RoamAbout
802.11 Wireless Networking Guide

9034042-02

CABLETRON SYSTEMS

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Cabletron Systems, Inc.
35 Industrial Way
Rochester, NH 03867

Order Number: 9034042-02

Versions Supported: RoamAbout Access Point firmware – V5.0 and later
RoamAbout Access Point Manager software – V6.0 and later
RoamAbout PC Card driver – V4.0 and later
RoamAbout PC Card Station Firmware – V4.0 and later

Web Site: http://www.cabletron.com/wireless

Getting Help

For additional support related to this device or document, contact Cabletron Systems using one of the following methods:

World Wide Web	http://www.cabletron.com/wireless
FAX	(603) 337-3075
Phone	(603) 332-9400
Internet mail	support@cabletron.com
To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: **TechWriting@cabletron.com** *Make sure to include the document Part Number in the email message.*	

Before calling Cabletron Systems, please have the following information ready:

- Your Cabletron Systems service contract number
- A description of the problem
- A description of any action(s) already taken to resolve the problem
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, and so forth)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, and so forth)
- Any previous Return Material Authorization (RMA) numbers

Contents

3 Designing and Implementing a Wireless Network

4 Installing the Wireless Network Tools

5 Configuring the Wireless Network

6 Maintaining the Wireless Network

7 Problem Solving

A RoamAbout Product Specifications

Glossary

Index

Preface

A RoamAbout wireless network consists of RoamAbout wireless products, such as the RoamAbout PC Card and RoamAbout Access Point, and other wireless products that use an 802.11 Direct Sequence (DS) compliant radio.

This manual describes how to design, install, configure and maintain a RoamAbout wireless network. It also describes how to troubleshoot problems that may arise during installation or operation.

Intended Audience

This manual is intended for the wireless network manager. You should have a basic knowledge of Local Area Networks (LANs) and networking functions.

Associated Documents

The following lists each RoamAbout product and where to find additional information. These documents are available on the RoamAbout web site at:

www.cabletron.com/wireless

Component	Document
RoamAbout Access Point	*RoamAbout Access Point 2000 Hardware Installation Guide*
RoamAbout Access Point	*RoamAbout Access Point 2000 Hardware Installation Quick Start*
RoamAbout PC Card	*RoamAbout 802.11 PC Card Kit Installation*
	On-Line Help
RoamAbout PC Card MS-DOS/ Windows 3.1 Driver	*RoamAbout 802.11 PC Card MS-DOS and Windows 3.1 Installation Guide*
RoamAbout Client Utility	On-Line Help
RoamAbout Access Point Manager	On-Line Help
RoamAbout Outdoor Solution	*RoamAbout Outdoor Antenna Site Preparation and Installation Guide*

Chapter 1

Wireless Network Configurations

There are three basic RoamAbout wireless network configurations:

- One or more Access Points connecting wireless clients to a wired network, using the Workgroup Bridge mode. A wireless client can be any computer with an 802.11 Direct-Sequence (DS) compliant radio card. This type of network is referred to as a *wireless infrastructure network.*
- Two or more Access Points used as a wireless link connecting wired networks. This is called a *LAN-to-LAN configuration*. There are two variations of the RoamAbout LAN-to-LAN configurations:
    - — Point-to-Point which connects two wired networks, using the LAN-to-LAN Endpoint Bridge mode.
    - — Point-to-Multipoint which can connect multiple wired networks, using the LAN-to-LAN Multipoint Bridge mode.
- Wireless clients communicating among themselves without a connection to a wired network. This is called a peer-to-peer or *ad-hoc network*.

What a RoamAbout Access Point Provides

The RoamAbout Access Point is a 2-port bridge. One port connects to an Ethernet LAN. The other port connects to a wireless network. The wireless connection is provided by a RoamAbout 802.11 DS compliant PC Card.

Bridging Services

The RoamAbout Access Point provides the following bridging services:

- **Store-and-forward capability**

  The Access Point receives, checks, and transmits frames to other LANs, enabling the configuration of extended LANs.

- **Frame filtering based on address**

  Using the address database and the source and destination addresses from incoming frames, the Access Point isolates the traffic that should not be allowed on other LANs. This action reduces the total data traffic on an extended LAN by not forwarding the packets that have local destination addresses or packets that are not allowed to be forwarded. This increases bandwidth efficiency.

- **Data Link layer relay**

  The Access Point operates at the Data Link layer of the Open System Interconnection (OSI) model. Operation at this layer makes the Access Point transparent to the protocols that use the LAN connectivity service. This protocol transparency is a key factor in the extended LAN service.

- **Dynamic address learning**

  The forwarding and translating process module automatically adds new source addresses to the address database while the Access Point is operating. This reverse learning of the address and port association allows automatic network configuration without prior downline loading of configuration data to the Access Point. Address learning is protocol and management entity independent.

  An Aging Timer determines how long an address remains in the database. The timer measures the time since data was last addressed to or from a particular node. If the timer lapses without any traffic, the node's address is removed from the database. The Aging Timer interval can be modified by a Network Management System.

- **Workgroup Bridge mode**

  In Workgroup Bridge mode, the Access Point communicates with wireless clients. The Access Point learns addresses only from the wireless side of the network. The Access Point only forwards packets to multicast addresses, broadcast addresses, and known addresses on the wireless LAN. The default Aging Timer interval is 32 minutes.

- **LAN-to-LAN Endpoint Bridge mode**

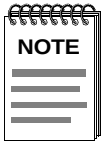
  In a Point-to-Point configuration, both Access Points are configured as Endpoints.

  In this mode, the Access Point filters packets based upon their destination address and forwards all packets with unknown addresses.

- **LAN-to-LAN Multipoint Bridge mode**

  This mode is used where multiple Access Points are configured as dedicated wireless links between LANs in a Point-to-Multipoint configuration. The LAN-to-LAN Multipoint option is only available on the Access Point 2000 with V6.0 or later firmware. One Access Point must be designated as the Central Access Point. The Central Access Point can communicate with up to six other Access Points configured as Endpoints.

  In this mode, the Access Point filters packets based upon their destination address and forwards all packets with unknown addresses.



You must purchase a license with a valid activation key to enable Multipoint bridge mode. Contact your Cabletron Representative.

Other RoamAbout Access Point Features

The Access Point includes the following features:

- Communication with any 802.11 Direct Sequence (DS) compliant radio in a wireless client.
- Support for up to 250 wireless users, per Access Point, in an infrastructure network.
- 802.11 Wired Equivalent Privacy (WEP 40-bit data encryption) and enhanced 128-bit data encryption.
- Secure Access, which requires clients to have the correct Wireless Network Name before it can join the wireless network.

- Roaming, where wireless clients can roam from one Access Point to another in the same wireless LAN without losing connectivity.
- Local management via its local console port or remote management by the RoamAbout Access Point Manager software, or Network Management Station (NMS).
- Support for RMON Groups 1, 2, 3, and 9 (Statistics, History, Alarms, and Events).
- Upgradeable via a downline-load using BOOTP and TFTP.
- 802.11 power management.
- 8000 node forwarding address database.
- Redundancy through an 802.1d Spanning Tree.
- Settable protocol filtering.
- Settable source and destination address filtering.

What a RoamAbout PC Card Provides

The RoamAbout PC Card is an IEEE 802.11 Direct Sequence (DS) compliant wireless network interface card.

The RoamAbout PC Card functions like any standard wired Ethernet card; however, the RoamAbout PC Card uses radio frequencies instead of a cable for the LAN connection. When installed in a computer, the PC Card and computer are referred to as a *RoamAbout wireless client.*

The RoamAbout PC Card includes the following features:

- Fits into any PC card type II slot.
- RoamAbout ISA Adapter Card option, which allows installation into computers that do not have a PC card slot but do have an available ISA bus slot.
- 802.11 DS compliant radio.
- Communication with 802.11 DS compliant Access Points or other 802.11 clients.
- RoamAbout Client Utility, which allows you to monitor the quality of wireless communication.
- Support for Windows 95, Windows 98, Windows NT, Windows 2000, MS-DOS, Windows 3.x, WinCE, Linux, and Apple PowerBook computers.
- 802.11 power management.
- Wired Equivalent Privacy (WEP) security.

- Roaming, where the client can move from one Access Point to another in the same wireless network without losing LAN connectivity.
- Roaming over multiple channels. The RoamAbout PC Card automatically uses the same channel as the associated Access Point.
- The RoamAbout PC Card is also used in a RoamAbout Access Point as the wireless port to provide wireless communication. For this manual, the Access Point with the PC Card are usually considered one unit.

Wireless Infrastructure Network

In a wireless infrastructure network, wireless clients communicate with an Access Point to connect to a wired LAN. A RoamAbout wireless infrastructure network can support clients with various operating systems, such as Windows 95, Windows 98, Windows NT, Windows 2000, MS-DOS, Windows 3.1, WinCE, Linux, and Apple Macintosh.

The area where a client can communicate with the Access Point is called a *coverage area*. To increase the coverage area, you can add Access Points to the wireless network.

Single Access Point

You can have one wireless infrastructure network with one Access Point. Each wireless client must communicate with the Access Point to connect to the wired network.

You can also have multiple wireless infrastructure networks, each with a single Access Point and different wireless names. Each network is a separate entity. Clients cannot roam between networks.

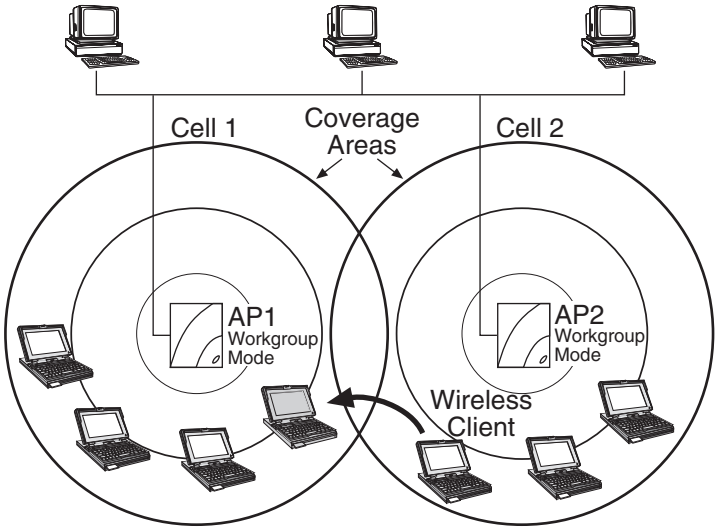
Multiple Access Points

A wireless infrastructure network can consist of multiple Access Points. This extends the coverage area of the wireless network. To allow roaming, each Access Point in the wireless network must use the same Wireless Network Name.

In this configuration, the wireless network consists of cells. A *cell* is a single Access Point and its wireless clients within a network of multiple Access Points.

Figure 1-1 shows two Access Points in the same wireless network.

Figure 1-1: Cells Within a Wireless Infrastructure Network Configuration



To allow wireless clients to physically move within a wireless network, the coverage areas should overlap. In Figure 1-1, Cell 1 and Cell 2 share overlapping areas of coverage. As a wireless client moves from Cell 2 to Cell 1, the necessary infrastructure network information is passed from AP1 to AP2 while maintaining LAN connectivity. The capability of moving from one Access Point to another without losing the network connection is called *roaming*.

When a wireless client (such as the laptop computer in Figure 1-1) approaches the outside boundary of a coverage area, the client can sense that another Access Point using the same Wireless Network Name is providing a better quality signal. The client then automatically switches to the other Access Point. If the other Access Point is using a different channel, the client automatically switches to that channel.

Wireless Client Behavior

You can configure the wireless client to connect to a specific wireless network or the first available wireless network.

If you configure the client to connect to a specific wireless network, the client establishes a radio connection to the Access Point in the specified wireless network that provides the best communications quality. Access Points in a different wireless network are ignored.

If you configure the client to connect to the first available wireless network (the Wireless Network Name = ANY), the client establishes a radio connection to the Access Point that provides the best communications quality. Be aware that if there are multiple wireless networks, the client could connect to an Access Point that is not in the network you want to join.

In either configuration, the client automatically matches the radio channel used by the Access Point.

A wireless client configured to connect to any available network does not automatically switch networks after it makes a connection to a wireless network; for example:

> Your wireless client is configured to connect to the first available wireless network. The first available network is called SouthSide. Once the connection is made, you move your client out of range of SouthSide, but in range of another wireless network called NorthSide. The wireless client loses the connection to SouthSide but does not make the connection to NorthSide. To connect to NorthSide, you need to restart the client. After the restart, the wireless client connects to NorthSide since it is the first available wireless network.

LAN-to-LAN Configuration

You can connect separate LANs over a wireless link by configuring two or more RoamAbout Access Points to communicate with each other. This is called a LAN-to-LAN configuration.

There are two variations of the RoamAbout LAN-to-LAN configuration:

- Point-to-Point, using the LAN-to-LAN Endpoint Bridge mode, which connects two wired networks.
- Point-to-Multipoint, using the LAN-to-LAN Multipoint Bridge mode, which can connect multiple wired networks.

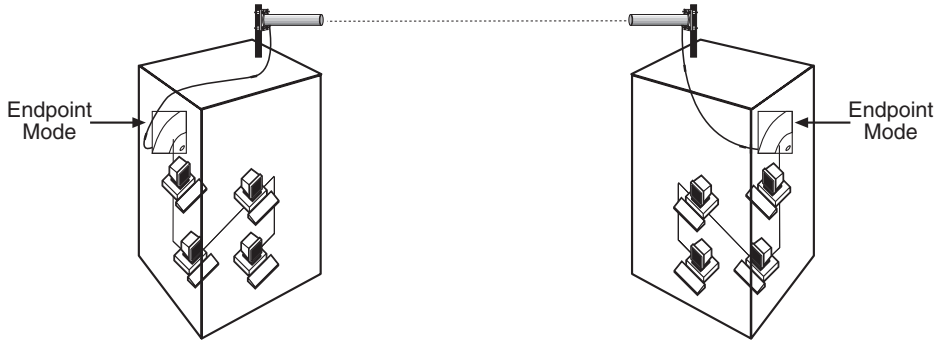
Typically, the Access Points are configured with outdoor antennas. If you use an outdoor antenna, you should have a professional antenna installation company perform the installation. Contact your Cabletron sales representative or visit the RoamAbout web site for more information about the outdoor antenna kits.

A Central Access Point uses an omni-directional antenna so that it can communicate with multiple Access Points in different directions. The Endpoint Access Points usually use a directional antenna pointed at the Central Access Point. The directional antenna allows you to increase the distance between Access Points. There must be a clear line sight between antennas to avoid a reduction in the signal level.

Point-to-Point

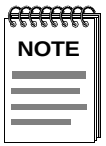
Figure 1-2 shows two Access Points, configured as LAN-to-LAN Endpoint Bridge mode, in different buildings using an outdoor antenna to connect the LANs in those buildings. As shown in the figure, both Access Points use a directional antenna. You can also configure the Access Points to connect two LANs in the same building.

Figure 1-2: Point-to-Point Configuration



Point-to-Multipoint

You can connect wired LANs in different buildings using the LAN-to-LAN Multipoint feature. At least one of the Access Points is configured as a Multipoint Access Point, called the Central Access Point. The Central Access Point can communicate directly with up to six Access Points. The six Access Points are configured as Endpoints, which can only communicate directly to the Central Access Point.



The Wireless Relay Setting must be enabled to allow the Endpoint Access Points in the configuration to communicate with each other through the Central Access Point.

