages and undergoes service and maintenance.

## 1.4 Medical Device Performance

Verify the normal operation of the medical device with the RF transmitters turned off. After the test is completed, verify that the medical device operates normally.

During testing, the responses of the medical device should be recorded as a function of the WirelessLAN radio distance and orientation. The following is suggested as guide in noting device performance changes that might occur during the test. However, any deviations from normal operation should be noted.

1. No change in operation
2. Cessation of function without visible and/or audible alarm.
3. Cessation of function with visible and/or audible alarm.
4. Change in function or delivered therapy with alarm.
5. Change in function or delivered therapy without alarm.
6. Reboot or power down with loss of data.
7. Reboot or power down without loss of data.
8. Manual reset required to continue operation.
9. Change in mode or operational state without alarm.
10. Change in mode or operational state with alarm.
11. Visible and/or audible alarm with continuation of function.
12. Alarm malfunction or failure to alarm.
13. Change in measured and/or displayed data with change in operation.
14. Change in measured and/or displayed data without change in operation.
15. Change in audio indicator.
16. Distortion of displayed waveforms.
17. Display malfunction.
18. Recorder malfunction.
19. Error message or service code.

## 1.5 Recommended Test Distances

The WirelessLAN radios should be tested at the following test distances:

| Initial Test | l.0 m |
|---|---|
| Middle Distance l | 0.5 m |
| Middle Distance 2 | 0.25 m |
| Minimum Distance | 0.10 m |

If WirelessLAN is going to be used closer to the medical devices than the minimum distance recommended, then the minimum distance should be adjusted to the minimum operational distance. E.g. if the WirelessLAN radio is to be used within 2.0 cm of the medical device, then the minimum test distance should be changed to 2.0 cm (0.02 m).

## 1.6 Antenna Orientation

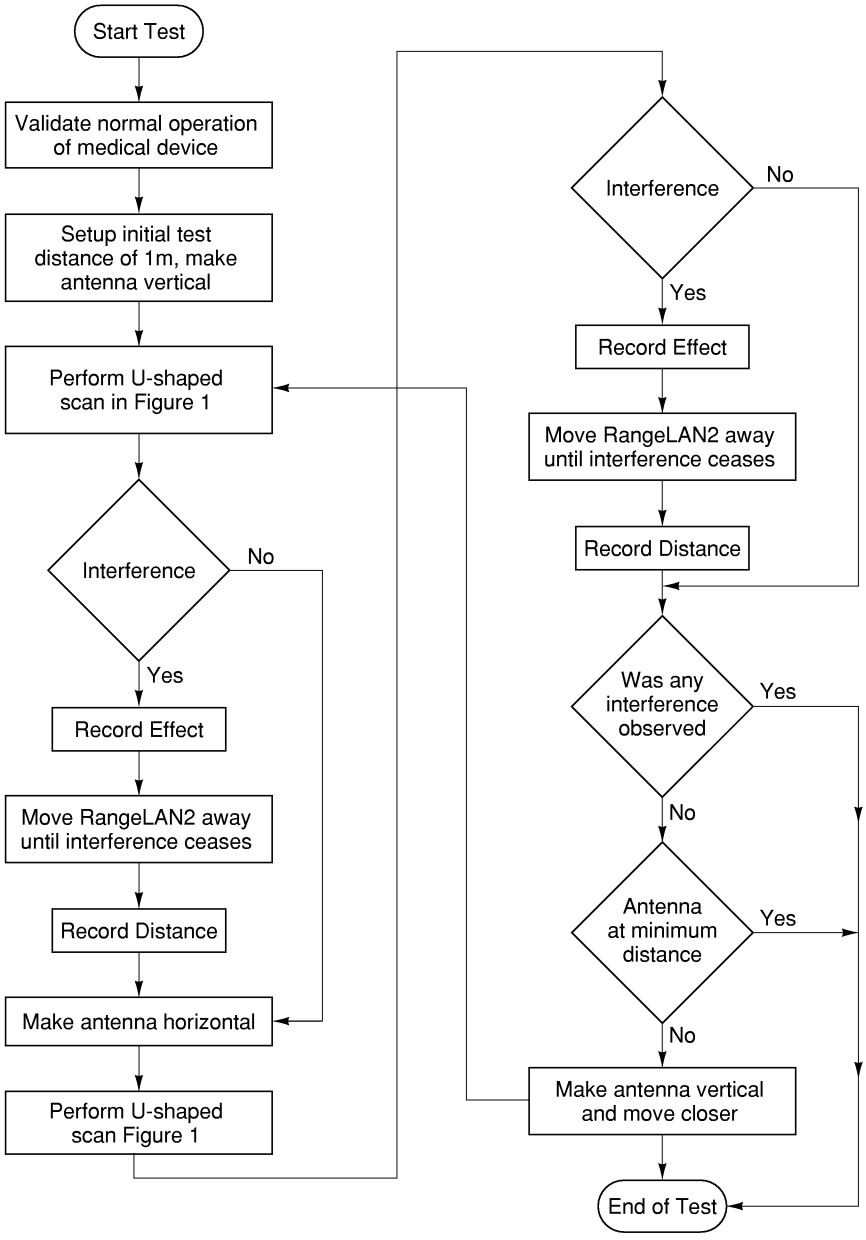
The WirelessLAN radio should be tested with its antenna in both a horizontal and a vertical orientation.