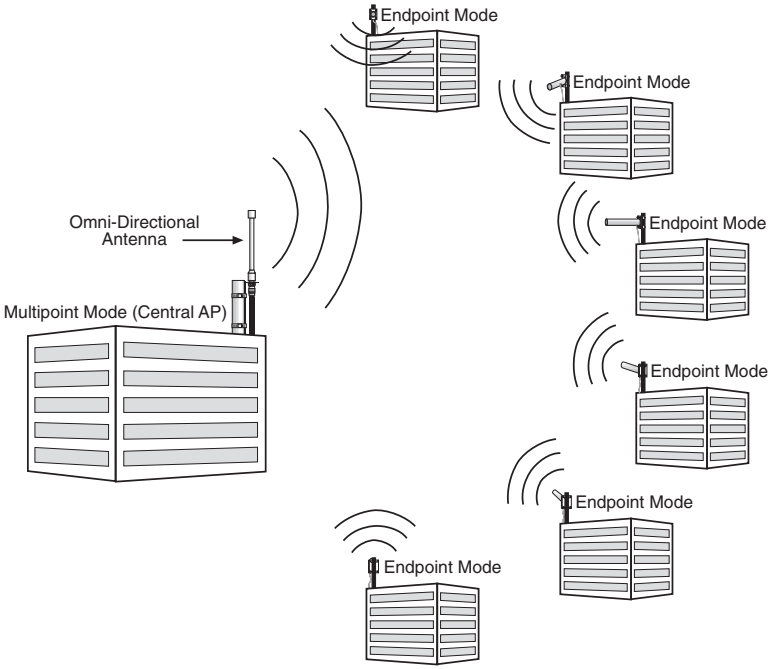
Configuration Examples

Figure 1-3 shows an example of a Multipoint configuration. You can have any of the following configurations:

- One Central Access Point with up to six Endpoint Access Points. The Endpoint Access Points can only communicate with the Central Access Point and not directly with each other. Therefore, the Central Access Point should be connected to the main wired LAN with the Wireless Relay setting disabled.

  If you enable the Wireless Relay Setting, each of the Endpoint Access Points in this configuration can communicate with each other through the Central Access Point.

Figure 1-3: Point-to-Multipoint Configuration



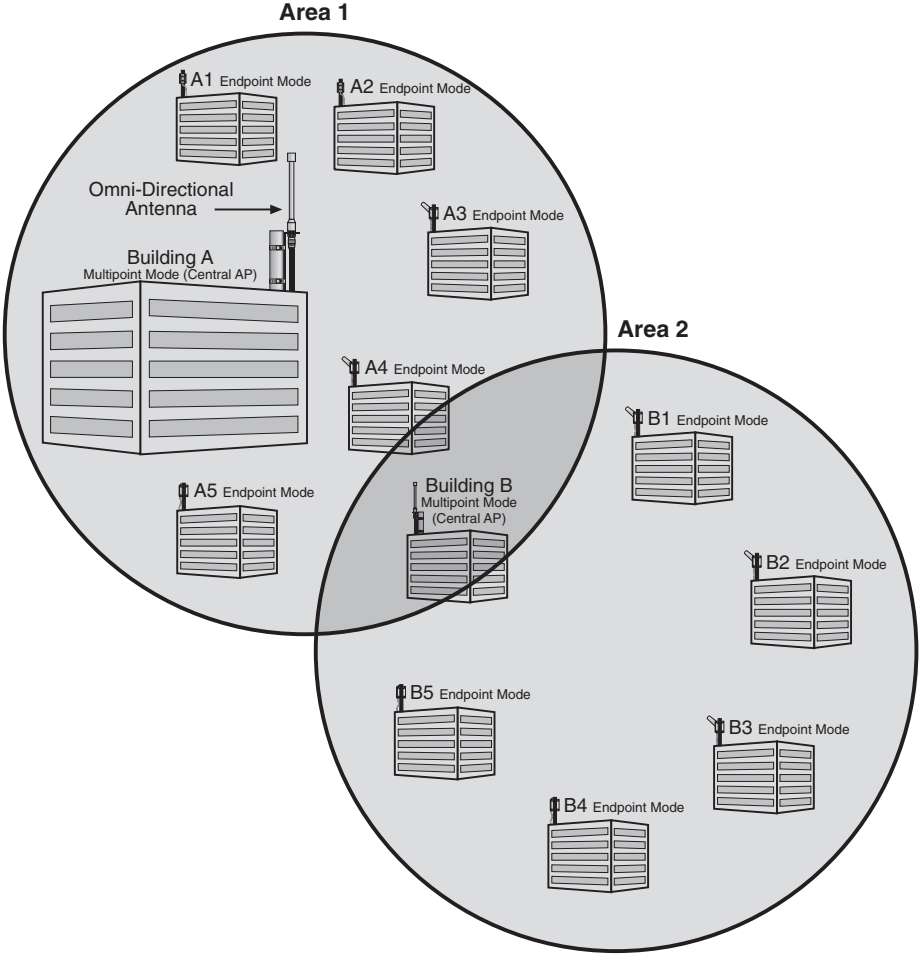
- Two or more Central Access Points in the same Point-to-Multipoint configuration. In this configuration, up to six Access Points are configured to communicate with the same Central Access Point. You can configure one or more of those six Access Points as a Central Access Point to communicate with up to five additional Access Points. This configuration requires Wireless Relay to be enabled.

  In Figure 1-4, Building A is the Central Access Point for Buildings A1 through A5 and Building B. However, Building B is also the Central Access Point for Buildings A and Building B1 through B5. You could expand this one further by making Building B3 a Central Access Point for five other buildings, although adding additional hops may decreases network performance.

  To avoid bridging problems, do not configure an Access Point as an Endpoint for more than one Central Access Point. In Figure 1-4, you would not configure Building B1 as an Endpoint to communicate directly to Building A.

  Figure 1-5 provides examples of configurations that cause network loops.

Figure 1-4: Point-to-Multipoint-to-Multipoint Configuration

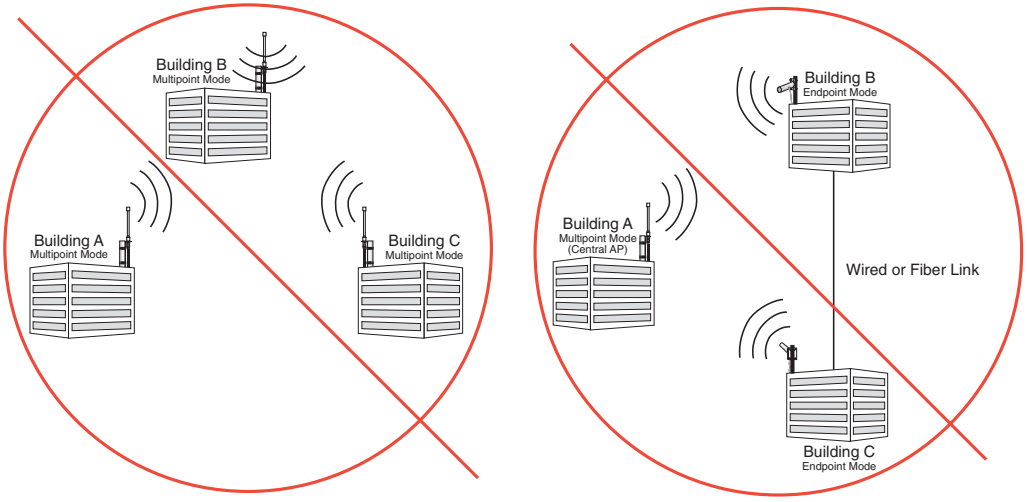


Preventing Network Loops

It is important to avoid Point-to-Multipoint configurations that will cause bridge loops. A bridge loop occurs when two parallel network paths are created between any two LANs, causing packets to be continuously regenerated through both parallel paths. This situation eventually renders the network unusable due to the excessive traffic that is being generated by the loop. The Access Point spanning tree function corrects this type of problem by shutting down the bridge and possibly shutting down a segment of the network.

Figure 1-5 provides examples of configurations that cause Network Loops.

Figure 1-5: Network Loops



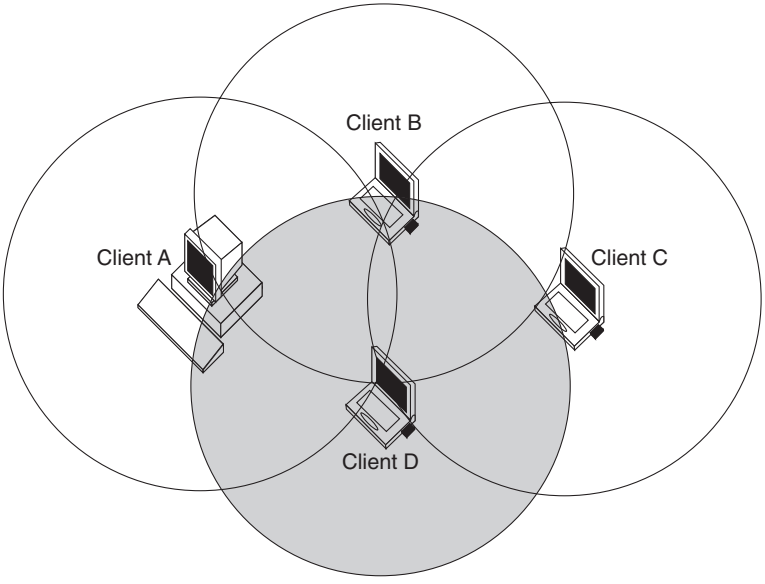
Ad-Hoc Network

Wireless ad-hoc networks do not include Access Points. Instead, the ad-hoc network is a loose association, or workgroup, of computers that can communicate with each other using the PC Card in Ad-Hoc Mode. Figure 1-6 shows an ad-hoc network.

The ad-hoc network is also known as a peer-to-peer network or independent network. The size of the ad-hoc network coverage area is determined by various factors, such as proximity and obstacles in the environment. In Figure 1-6, Client D has a coverage area (shown in gray) that touches all the other clients. This client can communicate with the other clients. Client C's coverage area does not touch Client A. These clients cannot communicate unless they move closer together.

The number of clients that the ad-hoc network can support is determined by the network utilization of each client. For example, a large number of clients could use the network for reading e-mail with very good network performance, but a few clients transferring large files could slow the network response time for all the clients.

Figure 1-6: Ad-Hoc Network



Optional Antennas

The RoamAbout PC Card has two integrated antennas that perform best in an open environment with as few obstacles as possible. Depending on the environment and wireless network configuration, you may need an optional antenna.

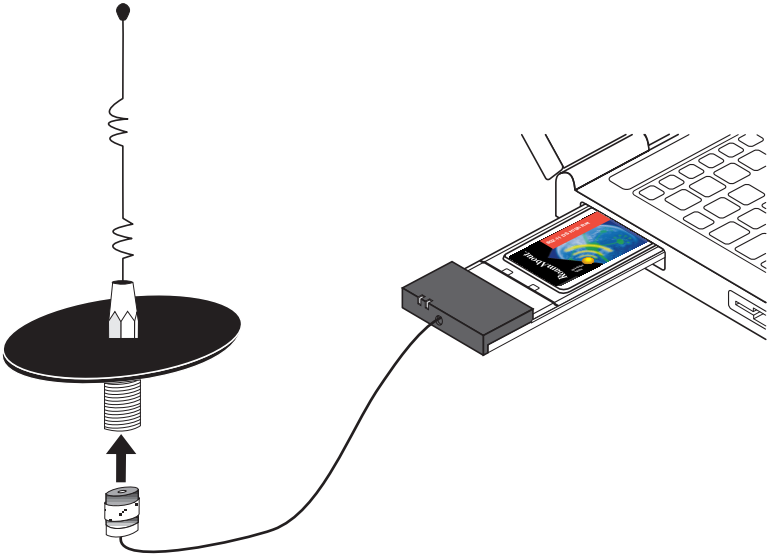
The following sections describe the types of optional antennas available with the RoamAbout products.

Vehicle-Mount Antenna

The RoamAbout Vehicle-Mount antenna (Figure 1-7) is a 5 dBi omni-directional antenna that connects vehicles with an on-board client to the wireless network. The sturdy design allows you to mount it on vehicles, such as the roof of a fork-lift truck, to allow continuous access to networked data, whether inside or outside of the building.

You connect the Vehicle-Mount antenna to the PC Card using the special 2.5 meter (8 foot) cable. To connect an antenna to the PC Card, insert the connector into the socket on the extended side of the PC card. To protect the socket from dust, it is shielded with a cap. You must remove the cap. See the "Vehicle-Mount Antenna Specifications" section on page A-7 for the antenna specifications. For mounting and installation instructions, see the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide*.

Figure 1-7: Vehicle-Mount Antenna



Range Extender Antenna

Use the Range Extender Antenna (Figure 1-8) to ensure optimal transmission and reception quality for situations where the integrated antennas are shielded, such as:

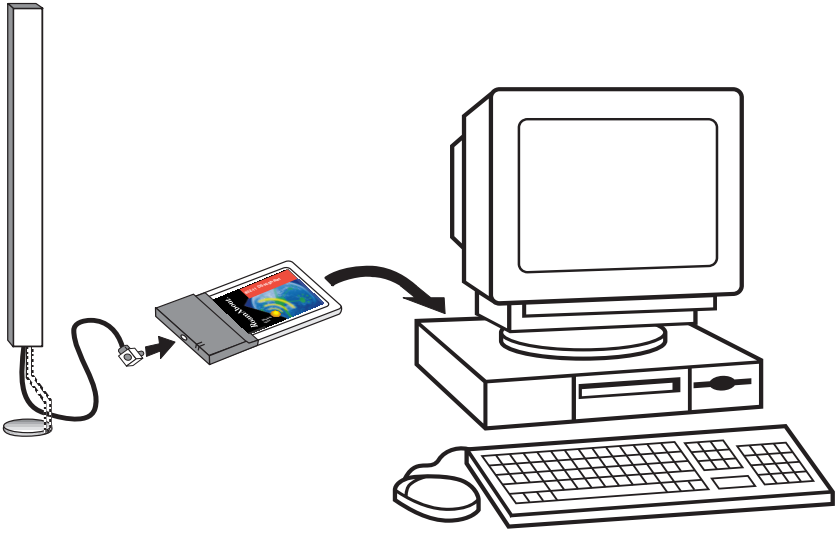
- The wireless device is close to metal surfaces.
- The wireless device is installed in a hidden location, such as in a cabinet.
- Objects shield the wireless device.

The Range Extender antenna has a mounting bracket and a base for vertical positioning that allows you to place the antenna on top of a table or cabinet, or attach it to the wall or ceiling. To connect an antenna to the PC Card, insert the connector into the socket on the extended side of the PC card. To protect the socket from dust, it is shielded with a cap.

Typically, the Range Extender Antenna is used with a desktop client. See the "Range Extender Antenna Specifications" section on page A-6 for the antenna specifications.

To avoid damage, do not place the Range Extender Antenna on top of, or close to a monitor. Many computer monitors have a degauss option. An electromagnetic discharge that may occur when degaussing the monitor may damage the antenna.

Figure 1-8: Range Extender Antenna



Outdoor Antenna Kit

There are two RoamAbout antennas available for outdoor use:

- 14-dBi directional antenna
- 7-dBi omni-directional antenna

The RoamAbout outdoor antennas support outdoor LAN-to-LAN wireless links that are used to connect separate LANs. The directional antenna is typically used in a Point-to-Point wireless link. The omni-directional antenna is typically used in a Point-to-Multipoint configuration. The omni-directional antenna can also be used in a wireless infrastructure network.

Refer to the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide* or the RoamAbout web site for more information.

Chapter 2

Understanding Wireless Network Characteristics

This chapter describes many of the wireless networking concepts and characteristics. You should be familiar with this information before you design, implement, or manage a RoamAbout wireless network. Not all characteristics apply to all of the network configurations.

Wireless Network Name

A wireless network name is the name of the wireless infrastructure network. To add an Access Point to an existing wireless network, configure the Access Point with the name of the wireless network. To create a new wireless infrastructure network, configure the Access Point with a unique wireless network name. The wireless network name is case sensitive.

For security, configure all the clients in the wireless network with the wireless network name. The Access Point has a Secure Access feature that only allows clients with the correct network name to access the network.

If security is not an issue, disable the Secure Access feature on the Access Point. Clients can be configured without a network name (the network name field is blank) or use **ANY** (all uppercase) as the wireless network name and still connect to the network.

The wireless network name is not used in an ad-hoc network or in a LAN-to-LAN configuration.

MAC Address

The MAC address is a unique identifier for networking devices. Each LAN device (including Ethernet cards, bridges, routers, and gateways) is identified by a unique factory-set MAC address.

RoamAbout Access Points have two MAC addresses:

- One MAC address for the wired Ethernet interface, which is printed on the Access Point.
- One MAC address for the RoamAbout PC Card installed in the Access Point, which is printed on a label on the back side of the card.

RoamAbout wireless clients are identified by the MAC address of the RoamAbout PC Card.

You cannot change the universal MAC address of a networking device. However, some network operating systems have a user-defined local MAC addressing scheme, which requires that each device be identified by a local MAC address value. The universal MAC address is aliased with a value according to the MAC addressing scheme. You can enter a local MAC address value on a RoamAbout client, but not on a RoamAbout Access Point. Most network systems do not require local MAC addresses.

Channel Frequencies

The channel sets the center radio frequency for the wireless device. The RoamAbout PC Card can support up to 14 channels; however, the number of available channels varies in different countries.

Access Points within the same wireless infrastructure network can be set to different channels. You can change the channel in an Access Point, but you cannot change the channel in a client. Instead, the client automatically uses the same channel as the Access Point. In an ad-hoc network, the client can only use the factory-set channel.

Wireless clients automatically switch to the Access Point's channel when roaming between Access Points in a wireless network; for example, there are two Access Points in a wireless network where Access Point 1 uses channel 1 and Access Point 2 uses channel 6. When connected to Access Point 1, the client automatically uses channel 1. When roaming to Access Point 2, the client automatically changes to channel 6.

To avoid radio interference, adjacent Access Points should be set to different channels that are at least five channels apart. The Access Points do not necessarily have to be in the same wireless network. For example, you have three Access Points whose coverage areas overlap; set the channels to 1, 6 and 11, if possible. Due to local radio regulations, not all channels are available in all countries.

In a LAN-to-LAN configuration, the Access Points must be set to the same channel.

In an ad-hoc network, all clients must use the same channel to communicate. Since the RoamAbout PC Cards use the same default channel, this is only an issue when clients use other PC Cards set to a different channel.

See the “Supported Frequency Sub-Bands” section on page A-5 for a list of channels supported by country.

Transmit Rate

The transmit rate identifies the preferred data transmission speed of the Access Point. The actual data transmission speed is subject to the type of PC Cards at both ends of the wireless link and the communications quality of the link.

Transmissions at faster rates allow for higher data throughput and quicker network response times. However, transmissions at lower rates are usually more reliable and cover longer distances than the higher rates. You might use a lower rate in the following situations:

- The client is at the extreme edge of the coverage area (see Figure 2-1). Using a lower rate covers the longer distance more reliably than a higher rate.
- There are numerous retransmissions due to a low signal level. Using a lower transmit rate prevents the PC Card from slowing network response times by transmitting data unsuccessfully at a higher rate then retransmitting at a lower rate.

As shown in Figure 2-1, an Access Point can have clients using different transmit rates in a wireless infrastructure network.

The following sections describe the auto rate and fixed rate settings.

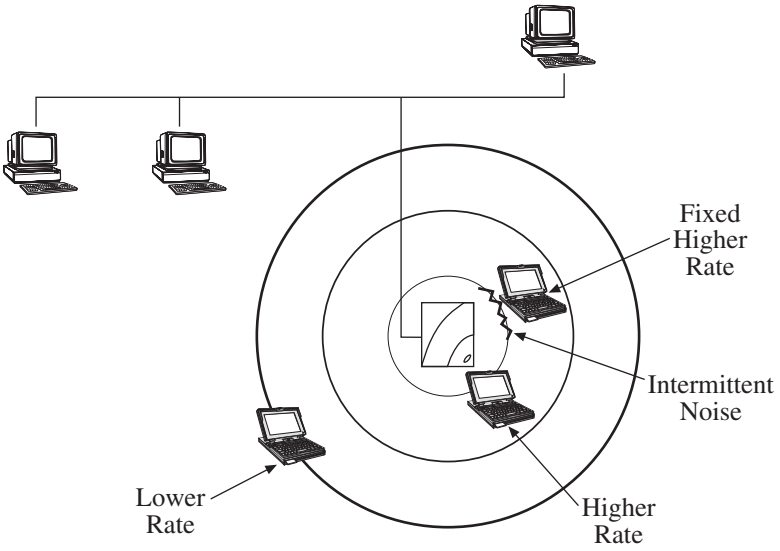
Auto Rate

With the Auto Rate option, the PC Card in a client or Access Point automatically switches to a lower rate when data transmissions fail more than once. Shortly after completing the transmission, the PC Card returns to transmitting data at the higher rate.

In most environments, Auto Rate allows the PC Card to use a higher rate for better data throughput, yet the PC Card can still use the more reliable slower rate when transmissions fail. A transmission can fail when the network experiences spurious noise interference.

Also use Auto Rate if you have Access Points with 11 Mbit/s PC Cards and a mix of clients with 11 Mbit/s and 2 Mbit/s PC Cards. The Access Point can communicate with both types of clients, but can communicate with the 11 Mbit/s clients at a higher rate than the 2 Mbit/s clients.

Figure 2-1: Using Various Transmit Rates



Fixed Rate

A fixed rate setting prevents the PC Card from retransmitting at a lower rate after a failed transmission. One example of why you would do this is when a microwave oven in the area produces noise in the same frequency as the wireless network (see Figure 2-1). The interference only occurs when the machine is in use. The interference may temporarily disrupt communications between a client and the Access Point. After a transmission fails more than once, the client retransmits at a lower rate. However, the interference also prevents communication at the lower rate. Retransmitting at a lower rate does not solve the problem and could decrease network performance. With fixed rate enabled, the client cannot retransmit at a lower rate.

A fixed transmit rate does not affect the receive rate. For example, an Access Point and a client both have 11 Mbit/s PC Cards, but the client is fixed to only transmit at 2 Mbit/s. The Access Point can send data at 11 Mbit/s to the client, and the client can respond by sending data at 2 Mbit/s.

However, you should not set the Access Point to a fixed rate of more than 2 Mbit/s if you have clients with 11 Mbit/s and 2 Mbit/s PC Cards. Otherwise, the 2 Mbit/s clients cannot communicate with the Access Point. The 2 Mbit/s clients can only receive data at a maximum of 2 Mbit/s.

Communications Quality

Communications quality is measured by the Signal to Noise Ratio (SNR). The SNR is a dynamic indicator that indicates the relative strength of the radio signal (signal level) versus the radio interference (noise level) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link between transmitter and receiver. A higher SNR value means a better quality radio link.

At the client, the RoamAbout Client Utility allows you to monitor the SNR, signal level, and noise level at the client. The client utility is provided in the RoamAbout PC Card kit.

For the Access Point, the Access Point Manager provides a Link Test diagnostic tool that monitors the SNR, signal level, noise level, and remote station capabilities.

Signal Level

The signal level values give you an indication of the distance between wireless devices. Using the RoamAbout Client Utility, you can observe a decrease of the signal level value when you move a client away from its Access Point. As an indicator for the communications quality, signal level should always be interpreted in combination with noise level:

- A high signal level with a low noise level provides excellent communications quality.
- A high signal level with a high noise level results in an average or poor SNR. Communications may not be as good as expected despite the strong signal level.
- A low signal level may still provide adequate communications when the noise level is relatively low.

Noise Level

The noise level indicates the presence of interference. Noise can be generated by various devices such as microwave ovens (2.4 GHz), elevator motors, and theft detection devices (like those used in retail stores). Noise level should always be related to the signal level:

- A low noise level with a high signal level provides excellent communications quality.
- A medium or high noise level with a high signal level results in an average or poor SNR. Communications may not be as good as expected despite the strong signal level.
- A high noise level most likely provides poor communications when the signal level is medium or low.

Data Throughput Efficiency

Data throughput efficiency is measured in transmissions sent, lost, or received. When a data transmission fails, the wireless device automatically retransmits the data. It is normal in many environments for a transmission to fail occasionally. Data is not lost since the wireless device automatically retransmits the data frames.

Many failed transmissions may result in longer network response times. Numerous retransmissions require more time and bandwidth to maintain network communication while contributing to the congestion of the medium. You can determine the amount of retransmissions in a wireless network using the RoamAbout Client Utility. The client utility is provided in the RoamAbout PC Card kit and is installed on clients.

AP Density and Roaming

AP Density is used to optimize the load balance of the number of wireless clients per Access Point. AP Density affects the sensitivity of the radio receiver, which determines when clients roam from one Access Point to another. *Roaming* allows wireless clients to move between cells in a wireless infrastructure network without losing the connection to the network.

The RoamAbout client can sense all the Access Points in a wireless network that are within range. As you move the client away from its Access Point and the SNR decreases, the client automatically switches to an Access Point with a better SNR. The client also changes its frequency channel to match the Access Point. The transition is transparent where the user is not aware that a transition occurred. Changing the AP Density to account for the distance between Access Points allows the clients to roam between Access Points more efficiently.

AP Density is not used in LAN-to-LAN configurations or the ad-hoc network.

The AP Density setting must be the same for all Access Points and wireless devices in your wireless network. Failure to do so may cause unpredictable results for the wireless client in your network.

Using non-matching values may seriously affect the wireless performance of the client. If Access Points are set to a High AP Density, a client with a Low AP Density may continue to transmit to the same Access Point instead of roaming. Meanwhile, the Access Point ignores the client because the client's transmissions fall below the receiver threshold. If the Access Points are set to a Low AP Density, a client with a High AP Density may try to prematurely roam to another Access Point.

There are three AP Density parameters available:

- **Low** (default). The Low setting provides maximum coverage using a minimum number of Access Points. This option is typically used for single-cell networks, but also provides an efficient and cost effective solution for networks that include multiple wireless clients.
- **Medium**. The Medium setting can be used for environments where Access Point stations experience slow response times even when the radio communication is excellent.
- **High**. The High setting should only be used when you are designing a wireless infrastructure that includes a high concentration of Access Point devices.

RTS/CTS Protocol

Each device in a wireless network can sense transmissions from other devices in its network that use the same frequency. To avoid collisions and lost data, a device only transmits when it senses that no other device is transmitting. This behavior is referred to as the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol. The RTS/CTS (Request to Send/Clear to Send) protocol is useful when collisions do occur. Collisions can occur if:

- Two clients are unable to sense each other's transmissions and simultaneously transmit to the Access Point.

The RTS/CTS protocol forces a wireless device to perform the following.

- When a packet to be transmitted is shorter than the RTS/CTS threshold, the device transmits when it senses that the medium is free. The RTS/CTS protocol is not used.

A shorter packet is less likely to have a collision than a longer packet.

- When the packet exceeds the threshold, the device sends an RTS message and waits until the receiving device responds with a CTS message.

The RTS message includes the length of the frame that the device wishes to transmit. The receiving device includes this information as a radio-silence time indicator in its CTS response message. The CTS message announces to all the devices in the wireless network which device is allowed to transmit its message. All other devices defer their transmissions for the radio-silence time identified in the CTS message.

Access Point - RTS Threshold

The RTS Threshold on a RoamAbout Access Point specifies the packet size of transmissions, where messages larger than the specified size must use the RTS/CTS protocol. The default value, 2347, effectively turns off the RTS Threshold.

A lower RTS Threshold is useful when collisions frequently occur at the Access Point. This can be caused when the Access Point and a client (or Access Point in a LAN-to-LAN configuration) transmit data to each other simultaneously. A lower RTS Threshold forces the Access Point to send an RTS to the device before transmitting a packet that exceeds the threshold. The Access Point waits until the device responds with a CTS message.

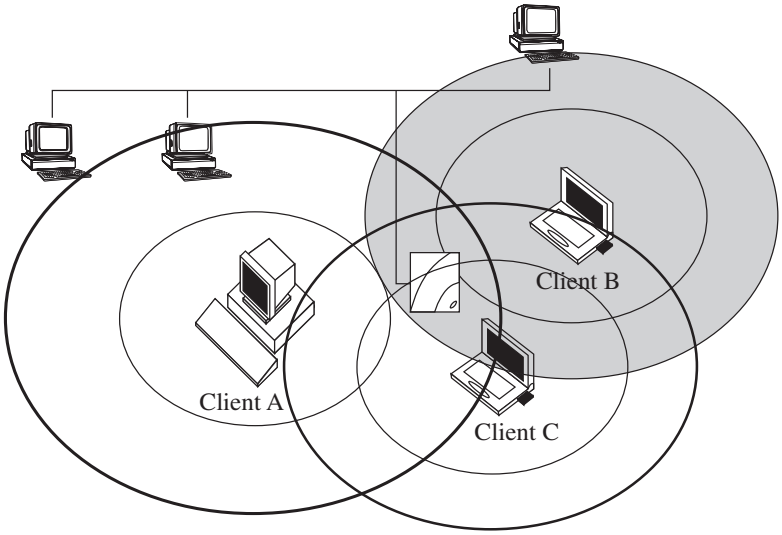
Lowering the RTS Threshold imposes additional network overhead that could negatively affect the throughput performance. You should only lower the RTS Threshold when the wireless network experiences frame collisions and lost messages.

Wireless Client - Medium Reservation

Use Medium Reservation to resolve a hidden station problem. A wireless device is a hidden station when its transmissions cannot be sensed by another wireless device in the same network. Therefore, multiple devices could transmit at the same time. This problem can occur with clients located at opposite ends of an Access Point coverage area.

Figure 2-2 illustrates a hidden station example. Clients A and B are within range of the Access Point. However, Client B cannot sense transmissions from Client A, since Client A is outside of Client B's coverage area (shown in gray). Client B could transmit while Client A is transmitting. Therefore, messages of both Client A and B collide when arriving simultaneously at the Access Point. The collision results in a loss of messages for both clients. Figure 2-2 also illustrates that Client C is not hidden from the other clients.

Figure 2-2: Hidden Station Example



To avoid a hidden station problem, move the clients or Access Point if possible so that the devices can sense each other's transmissions. Otherwise, set Medium Reservation on the clients with the problem to the **Hidden Stations** setting, which imposes an RTS/CTS Threshold value of 500. You do not change the RTS Threshold on the Access Point.

Medium Reservation forces the client to send an RTS to the Access Point before transmitting a packet that exceeds the threshold. The client waits until the Access Point responds with a CTS message. However, Medium Reservation imposes additional network overhead that could negatively affect the data throughput performance. You should only use this setting when the density of clients and Access Points is low and you witness poor network performance due to excessive frame collisions at the Access Points.

802.11 Power Management

Power management can extend the battery life of clients by allowing the client to sleep for short periods of time while its messages are buffered by the Access Point.

You may need to balance wireless performance versus battery-life. Power management imposes a more active use of the wireless medium, which might lead to more frequent transmission delays experienced as slower network response times during file transfers.

With slower response times, the client may spend more time in operational mode resulting in less effective power management. In such cases, disabling power management on the client might result in better throughput performance.

The RoamAbout PC Card 802.11 power management is separate from any power management function on your computer.