## 1.7 Platform for the WirelessLAN

The WirelessLAN radio should be tested in the same hand held computer that is going to be used within the healthcare facility. This will often be a PC notebook. The tests should be run twice: once using the hand held device without the WirelessLAN radio installed, and once with the WirelessLAN radio installed and operating.

## 1.8 Test Flowchart

The following diagram is a flowchart outlining the test procedure. The movement of the transmitter should be in the pattern of a “U”.



# Glossary of Terms

**Access Point**

An internetworking device that connects wired and wireless networks together.

**Bandwidth**

The width (in Hertz) of the frequency range that a signal occupies. Typical narrow band signals occupy 25 KHz. The GE Medical Systems wireless signals occupy 1 MHz.

**Bridge**

An internetworking device that incorporates the first two layers of the OSI model and allows connection of networks or subnetworks with similar architectures.

**Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)**

CSMA is a protocol in which each node senses whether or not a message has been posted on the media channel. CA is an optimization which listens before talking to avoid collisions.

**Channel**

The frequency hopping sequence.

**Direct Sequencing**

A spread spectrum technique by which the transmitted signal is spread over a particular frequency range.

**Federal Communications Commission (FCC)**

A U.S. government agency that regulates the use of Radio Frequency equipment.

**Frequency Hopping**

A spread spectrum technique by which the band is divided into a number of channels and the transmissions hop from frequency to frequency in a pre-specified sequence. A channel is a hopping sequence.

**Interference**

A situation that occurs when an unwanted RF signal occupies the same frequency band as a desired signal.

**Internet Protocol (IP)**

The messenger protocol of TCP/IP, responsible for addressing and sending TCP packets over the network.

**Internet Protocol Address (IP Address)**

A 32-bit address assigned to TCP/IP hosts. Used to identify a node on a network and to specify routing information on an internetwork. Each node on the internetwork must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID assigned by the network administrator.

**IP**

See Internet Protocol.

**ISA**

Industry Standard Architecture.

**ISO**

ISO's (International Standards Organization) seven-layer communications network architecture reference model. The seven layers include Application, Presentation, Session, Transport, Network, Data Link and Physical.

**MAC Address**

The address for a device as it is identified at the media access control layer in the network architecture.

**NDIS**

See Network Driver Interface Specification.

**Network Driver Interface Specification (NDIS)**

In **Windows** networking, the interface for network adapter drivers. All transport drivers call the NDIS interface to access network adapter cards.

**Packet**

A transmission unit of fixed maximum size that consists of binary information representing both data and a header containing an ID number, source and destination addresses, and error-control data.

**Port ID**

The method TCP and UDP use to specify which application running on the system is sending or receiving the data.

**Protocol**

A set of rules and conventions by which two computers pass messages across a network.

**Router**

An internetworking device which incorporates the first three layers of the OSI model and connects multiple networks together.

**Routing**

The process of forwarding packets to other gateways until the packet is eventually delivered to a gateway connected to the specified destination.

**Simple Network Management Protocol (SNMP)**

A protocol used to manage network activity.

**SNMP**

See Simple Network Management Protocol.

**Spread Spectrum**

A radio data transmission modulation technique by which the transmitted signal is spread over a bandwidth wider than the information bandwidth. Spread Spectrum bands are designated by the FCC and require no user license.

**Subnet**

On the Internet, a subnet is any lower network that is part of the logical network identified by the network ID.

**TCP**

See Transport Control Protocol.

**TCP/IP**

See Transport Control Protocol/Internet Protocol.

**Transport Control Protocol (TCP)**

A connection-based Internet protocol responsible for breaking data into packets, which the IP protocol sends over the network. This protocol provides a reliable, sequenced communication stream for internetwork communication.

**Transport Control Protocol/Internet Protocol (TCP/IP)**

A suite of protocols developed under DARPA sponsorship for internetworking. The Internet protocols used to connect a world-wide internetwork of universities, research laboratories, military installations, organizations, and corporations. TCP/IP includes standards for how computers communicate, and conventions for connecting networks and routing traffic.

**UDP**

See User Datagram Protocol.

**User Datagram Protocol (UDP)**

A TCP complement offering a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets. Optional UDP data checksums validate header and data, but do not enforce acknowledgments, leaving this to the application.

THIS PAGE INTENTIONALLY LEFT BLANK

# INDEX

## L



## M



## N



## O



## P



## Q



## R



## S

## T



## U



## W

THIS PAGE INTENTIONALLY LEFT BLANK