RoamAbout Access Point

The RoamAbout Access Point automatically supports 802.11 power management. The only parameter that can be set is the Delivery Traffic Indication Message (DTIM) interval, which sets the buffering time. The default value of 1 corresponds to 100 milliseconds of sleep time. It is highly recommended that you do not change this value.

RoamAbout Client

You can enable or disable power management on a RoamAbout client. With power management enabled, the client goes into sleep mode to minimize power consumption. The wireless traffic is buffered in the Access Point that the client uses to connect to the network.

At regular intervals (defined by the Maximum Sleep Duration field), the client checks for network traffic addressed to the client. If there is no traffic addressed to the client, the client returns to sleep mode. If traffic is buffered at the Access Point, the client collects the buffered messages prior to returning to sleep mode.

The following discusses how power management can impact data throughput of the wireless network.

- Transaction processing applications show little or no difference in network performance when using power management. Examples of this type of application are hand-held scanners or clients that use the wireless network only to send and receive e-mail.
- You may experience longer network response times when you transfer large files between the network and the client while power management is enabled. The size of the files and the recurrence of file transfers are a factor. If modifying a document over the network, any auto save feature could cause frequent file transfers.
- The Access Point could cause longer network response times if a number of clients use the same Access Point for buffering messages while in sleep mode.

There are two power management parameters on RoamAbout clients:

- **Receive All Required Multicasts**. Keep this enabled to receive multicast messages from the wireless network. Missing these messages might result in losing the network connection or other network problems.

  You can disable this option to achieve the best possible power savings. However, make sure that the wireless LAN, the higher layer protocols of the network system, and the application running on your device do NOT need multicast messages for proper communication.

An example of when you can disable this option is when your wireless device is a hand-held scanning device communicating to a network via a single protocol system.

- **Maximum Sleep Duration**. This is the listen interval in milliseconds that the client applies to verify if there is traffic on the network addressed to the client. You should not change the default value of 100 milliseconds, since this may interfere with the operation of the network operating system.

  However, a value between 100 and 500 milliseconds may be considered when operating a wireless powered hand-held terminal connected to a network infrastructure that can handle a less critical latency for optimal performance.

Security

The following lists the types of security in a RoamAbout wireless environment:

- Network operating system security
- RoamAbout Access Point Secure Access
- Wired Equivalent Privacy (WEP) Encryption
- Simple Network Management Protocol (SNMP) community names
- Console port password

Network Operating System Security

To access networking data or services, a wireless client needs to run an appropriate network operating system. Most network operating systems use standard security measures such as login names and passwords.

When you follow the standard network security procedures and guidelines recommended for your network operating system, an unauthorized user cannot access network data or services without the appropriate user name and password.

For detailed information, consult the documentation that came with the network operating system or refer to the reseller of your LAN software.

RoamAbout Access Point Secure Access

When Secure Access is enabled, the Access Point denies access to wireless clients that do not use the correct wireless network name. When Secure Access is disabled, the Access Point allows access to clients that use **ANY** (all uppercase) as the wireless network name or have a blank wireless network name.

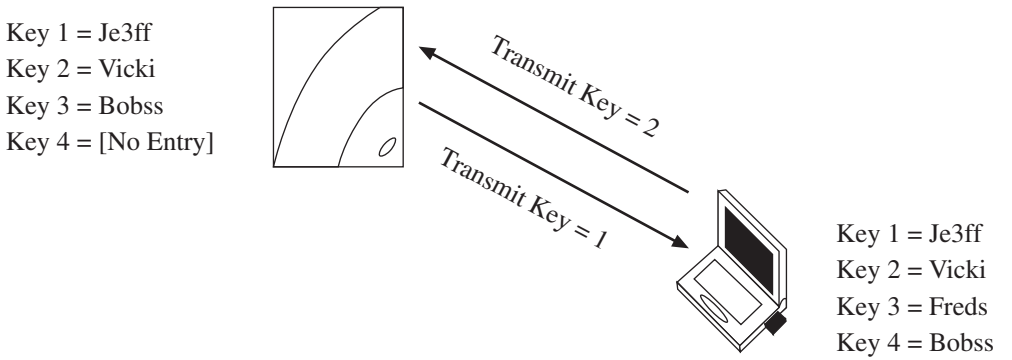
Wired Equivalent Privacy (WEP) Encryption

The WEP feature encrypts all data transmitted within the wireless network. The encryption uses the RC4 algorithm as defined in the IEEE 802.11 Wired Equivalent Privacy standard.

The RoamAbout devices can be configured with four encryption keys. Each key is placed in a specific position (Key 1, Key 2, Key 3, or Key 4). You select one key to encrypt transmitted data. To decipher the data, the receiving wireless device must have the key used to encrypt the data in the same position as the sending device.

The receiving device can transmit data back to the sending device using a different key for transmission, as long as the other device has the transmitting key in the same position. In Figure 2-3, the Access Point uses Key 1 to encrypt transmitted data, which the client can decipher. If the Access Point uses Key 3 to encrypt transmitted data, it cannot be deciphered by the client. The Bobss key is Key 3 on the Access Point but Key 4 on the client.

Figure 2-3: Using Encryption



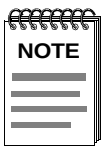
As shown in Figure 2-3, the Access Point uses Key 1 to encrypt transmitted data and the client uses Key 2 to encrypt transmitted data. Both devices can communicate.

In a wireless infrastructure network, you can:

- Configure the Access Points to only accept encrypted data from clients. Only clients that have the correct encryption keys can participate in this network.
- Configure the Access Points to accept encrypted data from clients with encryption enabled, and unencrypted data from clients without encryption enabled. This allows clients who require security to use encryption without preventing other clients from using the network.

In a LAN-to-LAN configuration, use encryption to have a secure wireless link.

In an ad-hoc network, use encryption to prevent uninvited users from joining the network.



Broadcast and multicast messages are not encrypted.

SNMP Community Names

The SNMP community name allows management tools using SNMP to display or modify Access Point parameters remotely. The Access Point supports a read/write community name and a read-only community name.

By default, the Access Point uses **public** as the default read/write community name. This allows any management tool using SNMP to access the Access Point and change parameters. By changing the read/write community name, users must enter the correct community name to modify the Access Point parameters.

The read-only community name allows the management tools to view but not change the Access Point parameters. You can change the read-only name so that users must enter the correct name before they can view the Access Point parameters.

Console Port

The RoamAbout console port has two security features:

- You can configure the console port to require a password before users can access the Installation Menu.
- You can configure the console port to prevent any management system from using SNMP to modify the encryption parameters.

Network Protocols

When you install a RoamAbout PC Card in a computer using a Windows operating system, you may need to install and configure a set of networking protocols. The type of protocols needed depends on the network operating system used within your LAN environment. The most common protocols are:

- IPX/SPX compatible protocols if your networking environment is using the Novell NetWare network operating system.
- NetBEUI if you want to use file and print sharing supported by Microsoft Client for Microsoft Networks.

- TCP/IP if you want to connect your computer to a network that uses IP addressing or you would like to connect to the Internet.

These networking protocols can operate simultaneously with other networking protocols.

When you install a RoamAbout PC Card in an Apple computer, you may need to install and enable Apple's Open Transport or Apple Classic network protocols along with TCP/IP.

Wireless Traffic

In addition to data, wireless network traffic includes beacons and various types of messages.

Beacons

A *beacon* is a message that is transmitted at regular intervals by the RoamAbout Access Points to all wireless clients in the wireless infrastructure. Beacons are used to maintain and optimize communications by helping mobile RoamAbout clients to automatically connect to the Access Point that provides the best communications quality.

Beacons are transmitted at 2 Mbit/s when the transmit rate is set to auto rate, as described in the "Transmit Rate" section on page 2-3. If the transmit rate is fixed, the beacons are transmitted at the fixed rate.

Message Types

When a device in the wireless network transmits data, it can take one of these forms:

- Broadcast - A data message transmitted by one device to all devices in the network.
- Multicast - A data message transmitted by one device to multiple devices in the network. Unlike broadcast messages, multicast messages do not always include all devices in the network.

  By default, the Access Point is configured to limit multicast traffic to 100 Kb/sec. Changing this parameter could cause multicast traffic to use more network bandwidth. Should a broadcast storm occur when this parameter is disabled, the multicast traffic could cause a serious degradation of network performance.
- Unicast - A data message transmitted by one device to another device.

Broadcast and multicast messages are transmitted at 2 Mbit/s when the transmit rate is set to auto rate, as described in the "Transmit Rate" section on page 2-3. If the transmit rate is fixed, the broadcast and multicast messages are transmitted at the fixed rate.

Protocols and Filters

The RoamAbout Access Point has two types of filters:

- Protocol filter
- MAC address filter

Use the protocol filter to NOT forward specific protocol traffic to the wireless network, which can reduce unnecessary traffic and increase the network response time. However, filtering the wrong protocols can negatively affect the operation of the network. When solving network problems, you should clear all filters.

Use the MAC address filter to NOT forward traffic being sent to a specific device. The device can be on either side of the Access Point (wired or wireless). All traffic destined for the device with the specific MAC address is not forwarded by the Access Point.

These filters are only available using the Access Point Manager program or a Network Management Station that uses SNMP.

Spanning Tree Protocol

The RoamAbout Access Point uses 802.1d Spanning Tree Protocol to prevent network loops. A loop occurs when there are alternate routes between networks. A loop can cause bridges to continually forward multicast traffic and degrade network performance.

You can enable or disable the Spanning Tree when in Endpoint bridge mode on Access Points with the V5.01 or later firmware release. Spanning Tree is disabled when in Workgroup bridge mode and enabled in Multipoint bridge mode.

In normal LAN-to-LAN operation, keep Spanning Tree ENABLED. You should only disable Spanning Tree when using an application in a configuration that requires it, such as using the SmartTrunk feature found on the Cabletron SmartSwitch product line for load balancing.

Avoiding Bridge Loops in Point-to-Multipoint Configurations

It is important to avoid Point-to-Multipoint configurations that will cause bridge loops. A bridge loop occurs when two parallel network paths are created between any two LANs, causing packets to be continuously regenerated through both parallel paths. This situation eventually renders the network unusable due to the excessive traffic that is being generated by the loop. The Access Point spanning tree function corrects this type of problem by shutting down the bridge and possibly shutting down a segment of the network.

RoamAbout Access Point SNMP Management

The Access Point supports the Simple Network Management Protocol (SNMP) through any standard Network Management Station (NMS) that supports SNMP. The SNMP management capability enables you to manage standard SNMP MIB characteristics, such as protocol filtering and address filtering.

The management systems use MIB objects to manage the Access Point. The Access Point supports the following MIB objects:

- MIB II (RFC–1213)
- IETF Bridge MIB (RFC–1493)
- Ethernet MIB (RFC–1398)
- DEC ELAN Vendor MIB
- HUB PCOM MIB
- RoamAbout Access Point MIB
- RMON MIB (RFC–1757)
- 802.11 MIB

To perform SNMP management on the Access Point, you must assign it an IP address. Also, the Network Management Station needs to have the Access Point read/write community name. The default community name is **public**.

Chapter 3

Designing and Implementing a Wireless Network

The first step in designing a wireless network is to determine which network configuration best fits your needs. The wireless network configurations are discussed in Chapter 1.

Once you have chosen a configuration, this chapter lists the various site requirements necessary for each type of network.

Infrastructure Network

To plan a wireless infrastructure network, determine the following:

- Coverage area - the area where the clients are located. If the clients are mobile, this is the area where the clients can connect to the network.
- Supported users - the number of clients that you expect to support.
- Network utilization - how users intend to use the network. Utilization includes frequently transferring large files (heavy utilization) or only accessing e-mail (light utilization).

These factors, described in the following sections, help you to determine the amount of Access Points needed. Afterwards, you need to examine the Access Point hardware requirements and the wireless client system requirements.

When designing a wireless network, consider the security issues for your environment. Security can include keeping the Access Point in a locked closet, preventing unauthorized users from joining the wireless network, and using data encryption to ensure that sensitive data is kept private.

Determining the Coverage Area and Supported Users

Coverage area is determined by a number of factors, including physical obstructions and noise levels as shown in Figure 3-1.

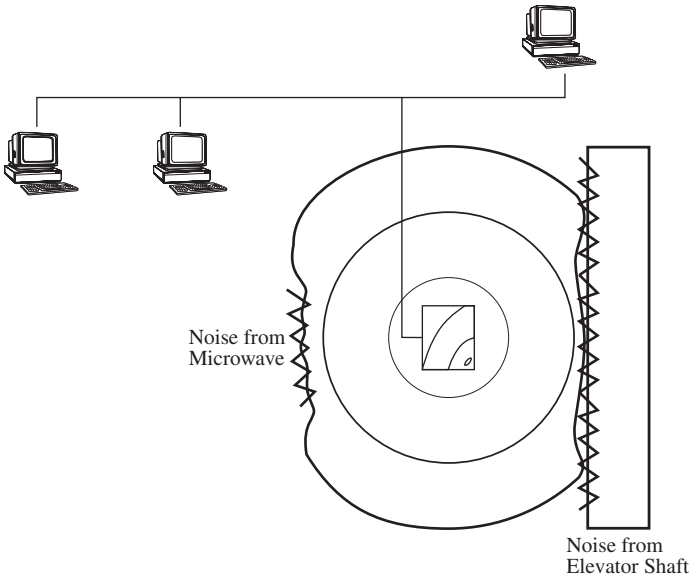
The following is an example of the coverage area in a semi-open environment, which is defined as work space divided by shoulder-height, hollow wall elements. The distances in your environment may be different.

- 11 Mbit/s - 165 feet (50 meters)
- 5.5 Mbit/s - 230 feet (70 meters)
- 2 Mbit/s - 300 feet (90 meters)
- 1 Mbit/s - 375 feet (115 meters)

The faster the transmit speed, the shorter the coverage area at that speed. An Access Point with an 11 Mbit/s PC Card can communicate with clients up to a distance of 375 feet in a semi-open environment. However, only clients within the first 165 feet can communicate at 11 Mbit/s. Clients between 165 and 230 feet communicate at 5.5 Mbit/s. Clients between 230 and 300 feet communicate at 2 Mbit/s; and clients between 300 to 375 feet communicate at 1 Mbit/s.

Noise levels in the radio frequencies can reduce the coverage area. Such noise can be generated by microwave ovens and elevator motors.

Figure 3-1: Coverage Area



A RoamAbout Access Point can support up to 250 users within its coverage area. However, this number can be significantly reduced by various factors, such as noise or obstructions in the coverage area, and the network utilization by each client. If your desired coverage area is larger or the number of users is greater, you need to install multiple Access Points.

Be aware of potential hidden station problems. If possible, arrange the coverage area to minimize or prevent any two clients from being within range of the Access Point, but out of range from each other.

Selecting the Location for a Single Access Point

The Access Point should be placed as close as possible to the center of the planned coverage area. If it is necessary to install the Access Point in an obstructed location, use the optional Range Extender antenna to extend the coverage area of the Access Point. The Range Extender antenna should also be used if, for security reasons, you need to install the Access Point in a closed location, such as a closet. Before mounting the Access Point, review the hardware requirements described in the installation documentation that came with the RoamAbout Access Point.

For best placement, configure the Access Point and a client and use the procedure in the "Optimizing RoamAbout Access Point Placement" section on page 6-6 before permanently mounting the Access Point.

Selecting the Locations for Multiple Access Points

Consider the following:

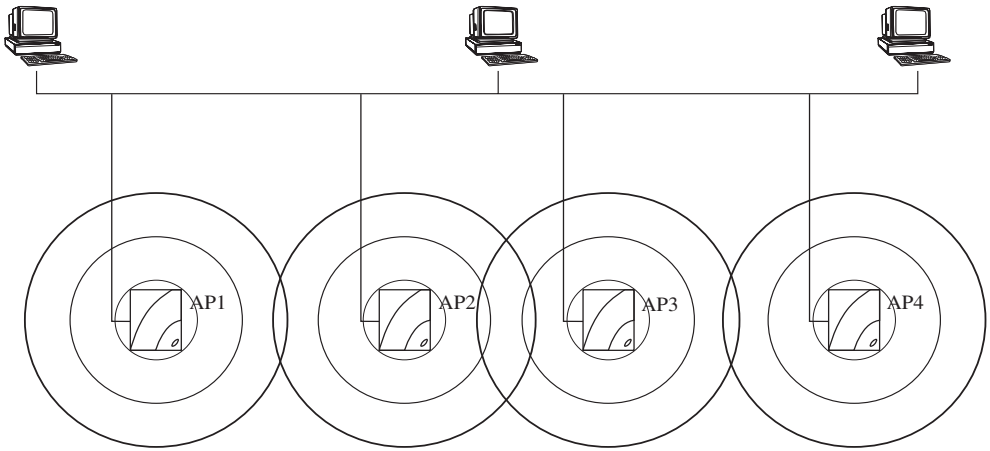
- Each coverage area must overlap another coverage area to allow roaming for clients.
- The amount of overlap depends on number of users in a coverage area and utilization of the network.

  If you expect that one coverage area has more users or higher network utilization than the other coverage areas, increase the overlap of the adjacent coverage areas by moving the Access Points closer together (see Figure 3-2).
- If possible, have the adjacent Access Points whose coverage areas overlap use different channels that are at least five channels apart.
- Be aware of potential hidden station problems. If possible, arrange the coverage area to minimize or prevent any two clients from being within range of the Access Point but out of range with each other.

For best placement, configure the Access Point and a client and use the procedure in the "Optimizing RoamAbout Access Point Placement" section on page 6-6 before permanently mounting the Access Point.

Before mounting the Access Point, review the hardware requirements described in the installation documentation that came with the RoamAbout Access Point.

Figure 3-2: Overlapping Coverage Areas



Using Multiple Wireless Infrastructure Networks

Instead of creating multiple cells in a single infrastructure network, you can have separate infrastructure networks. The advantages include:

- Preventing too many users from roaming to a particular coverage area by configuring some users to use one network, and other users to a different network. This is a form of load balancing.
- Creating a secure network for security-sensitive users and a general, less secure network for other users. For example, on a college campus you can create a wireless network that uses encryption for use by the faculty, and a wireless network that does not use encryption for use by students.

The coverage areas of Access Points in different networks can overlap without interference as long as they use different channels. If possible, have the Access Points use different channels that are at least five channels apart.

Using an Outdoor Antenna

You can extend the coverage area of a wireless infrastructure network by connecting an outdoor omni-directional (7 dBi) antenna to the Access Point.

Typically, you only use the omni-directional antenna in an indoor/outdoor environment, such as in and around a warehouse. Also, the clients should be configured with the RoamAbout Vehicle-Mount antennas. Refer to the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide* for the procedures to install a RoamAbout outdoor antenna.

LAN-to-LAN Network Configuration

There are two types of LAN-to-LAN configurations. The LAN-to-LAN Endpoint Bridge mode is used in a Point-to-Point configuration to connect two separate wired LANs. The LAN-to-LAN Multipoint Bridge mode is used in a Point-to-Multipoint configuration to connect multiple wired LANs. Typically, the LANs are in different buildings and the configuration requires the RoamAbout outdoor antenna kit.

Consider the following:

- Type of antenna. Use two directional antennas in a Point-to-Point link. Use one omni-directional antenna and up to six directional antennas in a Point-to-Multipoint configuration.
- Outdoor antenna installation. You should use a professional antenna installation company to install the outdoor antennas.
- Grounding system. The Access Point and the outdoor antenna must use the same grounding system.
- Connecting of the outdoor antenna to the Access Point, and connecting the Access Point to the wired LAN.

Refer to the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide* for the detailed procedures to determine distances and install an outdoor configuration.

If you are not using an antenna, the Access Points should be within each other's coverage area. The speed you wish to use for your wireless link is one factor that determines the distance between the Access Points. Other factors include physical obstructions and noise levels. The following is an example of the coverage area in a semi-open environment, which is defined as work space divided by shoulder-height, hollow wall elements. The distances in your environment may be different.

- 11 Mbit/s - 165 feet (50 meters)
- 5.5 Mbit/s - 230 feet (70 meters)
- 2 Mbit/s - 300 feet (90 meters)
- 1 Mbit/s - 375 feet (115 meters)

Before mounting the Access Point, review the hardware requirements described in the installation documentation that came with the RoamAbout Access Point.

Ad-Hoc Network

The only requirement for an ad-hoc network is the ability to communicate with one or more other wireless users. To do this:

- All PC Cards must use the same channel. You cannot change the default channel of the RoamAbout PC Card. The default channel is listed in Table A-3 on page A-5.
- Determine the size of the coverage area. The speed of the RoamAbout PC Card is one factor that determines the client coverage area. Other factors include physical obstructions and noise levels. The following is an example of the coverage area in a semi-open environment, which is defined as work space divided by shoulder-height, hollow wall elements. The distances in your environment may be different.
  - 11 Mbit/s - 165 feet (50 meters)
  - 5.5 Mbit/s - 230 feet (70 meters)
  - 2 Mbit/s - 300 feet (90 meters)
  - 1 Mbit/s - 375 feet (115 meters)

  The faster the transmit speed, the shorter the coverage area at that speed. A client with an 11 Mbit/s PC Card can communicate with other clients up to a distance of 375 feet in a semi-open environment. However, only clients within the first 165 feet can communicate at 11 Mbit/s. Clients between 165 and 230 feet communicate at 5.5 Mbit/s. Clients between 230 and 300 feet communicate at 2 Mbit/s; and clients between 300 to 375 feet communicate at 1 Mbit/s.

  If using a card other than the RoamAbout PC Card in wireless clients, refer to that card's documentation for information about allowable distances.
- Make sure that the computer meets the RoamAbout PC Card requirements as described in the "System Requirements for Wireless Clients" section on page 3-8.

System Requirements for Wireless Clients

The RoamAbout PC Card has drivers for the following operating systems:

- Windows NT V3.51 and later, Windows 95, and Windows 98 (same driver)
- MS-DOS and Windows 3.1 (refer to the *RoamAbout 802.11 PC Card MS-DOS and Windows 3.1 Installation Guide*)
- Apple Macintosh

The Windows 2000 operating system contains the RoamAbout driver; however, this version of the driver does not support encryption. For the latest version of the RoamAbout drivers, see the RoamAbout web site at:

www.cabletron.com/wireless

You can have clients with various operating systems in the same wireless network.

You may need to install the appropriate networking protocols when installing the RoamAbout PC Card in the computer. The most common protocols include TCP/IP and NetBEUI.

If the computer does not have a PC Card slot but has an available ISA bus slot, you need to install the optional ISA adapter kit.

Wireless Network Hardware Installation Overview

Once you have designed the wireless network and determined where to place the wireless devices, install and configure the hardware as described in the following sections.

Wireless Infrastructure Network

The following is an overview of the steps to install the wireless devices in a wireless infrastructure network.

1. Install the RoamAbout Access Point in the location you have chosen. Refer to the RoamAbout Access Point documentation to install the Access Point hardware.
2. Install a tool to configure the Access Point as described in Chapter 4.
3. Configure the Access Points using the procedures in Chapter 5. You should configure the Access Points before configuring clients. A number of client settings depend on the Access Point settings.
4. Create wireless clients by installing the RoamAbout PC Card into the appropriate computers. Refer to the RoamAbout PC Card documentation.
5. If installing the RoamAbout Client Utility (recommended), follow the installation procedure in the "RoamAbout Client Utility" section on page 4-6.
6. Configure the wireless clients using the procedures in Chapter 5.

LAN-to-LAN Configuration

The following is an overview of the steps to install the Access Points in a LAN-to-LAN configuration.

1. If using an outdoor antenna, follow the instructions in the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide.*
2. Install the RoamAbout Access Points in the locations you have chosen. Refer to the RoamAbout Access Point documentation to install the Access Point hardware.
3. Choose and install a tool to configure the Access Point as described in Chapter 4.
4. Configure the Access Points using the procedure in the "Configuring Access Points in a Point-to-Point Network" section on page 5-9 or "Configuring the Access Point for Point-to-Multipoint" section on page 5-13.

Ad-Hoc Network

The following is an overview of the steps to install the wireless clients in an ad-hoc network.

1. Create wireless clients by installing the RoamAbout PC Card into the appropriate computers. Refer to the RoamAbout PC Card documentation.
2. If installing the RoamAbout Client Utility (recommended), follow the installation procedure in the "RoamAbout Client Utility" section on page 4-6.
3. Configure the wireless clients, as described in the "Configuring Clients for an Ad-Hoc Network" section on page 5-18.

Chapter 4

Installing the Wireless Network Tools

You can configure the Access Point using one or more of these tools:

- RoamAbout Access Point Manager
- RoamAbout Access Point console port
- Network Management Station (NMS)

To configure the Access Point for the first time, you need to use the RoamAbout Access Point Manager or the console port.

RoamAbout Access Point Manager

The RoamAbout Access Point (AP) Manager is a configuration tool for new Access Points and a management tool to assist the ongoing management and support of RoamAbout wireless networks. The AP Manager can manage multiple Access Points simultaneously.

The AP Manager has the following features:

- Ability to manage multiple Access Points remotely, including changing parameters on multiple Access Points in a wireless network with a single command.
- Ability to group Access Points. For example, you can group together all the Access Points in one wireless network and have a second group for Access Points in another wireless network.
- Ability to view Access Point parameters such as statistics, firmware version number, MAC addresses, amount of memory, and card type.
- Integrity checking for many wireless parameter changes. This warns the you if a common wireless network management mistake is about to be made, or if the operation requested is unusual and usually not recommended.
- Integrity checking of an existing wireless network configuration for consistent settings and common management errors.
- Improved wireless network performance through packet filtering and recommended filter settings.
- Integrated with a BootP/TFTP application for simple Access Point firmware upgrades, also called flash upgrades.
- Support for 802.11 radio technology as well as the earlier versions of the RoamAbout Direct Sequence (DS) and Frequency Hopping (FH) products.

Installing the AP Manager

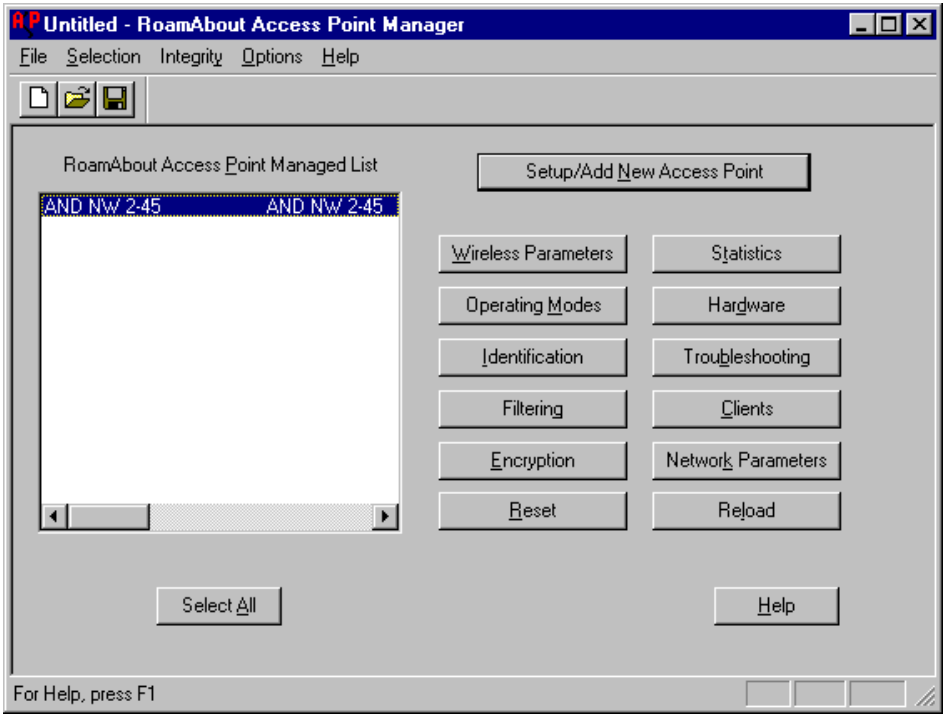
The AP Manager supports the Windows 95, Windows 98, and Windows NT (V4.0 or later).

The AP Manager can manage Access Points from a wireless computer. However, the AP Manager needs to be on a computer connected to the same wired LAN as the Access Point to assign an IP address or upgrade the Access Point firmware.

The AP Manager is included on diskettes in the RoamAbout Access Point kit. To install the AP Manager, insert the diskette into the diskette drive and start the setup program (typically located at **a:\setup**). Follow the on-line instructions.

After the installation, you can open the AP Manager main window (Figure 4-1) by clicking the **Start** button on the Windows desktop and selecting **Programs→RoamAbout→RoamAbout Access Point Manager**.

Figure 4-1: RoamAbout Access Point Manager Main Window



Using the AP Manager

You can manage Access Points individually or as a single group. You can group Access Points based on any criteria, such as:

- All Access Points belonging to the same network are in one group. For example, have one group for the Accounting network and one group for the Engineering network.
- To avoid confusion, you should have different groups for Access Points in an infrastructure network and Access Points in a LAN-to-LAN configuration. Access Points in these configurations are managed differently.
- If you have earlier releases of the RoamAbout Access Point, you can group non-802.11 compliant Access Points together, separate from the 802.11 Access Points.

The AP Manager saves each group in a configuration file (*.CFG). When you open a configuration file, the Access Points in the group are displayed in the Managed List field on the main window (see Figure 4-1). You can add or remove Access Points from the configuration file. Click the **Help** button for a description of the AP Manager main window. Chapter 5 contains the procedures to configure Access Points using the AP Manager.

Each time you open the AP Manager, the **RoamAbout Access Point Managed List** field is blank. You need to open a file by clicking **File** in the menu bar, selecting **Open**, and choosing a configuration file. All the Access Points in that group are displayed in the Managed List field.

To display the settings that the Access Point is currently using, select the Access Point in the Managed List field and click the various buttons, such as **Wireless Parameters**, **Operating Modes**, **IP Network Parameters**, and **Hardware**. Click the Help button in each dialog box for a description of the dialog box.

To check the Signal-to-Noise Ratio (SNR) between the Access Point and another device in the same wireless network, select **Integrity** in the menu bar and select **Link Test**.

Other SNMP Management Tools

The Access Point supports the Simple Network Management Protocol (SNMP) through any standard Network Management Station that supports SNMP. The SNMP management capability enables you to manage standard SNMP MIB characteristics, such as protocol filtering and address filtering.

To manage the Access Point with a Network Management Station (NMS) you must first use the console port or AP Manager to configure the Access Point with a valid IP address.

The following Access Point settings are only accessible from an NMS:

- RMON parameters
- Multicast rate limiting value (AP Manager and console port only enable or disable the 100 Kb/sec value)
- Aging timer

RoamAbout Access Point Console Port

You can manage the Access Point by connecting a terminal or personal computer running terminal emulation software to the console port. Signals from the console port conform to the EIA-232D signaling standard at 9600 baud only. The port appears as a data terminal equipment (DTE) device. You do not need to use the console port if you use the AP Manager to manage the Access Point.

Refer to the RoamAbout Access Point installation document for the procedure to connect a device to the Access Point console port.

RoamAbout Client Utility

The RoamAbout Client Utility is a diagnostic tool for RoamAbout wireless networks. The RoamAbout Client Utility is provided with the RoamAbout client software kit which also contains the RoamAbout driver.

You use the client utility to:

- Check the quality of wireless communications between the RoamAbout client and the associated Access Point (or another client in an ad-hoc network).
- Check the communications quality between the client and all other Access Points (within radio range) in the wireless infrastructure network. This test allows you to optimize placement of the RoamAbout client and Access Points.
- Display information about the configuration settings of the RoamAbout client and the Access Point.
- Perform a diagnostic test on the RoamAbout PC Card.
- Check the version numbers of the RoamAbout components installed in the client.
- Store test results in log files.

You cannot use the client utility to change any of the RoamAbout parameters on the client.

Installing the Client Utility

The RoamAbout Client Utility is only available for the Windows 95, Windows 98, and Windows NT (version 4.0 or higher) operating systems. The client utility is on the same diskette as the RoamAbout driver, in the Utils folder. The client utility shipped with the RoamAbout driver might not fully work for previous generation RoamAbout drivers. You should always use the client utility that was shipped with the RoamAbout driver. After installing the RoamAbout driver, install the RoamAbout Client Utility as follows:

1. Insert the RoamAbout diskette for Windows 95 and NT into the diskette drive.
2. From the Windows Taskbar, click **Start** then select **Run**.
3. Type the path to the installation program. For example:

   a:\utils\setup.exe
4. Click **OK**.
5. Follow the on-line instructions.

Using the RoamAbout Client Utility

To start the RoamAbout Client Utility, click **Start**, then select **Programs→RoamAbout→RoamAbout Client Utility**.

The RoamAbout Client Utility window (Figure 4-2) displays the following information:

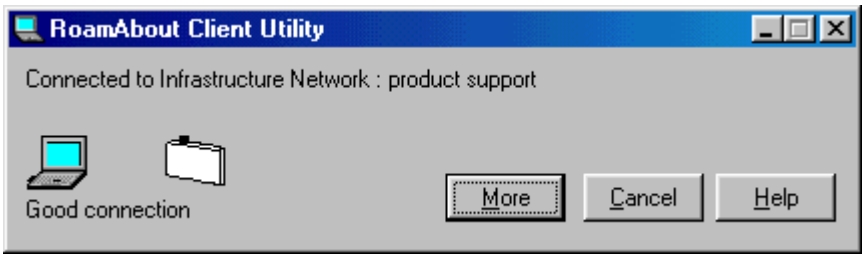
- If connected to an infrastructure network, the name of the network.
- The quality of the communications with the selected network as indicated by a Green (Good), Yellow (Adequate) or Red (Poor) indicator.
- Error message if the PC Card is not functioning properly.

Should you minimize this window, there is an icon (in the shape of a dish antenna) in the Taskbar that also indicates whether the connection is Good (Green), Adequate (Yellow), or Poor (Red).

Click the **More** button in the RoamAbout Client Utility window to display the Status/Functions window. This window displays the general performance of your wireless connection and provides access to the other features of the client utility.

For detailed information about each client utility window, consult the RoamAbout Client Utility on-line help by clicking the **Help** button in each window or pressing the <F1> key.

Figure 4-2: RoamAbout Client Utility Window



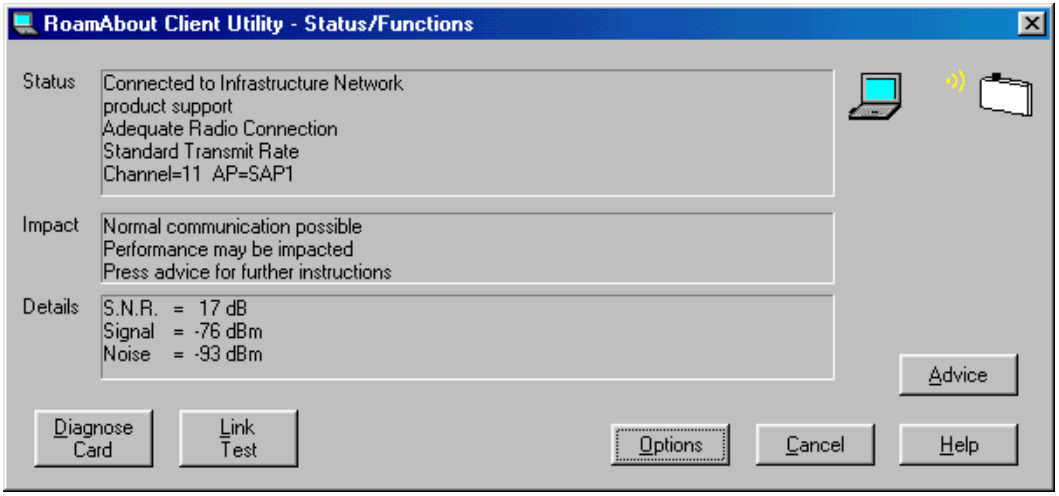
NOTE

If the wireless network uses encryption and the client does not, the initial client utility window could show a valid network connection. However, the client might not be able to exchange data with the network.

Status/Functions

The RoamAbout Client Utility Status/Functions window (Figure 4-3) displays information about the network connection and communications quality. If the client is unable to connect to a network, the **Status** and **Impact** fields provide information that can help you determine the cause.

Figure 4-3: RoamAbout Client Utility Status/Functions Window



Optionally, you can:

- Click the **Advice** button for additional status information and to troubleshoot unexpected results.
- Click the **Diagnose Card** button to test the PC Card and to check the versions of hardware, firmware, and software. Use this button when the Status/Functions window indicates that the PC Card is not functioning properly.
- Click the **Link Test** button to test a specific wireless link.
- Click the **Options** button to access the enhanced mode setting, which allows you to display or hide advanced diagnostic tools. This button also allows you display the Status/Functions window immediately when you start the client utility.
- Click the **Site Monitor** button to perform a site survey or optimize placement of the Access Points. This button is displayed only when you use the **Options** button to enable enhanced mode.

Diagnose Card

The card diagnostics enables you to:

- Test the RoamAbout PC Card.
- Display a set of communication statistics.
- Display the configuration settings of the PC Card. The configuration settings can only be displayed when the client utility is in enhanced mode, which you can enable by clicking the **Options** button in the Status/Functions window.

Run the card test only in situations where the Status/Functions window reports a card failure or when you suspect a configuration mismatch. When contacting RoamAbout technical support, the card test results may help the support representative determine the cause of a malfunctioning device.

Running the card test may temporarily disrupt the client from communicating with the network. In exceptional cases, you may lose the network connection.

Link Test

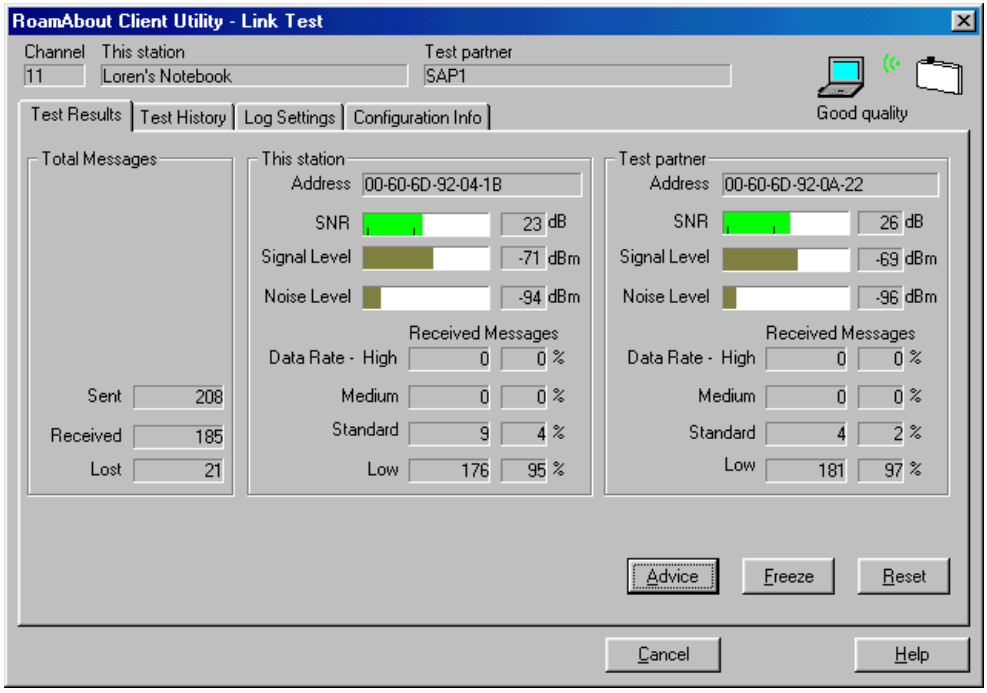
Use the RoamAbout Client Utility Link Test window (Figure 4-4) to investigate the specific link between the RoamAbout client and its test partner. If connected to a infrastructure network, the test partner is the associated Access Point. If configured for an ad-hoc network, you can select another client in the network to be the test partner.

To monitor the communications quality of the client connection to the network, Link Test actively exchanges test messages with the test partner.

When you run the Link Test while roaming through a network environment with multiple Access Points, the link test partner (Access Point) changes as you move from cell to cell. The link test mode enables you to investigate:

- The communications quality of the radio connection, which is the primary indicator of wireless performance.
- The data throughput efficiency of the radio connection, which is the secondary indicator of wireless performance.

Figure 4-4: RoamAbout Client Utility Link Test



Link Test also allows you to save measurement data to a log file. The logging function is only available when the client utility is in enhanced mode, which you can enable by clicking the **Options** button in the Status/Functions window.

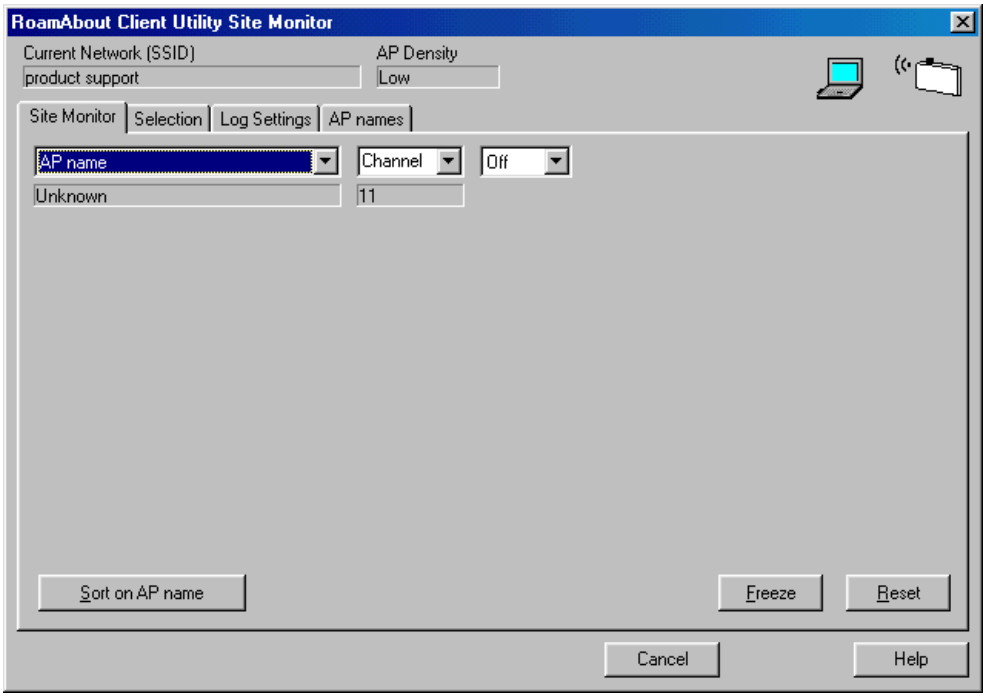
Site Monitor

You can use the RoamAbout Client Utility Site Monitor window (Figure 4-5) to monitor the radio communications quality with multiple RoamAbout Access Points simultaneously. The Site Monitor function is only available when the client utility is in enhanced mode, which you can enable by clicking the **Options** button in the Status/Functions window.

The Site Monitor window only displays the Access Points within range of the client. If the Site Monitor window does not display all the Access Points that you expect, the unlisted Access Point might be out of range of your client or using another wireless network name.

The Site Monitor window offers a set of pull-down menus that enable you to display and organize diagnostic information according to your preferences. The Site Monitor function also allows you to save measurement data to a log file.

Figure 4-5: RoamAbout Client Utility Site Monitor Window



Chapter 5

Configuring the Wireless Network

This chapter provides the procedures to configure the wireless device parameters. Before performing these procedures, you need to install the wireless network tools as described in Chapter 4.

If you are configuring a wireless infrastructure network, configure the Access Points first. Many of the wireless client parameters are based on the Access Point settings.

For infrastructure and ad-hoc networks, document the common settings for any clients that join the network at a future date.

Configuring Access Points in an Infrastructure Network

After installing the Access Point, you can configure it using the AP Manager or the console port as described in the following sections. When configuring a new Access Point, have the following information available:

- The Access Point wired MAC address, which is printed on the front of the Access Point. The MAC address for the RoamAbout Access Point 2000 is underneath the plastic cover.
- A valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway. The Access Point does not automatically obtain an IP address from a DHCP server.

You also need the Access Point SNMP read/write community name. By default, the community name is **public**. If you do not enter the correct community name, you cannot modify the Access Point or add it to the AP Manager group.

If adding Access Points to an existing wireless network, write down the network parameter settings before you begin configuring the Access Points. Parameters include the wireless network name, AP Density, and Secure Access.

Using the AP Manager

If you are currently managing Access Points with the AP Manager, you need to determine if the new Access Point belongs to an existing group. For a newly installed and unconfigured Access Point, do the following:

1. Start the AP Manager by clicking the **Start** button on the Windows desktop and selecting **Programs→RoamAbout→RoamAbout Access Point Manager**.
2. To add the Access Point to an existing group of Access Points, select **File→Open** from the menu bar and open the group. Otherwise, select **File→New** to start a new group.
3. In the AP Manager main window, click the **Setup/Add New Access Point** button. You are asked if you want to load an IP address.

   If the Access Point has an IP address, you must know the address to manage the Access Point from the AP Manager. The AP Manager cannot overwrite an existing IP address.
4. If the Access Point has an IP address, click **No**. Then enter the existing IP address and the Access Point SNMP read/write community name, which is by default **public**.

5. If the Access Point does not have an IP address, click **Yes** and enter the following:

   — Access Point's wired MAC address.
   — New, valid IP network address.
   — Access Point's SNMP read/write community name, which is by default **public**.
   — Optionally, a subnet mask and default gateway.

   Press the **Help** button for details about each field. Click **OK** when completed. You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager automatically displays the Identification and Wireless Parameter dialog boxes.

6. In the Identification dialog box, set the following parameters. Press the **Help** button in the dialog box for details about each field. Click **OK** when done.

   — **System Name**. Enter a unique name for each Access Point. This is not the same as the station name for the Access Point.
   — **Location**. Enter unique descriptive text for each Access Point that specifies the physical location of the Access Point.
   — **Contact**. Enter the name of the individual responsible for the Access Point.

7. In the Wireless Parameters dialog box, enter a wireless network name for the network. This name must be entered in all Access Points in the same infrastructure network. To prevent unauthorized access, you should replace the default wireless network name.

   The wireless network name can be any alphanumeric string (uppercase and lowercase) with a maximum of 32 characters. Spaces are allowed. The name is case sensitive. An example of a wireless network name is:

   My RoamAbout NETWORK 2

8. Enter a channel. If there are Access Points whose coverage areas overlap, set adjacent Access Points to different channels that are at least five channels apart if possible.

   The client automatically uses the same channel as the Access Point when it joins the wireless network.

9. Enter a station name. The station name is displayed when clients run the RoamAbout Client Utility. Select a name that helps identify the location of the Access Point. Each Access Point should have a unique station name.

10. Go to Step 19 to accept the default settings of the other wireless parameters. The default settings are usually appropriate for an infrastructure network. If you need to customize the Access Point configuration, continue with this procedure.

11. Click the **Advanced** button in the Wireless Parameters window.

12. Set **Bridge Mode** to **Workgroup**. This configures the Access Point to communicate with wireless clients.

13. Enable **Secure Access** if you want to prevent clients without the correct wireless network name from connecting to this Access Point. See the "Configuring Security" section on page 5-26 for more information.

14. Set the AP Density setting based on the following:

    — **Low** (default). The Low setting provides maximum coverage using a minimum number of Access Points. This option is typically used for single-cell networks, but also provides an efficient and cost effective solution for networks that include multiple wireless clients.

    — **Medium**. The Medium setting can be used for environments where Access Point stations experience slow response times even when the radio communication is excellent.

    — **High**. The High setting should only be used when you are designing a wireless infrastructure that includes a high concentration of Access Point devices.

15. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.

16. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.

17. In nearly all environments, you should not change the default DTIM of 1. For more information, see the "Configuring Power Management" section on page 5-25.

18. To use data encryption, use the procedure in the "Setting Encryption" section on page 5-27.

19. To implement your changes, select **Reset** from the main window, then select **Reset with Current Settings**. Allow approximately one minute for the Access Point to reset and complete its self-test.

20. Repeat this procedure to add additional Access Points. If separating the Access Points by groups, only add the Access Points that you want to group together.

    If you are creating a new group, click **File→Save As** from the menu bar. Choose a meaningful name and save the file. The file is saved with the .CFG file extension. To create another group, click **File→New** and repeat this procedure.

21. To configure the RoamAbout clients, write down the following Access Point settings:

    — Wireless network name, especially if Secure Access is enabled.

    — AP Density setting.

    — Data encryption keys, if used.

Using the Console Port

After installing the Access Point and setting up a console port device, you can configure the Access Point as follows:

1. Repeatedly press the <Return> key at the terminal that is connected to the console port until the RoamAbout Access Point Installation Menu appears. If using a computer, start the terminal emulation program and connect to the console port.

2. To allow the AP Manager or other management tools using SNMP to remotely manage the Access Point, perform the following:

   a) Choose **Set IP Address** from the Installation Menu.

   b) Enter the IP address, subnet mask, and default gateway.

3. Choose **Module-Specific Options** from the Installation Menu, then choose **Set Wireless Configuration**.

4. Choose a wireless network name for the network. This name must be entered in all Access Points in the same infrastructure network. To prevent unauthorized access, you should replace the default wireless network name.

   The wireless network name can be any alphanumeric string (uppercase and lowercase) with a maximum of 32 characters. Spaces are allowed. The name is case sensitive. An example of a wireless network name is:

   My RoamAbout NETWORK 2

5. Enter a channel. If there are other Access Points whose coverage areas overlap, set adjacent Access Points to different channels that are at least five channels apart if possible.

   The client automatically uses the same channel as the Access Point when it joins the wireless network.

6. Enter a station name. This name is displayed when clients run the RoamAbout Client Utility. Select a name that helps identify the location of the Access Point. Each Access Point should have a unique station name.

7. Go to Step 17 to accept the default settings of the other parameters. The default settings are usually appropriate for an infrastructure network. If you need to customize the Access Point configuration, continue with this procedure.

8. Enable Secure Access if you want to prevent clients without the correct wireless network name from connecting to this Access Point. See the “Configuring Security” section on page 5-26 for more information.

9. Set the AP Density setting based on the following:
   - **Low** (default). The Low setting provides maximum coverage using a minimum number of Access Points. This option is typically used for single-cell networks, but also provides an efficient and cost effective solution for networks that include multiple wireless clients.
   - **Medium**. The Medium setting can be used for environments where Access Point stations experience slow response times even when the radio communication is excellent.
   - **High**. The High setting should only be used when you are designing a wireless infrastructure that includes a high concentration of Access Point devices.
10. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.
11. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.
12. In nearly all environments, you should not change the default DTIM of 1. For more information, see the "Configuring Power Management" section on page 5-25.
13. Select **Bridge Mode Options** in the Module-Specific Options menu. Select **Set Bridge Mode** then **Workgroup**.
14. To use encryption, use the procedure in the "Setting Encryption" section on page 5-27.

    The Data Encryption menu also allows you to enable **Set Exclude SNMP**, which prevents any management tool using SNMP, including the AP Manager, from changing the encryption parameters.
15. To disable the 100 Kb/sec limitation on multicast traffic, select **Enable/Disable Default Rate Limiting** in the Module-Specific Options menu. By default, this feature is enabled to prevent too much multicast traffic from affecting network performance.
16. To prevent other users from using the console port to view or modify settings, enable **Enable/Disable Console Password** from the Installation Menu. Then choose **Set SNMP Read/Write Community** from the Installation Menu and enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.
17. To implement your changes, reset the Access Point by selecting **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the Access Point to reset and complete its self-test.
18. To configure the RoamAbout clients, write down the following Access Point settings:
    - Wireless network name, especially if Secure Access is enabled.
    - AP Density setting.
    - Data encryption keys, if used.

Configuring Clients in an Infrastructure Network

Have the Access Point settings available as you configure the RoamAbout clients.

1. At a Windows system, perform the following:
   a) From the Windows desktop, click **Start** then select **Settings→Control Panel**. Then double click the **Network** icon.
   b) For Windows 95 or 98, the Network dialog box is displayed. Click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.
   c) For Windows NT, click the **Adapters** tab. In the **Network Adapters** field, click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.
   d) Select the **Basic** tab.
2. At an Apple PowerBook system, open the **Apple** menu, select **Control Panels** then select **RoamAbout Setup**.
3. Enter the wireless network name that was entered in the Access Point. The name is case sensitive.

   If the Secure Access setting on the Access Point is disabled, you can leave the wireless network name field blank or enter **ANY** (all uppercase).
4. Optionally, enter a station name, which can be any name you choose for your computer (maximum of 32 characters). The station name is displayed at the Access Point and on other clients when they run the RoamAbout Client Utility. You should select a name that helps to identify the client.

   For Windows NT clients, the computer name is automatically used as the station name.
5. If the advanced settings on the Access Point are set to the default values, you can use the default values for the client. You do not need to perform the rest of this procedure. Instead, close the Properties window and restart the computer when prompted.
6. If you changed the default values on the Access Point, select the **Advanced** tab.
7. Only enter a MAC Address if your network uses a local MAC addressing scheme. Most networks do not. See the "Using a Local MAC Addressing Scheme" section on page 5-33 for more information.
8. Set the **AP Density** setting to match the Access Point AP Density setting. Using non-matching values may seriously affect the wireless performance of the client.
9. To modify the Transmit Rate and Fixed settings, see the "Configuring the Transmit Rate" section on page 5-23. The default settings work well in most environments.

10. Leave Medium Reservation disabled (no check mark) unless you have a hidden station problem as described in the "Configuring the RTS/CTS Protocol" section on page 5-24.

11. To change the default power management parameters, click the **Power Management** tab. For information on modifying the power management settings, see the "Configuring Power Management" section on page 5-25.

12. If the Access Point is using encryption, click the **Encryption** tab. By default, encryption is disabled. To enable encryption:

    a) Place a check mark in the **Enable Encryption** check box.

    b) Find out the keys used by the Access Points in the wireless network. In addition, you need to know the position (1, 2, 3, or 4) for each key. The RoamAbout devices can support up to four keys.

    c) Enter the keys in the **Encryption Key** fields. Make sure that the key you enter in position 1 is the same as the key in position 1 in the Access Point. Also, any keys entered in positions 2, 3, and 4 must match the keys in those same positions in the Access Point. However, you do not need to enter all the keys used by the Access Point.

       If you leave then return to the Encryption window, the characters in each Key field are replaced by asterisks (*) that fill the field.

    d) In the **Encrypt Data Transmissions using** field, select which key you want the client to use when transmitting data.

    Refer to the "Setting Encryption" section on page 5-27 for additional information.

13. Click **OK** to close the Properties window, and restart the computer when prompted.

Configuring Access Points in a Point-to-Point Network

You can configure two Access Points to communicate with each other in a LAN-to-LAN, Point-to-Point configuration using the AP Manager or the console port as described in the following sections. When configuring a new Access Point, have the following information available:

- The Access Point wired MAC address, which is printed on the front of the Access Point. The MAC address for the RoamAbout Access Point 2000 is underneath the plastic cover.
- A valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway. The Access Point does not automatically obtain an IP address from a DHCP server.

You need the Access Point SNMP read/write community name. By default, the community name is **public**. If you do not enter the correct community name, you cannot modify the Access Point or add it to the AP Manager group.

You also need the wireless MAC address of both Access Points. The wireless MAC address is NOT the same as the wired MAC address printed on the Access Point label. Perform one of the following to see the wireless MAC address:

- If both Access Points are currently managed by the AP Manager, select each Access Point from the **Managed List** field and click the **Hardware** button.
- Using the Access Point console port at each Access Point, choose **Show Current Settings** from the RoamAbout Access Point Installation Menu.
- Check the back of the PC Card used in the Access Points. The MAC address of the PC Card is the Access Point's wireless MAC address.

The following Access Point parameters are not used in this configuration:

- Wireless Network Name
- Secure Access
- AP Density
- Power Management (DTIM Period)

Using the AP Manager

Start at Step 1 if the Access Point is not managed by the AP Manager. If the Access Point is currently managed by the AP Manager, select the Access Point in the **Managed List** field, click the **Wireless Parameters** button, and go to Step 9.

1. Start the AP Manager by clicking the **Start** button on the Windows desktop and selecting **Programs→RoamAbout→RoamAbout Access Point Manager**.
2. To add the Access Point to an existing group of Access Points, select **File→Open** from the menu bar and open the group. Otherwise, select **File→New** to start a new group.
3. In the AP Manager main window, click the **Setup/Add New Access Point** button. You are asked if you want to load an IP address.

   If the Access Point has an IP address, you must know the address to manage the Access Point from the AP Manager. The AP Manager cannot overwrite an existing IP address.
4. If the Access Point has an IP address, click **No**. Then enter the existing IP address and the Access Point SNMP read/write community name, which is by default **public**.
5. If the Access Point does not have an IP address, click **Yes** and enter the following:

   — Access Point's wired MAC address.
   — New, valid IP network address.
   — Access Point's SNMP read/write community name, which is by default **public**.
   — Optionally, a subnet mask and default gateway.

   Press the **Help** button for details about each field. Click **OK** when completed. You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager automatically displays the Identification and Wireless Parameter dialog boxes.
6. In the Identification dialog box, set the following parameters. Press the **Help** button in the dialog box for details about each field. Click **OK** when done.

   — **System Name**. Enter a unique name for each Access Point. This is not the same as the station name for the Access Point.
   — **Location**. Enter unique descriptive text for each Access Point that specifies the physical location of the Access Point.
   — **Contact**. Enter the name of the individual responsible for the Access Point.
7. In the Wireless Parameters dialog box, enter a station name that helps identify the location of the Access Point. Each Access Point should have a unique station name.
8. Enter a channel. Both Access Points must use the same channel.
9. Click the **Advanced** button in the Wireless Parameters window.

10. Set the **Bridge Mode** to **LAN-to-LAN Endpoint**. This configures the Access Point to communicate with only one Access Point.

11. In the Wireless Parameters dialog box, enter the wireless MAC address of the remote Access Point.

12. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.

13. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.

14. To use data encryption, use the procedure in the "Setting Encryption" section on page 5-27.

15. To implement your changes, select **Reset** from the main window, then select **Reset with Current Settings**. Allow approximately one minute for the Access Point to reset and complete its self-test.

16. Repeat this procedure at the other Access Point.

Using the Console Port

To configure Access Points for a Point-to-Point configuration, do the following:

1. Repeatedly press the <Return> key at the terminal that is connected to the console port until the RoamAbout Access Point Installation Menu appears. If using a computer, start the terminal emulation program and connect to the console port.
2. To allow the AP Manager or other management tools using SNMP to remotely manage the Access Point, perform the following:
   a) Choose **Set IP Address** from the Installation Menu.
   b) Enter the IP address, subnet mask, and default gateway.
3. Choose **Module-Specific Options** from the Installation Menu, then choose **Set Wireless Configuration**.
4. Enter a channel. Both Access Points must use the same channel.
5. Enter a station name that helps identify the location of the Access Point. Each Access Point should have a unique station name.
6. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.
7. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.
8. Select **Bridge Mode Options** in the Module-Specific Options menu. Select **Set Bridge Mode** then **LAN-to-LAN Endpoint**. Select the first prompt for the remote wireless MAC address and enter the wireless MAC address of the remote Access Point.
9. To use encryption, use the procedure in the "Setting Encryption" section on page 5-27.
10. To prevent other users from using the console port to view or modify settings, enable **Enable/Disable Console Password** from the Installation Menu. Then choose **Set SNMP Read/Write Community** from the Installation Menu and enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.
11. To implement your changes, reset the Access Point by selecting **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the Access Point to reset and complete its self-test.
12. Perform this procedure on the other Access Point.

Configuring the Access Point for Point-to-Multipoint

You can configure up to seven Access Points in a LAN-to-LAN, Point-to-Multipoint configuration using the AP Manager or the console port as described in the following sections. When configuring a new Access Point, have the following information available:

- The Access Point wired MAC address, which is printed on the front of the Access Point. The MAC address for the RoamAbout Access Point 2000 is underneath the plastic cover.
- A valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway. The Access Point does not automatically obtain an IP address from a DHCP server.

You need the Access Point SNMP read/write community name. By default, the community name is **public**. If you do not enter the correct community name, you cannot modify the Access Point or add it to the AP Manager group.

You also need the wireless MAC address of both Access Points. The wireless MAC address is NOT the same as the wired MAC address printed on the Access Point label. Perform one of the following to see the wireless MAC address:

- If the Access Points are currently managed by the AP Manager, select the each Access Point from the **Managed List** field and click the **Hardware** button.
- Using the Access Point console port at each Access Point, choose **Show Current Settings** from the RoamAbout Access Point Installation Menu.
- Check the back of the PC Card used in the Access Points. The MAC address of the PC Card is the Access Point's wireless MAC address.

The following Access Point parameters are not used in this configuration:

- Wireless Network Name
- Secure Access
- AP Density
- Power Management (DTIM Period)

Using the AP Manager

Start at Step 1 if the Access Point is not managed by the AP Manager. If the Access Point is currently managed by the AP Manager, select the Access Point in the **Managed List** field, click the **Wireless Parameters** button, and go to Step 10.

1. Determine which Access Point is the Central Access Point, as described in the "Point-to-Multipoint" section on page 1-9.
2. Start the AP Manager by clicking the **Start** button on the Windows desktop and selecting **Programs→RoamAbout→RoamAbout Access Point Manager**.
3. To add the Access Point to an existing group of Access Points, select **File→Open** from the menu bar and open the group. Otherwise, select **File→New** to start a new group.
4. In the AP Manager main window, click the **Setup/Add New Access Point** button. You are asked if you want to load an IP address.

   If the Access Point has an IP address, you must know the address to manage the Access Point from the AP Manager. The AP Manager cannot overwrite an existing IP address.
5. If the Access Point has an IP address, click **No**. Then enter the existing IP address and the Access Point SNMP read/write community name, which is by default **public**.
6. If the Access Point does not have an IP address, click **Yes** and enter the following:

   — Access Point's wired MAC address.
   — New, valid IP network address.
   — Access Point's SNMP read/write community name, which is by default **public**.
   — Optionally, a subnet mask and default gateway.

   Press the **Help** button for details about each field. Click **OK** when completed. You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager automatically displays the Identification and Wireless Parameter dialog boxes.
7. In the Identification dialog box, set the following parameters. Press the **Help** button in the dialog box for details about each field. Click **OK** when done.

   — **System Name**. Enter a unique name for each Access Point. This is not the same as the station name for the Access Point.
   — **Location**. Enter unique descriptive text for each Access Point that specifies the physical location of the Access Point.
   — **Contact**. Enter the name of the individual responsible for the Access Point.
8. In the Wireless Parameters dialog box, enter a station name that helps identify the location of the Access Point. Each Access Point should have a unique station name.
9. Enter a channel. All Access Points must use the same channel.

10. Click the **Advanced** button in the Wireless Parameters window.

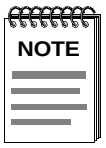
11. For the Central Access Point, perform the following:

    a) Set **Bridge Mode** to **LAN-to-LAN Multipoint**. The Multipoint Activation Key dialog box opens. This option is only available on Access Point 2000 with V6.0 or later firmware. You must enter a valid activation key to enable Multipoint bridge mode.

    b) In the Wireless Parameters dialog box, click the **Multipoint Properties** button.

    c) Enter the wireless MAC addresses of up to six Access Points in the fields provided. Any unused fields must be null (contain no characters).

    d) Enable or disable **Wireless Relay**. If enabled, the Endpoint Access Points can only communicate with each other through the Central Access Point. If disabled, each of the Endpoint Access Points in the configuration can only communicate with the Central Access Point and its wired LAN, and not with each other.



If an Access Point in the Point-to-Multipoint configuration is connected to a wired port, you must disconnect the wired port to manage it. Otherwise that Access Point can only be used as a relay and cannot be managed.

12. For the other Access Points, set **Bridge Mode** to **LAN-to-LAN Endpoint**. In the Wireless Parameters dialog box, enter the wireless MAC address of the Central Access Point. This configures the Access Point to only communicate with the Central Access Point.

13. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.

14. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.

15. To use data encryption, use the procedure in the "Setting Encryption" section on page 5-27.

16. To implement your changes, select **Reset** from the main window, then select **Reset with Current Settings**. Allow approximately one minute for the Access Point to reset and complete its self-test.

17. Repeat this procedure at the other Access Points.

Using the Console Port

To configure Access Points for a Point-to-Multipoint configuration, do the following:

1. Determine which Access Point is the Central Access Point, as described in the "Point-to-Multipoint" section on page 1-9.
2. Repeatedly press the <**Return**> key at the terminal that is connected to the console port until the RoamAbout Access Point Installation Menu appears. If using a computer, start the terminal emulation program and connect to the console port.
3. To allow the AP Manager or other management tools using SNMP to remotely manage the Access Point, perform the following:
   a) Choose **Set IP Address** from the Installation Menu.
   b) Enter the IP address, subnet mask, and default gateway.
4. Choose **Module-Specific Options** from the Installation Menu, then choose **Set Wireless Configuration**.
5. Enter a channel. All Access Points must use the same channel.
6. Enter a station name. Select a name that helps identify the location of the Access Point. Each Access Point should have a unique station name.
7. The default transmit rate setting works well in most environments. To modify this setting, see the "Configuring the Transmit Rate" section on page 5-23.
8. The default RTS Threshold setting works well in most environments. To modify this setting, see the "Configuring the RTS/CTS Protocol" section on page 5-24.
9. For the Central Access Point, perform the following:
   a) Select **Bridge Mode Options** in the Module-Specific Options menu. Select **Set Bridge Mode** then **LAN-to-LAN Multipoint**. You must enter a valid activation key to enable Multipoint bridge mode.
   b) Select each prompt for the remote wireless MAC address and enter the wireless MAC address of up to six Access Points. Any unused fields must be null (00-00-00-00-00-00).
10. For the endpoint Access Points, select **Bridge Mode Options** in the Module-Specific Options menu. Select **Set Bridge Mode** then **LAN-to-LAN Endpoint**. Select the first prompt for the remote wireless MAC address and enter the wireless MAC address of the Central Access Point.
11. To use encryption, use the procedure in the "Setting Encryption" section on page 5-27.

12. To prevent other users from using the console port to view or modify settings, enable **Enable/Disable Console Password** from the Installation Menu. Then choose **Set SNMP Read/Write Community** from the Installation Menu and enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.

13. To implement your changes, reset the Access Point by selecting **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the Access Point to reset and complete its self-test.

14. Perform this procedure on the other Access Points.

Configuring Clients for an Ad-Hoc Network

To configure clients for an ad-hoc network, perform the following:

1. From the Windows desktop, click **Start** then select **Settings→Control Panel**. Then double click the **Network** icon.
2. For Windows 95 or 98, the Network dialog box is displayed. Click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.
3. For Windows NT, click the **Adapters** tab. In the Network Adapters field, click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.
4. Select the **Basic** tab.
5. Select **Ad-Hoc Demo Mode**.
6. To modify the Transmit Rate and Fixed settings, see the "Configuring the Transmit Rate" section on page 5-23. The default settings work well in most environments.
7. To enable encryption, click the **Encryption** tab and perform the following:
   a) Place a check mark in the **Enable Encryption** check box.
   b) Determine a set of encryption keys for use by the ad-hoc network, and the position (1, 2, 3, or 4) for each key.
   c) Enter the keys in the **Encryption Key** fields. Make sure that the key you enter in position 1 is the same as the key in position 1 in the other clients. Any keys entered in positions 2, 3, and 4 must match the keys in those same positions in the other clients. However, you do not need to enter all the keys used by the other clients.

      Once you leave the Encryption window, the characters in each Key field are replaced by asterisks (*) that fill the field.
   d) In the **Encrypt Data Transmissions using** field, select the key to use when transmitting data. The transmission key must be entered in all the other clients.

   Refer to the "Setting Encryption" section on page 5-27 for additional information.
8. Click **OK** to close the Properties window. Restart the computer when prompted.

All clients must use the same frequency channel. The RoamAbout PC Card operates at its factory-set default channel (see Table A-3 on page A-5). Any other type of PC Card must also use the same radio frequency.

The Wireless Network Name and AP Density parameters are not used in an ad-hoc configuration. Also, you should not enable Power Management, since there is no device, such as an Access Point, to buffer messages while the client is in sleep mode.

Showing Current Access Point Settings

Before modifying parameters on the RoamAbout Access Point, view the current settings.

Using the AP Manager, select the Access Point from the **Managed List** field and click the various buttons, such as **Wireless Parameters**, **Operating Modes**, **IP Network Parameters**, and **Hardware**. In the Wireless Parameters dialog box, click the **Advanced** button to view all the wireless parameters. If you have changed any wireless parameters and have not yet reset the Access Point, both the operating (current) settings and the settings that take affect after the next reset are displayed.

Using the console port RoamAbout Access Point Installation Menu, choose **Show Current Settings** to display the current Access Point settings as shown below.

```
================================================================

RoamAbout Access Point CSIWS, Wireless Bridge: HW=V2.2,RO=V1.7,SW=V6.00
SysUpTime                          : 00:26:37   98 resets
SNMP Read/Write Community          : public
Console Password                   : Disabled
SNMP Trap Addresses                : Not Configured
Wired MAC Address                  : 08-00-2B-A3-89-61
IP Address                         : 16.20.40.156
Subnet Mask                        : 255.0.0.0
Default Gateway                    : Not Configured
Wireless MAC Address               : 00-60-6D-92-00-FB
Wireless Network Adapter           : RoamAbout IEEE 2.4 GHz DS 11 Mbit
Adapter Revisions                  : Hardware 4.000 Firmware 4.00
Encryption Capabilities            : 128 bit
Bridge Mode                        : Workgroup
Upline Dump                        : DISABLED
Memory                             : 16777216 bytes

================================================================
                    Press Return for Main Menu ...
```

To display the current wireless settings, choose **Module-Specific Options** then select **Show Wireless Configuration**. If you have changed a wireless parameter but not yet reset the Access Point, the new setting is NOT reflected in this display. The following example shows the screen associated with this option.

```
============================================================


RoamAbout Access Point Wireless Configuration

Current Station Name          : RoamAbout AP
Current Wireless Network Name : RoamAbout Default Network Name
Current Secure Access         : Enabled
Current Channel               : 2.4220 GHz  (802.11-3)
Current AP Density            : Low
Current RTS Threshold         : 2347
Current Transmit Rate         : Auto Rate Select
Current DTIM Period           : 001

                  Press Return for Main Menu ...
```

Showing Current Client Settings

To view or modify the RoamAbout client parameters, open the driver properties as follows:

1. From the Windows desktop, click **Start** then select **Settings→Control Panel**. Double click the **Network** icon.

   Alternately, right-click on **Network Neighborhood** on your desktop then select **Properties** from the menu.

2. For Windows 95 or 98, the Network dialog box is displayed. Click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.

3. For Windows NT, click the **Adapters** tab. In the Network Adapters field, click on **RoamAbout 802.11 DS** to highlight it, then click the **Properties** button.

   The RoamAbout Properties window (Figure 5-1) appears. On a Windows NT system, the **Driver Type** and **Bindings** tabs are not present and an **Adapter** tab is displayed.

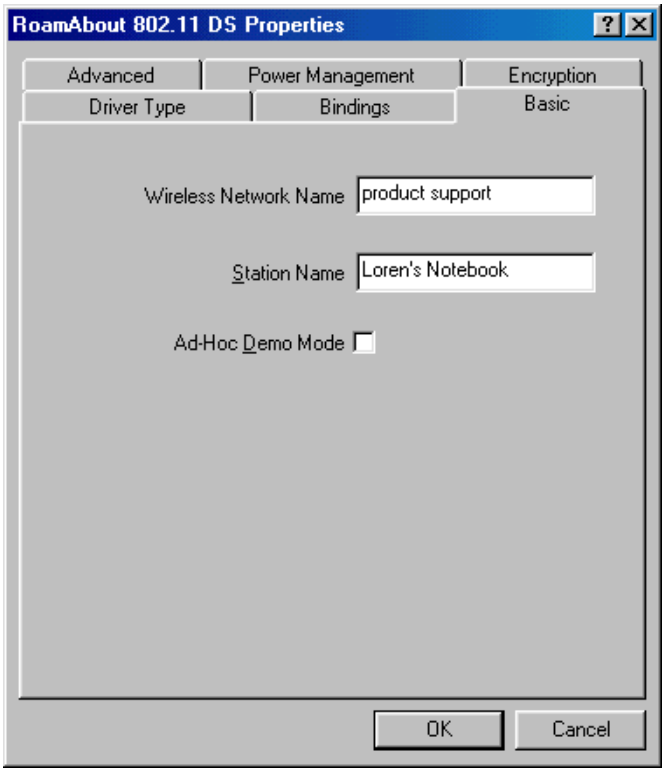
   The **Driver Type** tab lists which RoamAbout driver is used with the PC Card. The **Bindings** tab lists the available network protocols. The protocols with a check mark are associated with the PC Card.

   The **Adapter** tab lists the PC Card I/O Base Address and the Interrupt Request (IRQ) value. You can change these values if the RoamAbout PC Card uses the same I/O Base Address or IRQ as another device in the computer.

   Press <F1> on the keyboard for information about the RoamAbout Properties window.

4. At an Apple PowerBook system, open the **Apple** menu, select **Control Panels** then select **RoamAbout Setup**.

Figure 5-1: RoamAbout Properties Window (Windows 95/98 Version)



NOTE

A change to any of the driver's parameters requires a computer restart for that change to take effect. You are prompted for a restart after you make a change.

Configuring the Transmit Rate

The default setting is the highest transmit rate supported by the RoamAbout PC Card; Fixed is disabled. All RoamAbout PC Cards support, as a minimum, the 1 Mbit/s (Low) and 2 Mbit/s (Standard) transmit rates.

RoamAbout Access Point

To modify the transmit rate on the Access Point using the AP Manager, select the Access Point from the **Managed List** field and click the **Wireless Parameters** button. In the Wireless Parameters window, click the **Advanced** button. Use the **Help** button for a detailed description of the transmit rate settings.

To modify the transmit rate using the console port, choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu. From the module-specific menu, choose **Set Wireless Configuration**, then choose **Set Transmit Rate**. The **Auto Rate Select** option allows the Access Point to transmit at its highest supported transmit rate and to switch to the next lower supported rate when data transmissions fail more than once. The **xx Mbit/s Auto Rate** is the same as Auto Rate Select, except that **xx** determines the Access Point's highest transmit rate. If you do not want to change the transmit rate, press <Enter> to go back to the previous menu.

RoamAbout Client

To modify the transmit rate settings on a client, perform the following:

1. Open the RoamAbout Driver Properties window, as described in the "Showing Current Client Settings" section on page 5-21.
2. Click the **Advanced** tab. Press <F1> for information about the Advanced window.
3. Select the transmit rate.
4. Enable or disable the Fixed setting. When Fixed is enabled, the client does not retransmit failed transmissions at a lower rate (auto rate is disabled).
5. Click **OK** to close the Properties window, and restart the computer when prompted.

Configuring the RTS/CTS Protocol

The RTS/CTS protocol forces the wireless device to transmit an RTS (Request To Send) signal and wait for a CTS (Clear To Send) signal from the receiving wireless device before transmitting a message. Any messages that are shorter in length than the length defined by the RTS/CTS setting do not use the RTS/CTS protocol.

You should not use RTS/CTS unless you have a problem.

RTS Threshold on Access Points

The RoamAbout Access Point uses the RTS Threshold to define the length of messages that must use RTS/CTS. When the message exceeds the threshold, the Access Point sends an RTS to the client (or Access Point in a LAN-to-LAN configuration). The Access Point waits until the device responds with a CTS message.

To reduce or eliminate collisions at the Access Point:

1. Set the RTS Threshold to 500.

   Using the AP Manager, select the Access Point from the **Managed List** field and click the **Wireless Parameters** button. In the Wireless Parameters window, click the **Advanced** button.

   Using the console port, choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu, then choose **Set Wireless Configuration**. If you do not want to change the value, press <Enter> to go back to the previous menu.

2. At a RoamAbout client, use the RoamAbout Client Utility Link Test to determine if the lowered RTS Threshold reduced collisions. You can also use the AP Manager, by selecting **Integrity** from the menu bar, then selecting **Link Test**.

Medium Reservation on RoamAbout Clients

By default, Medium Reservation is disabled. You should only use Medium Reservation if you have a hidden station problem. To modify the Medium Reservation setting on a client, perform the following:

1. Open the RoamAbout Driver Properties window as described in the “Showing Current Client Settings” section on page 5-21.
2. Click the **Advanced** tab. Press <F1> on your keyboard for detailed information.
3. In the Medium Reservation field, select **Off** or **Hidden Stations**.
4. Click **OK** to close the Properties window. Restart the computer when prompted.

Configuring Power Management

By default, power management is disabled on the client. To enable power management:

1. Open the RoamAbout Driver Properties window as described in the "Showing Current Client Settings" section on page 5-21.
2. Click the **Power Management** tab. Press <F1> on your keyboard for detailed information about this window.
3. Place a check mark in the **Card Power Management** check box.
4. Place a check mark in the **Receive All Required Multicasts** check box (recommended).

   You should keep this option enabled to allow the client to receive multicast messages from the wireless network. Missing these messages might result in losing the network connection or other network problems.
5. In nearly all cases, do not change the default value of 100 in the **Maximum Sleep Duration** field. However, a value between 100 to 500 milliseconds may be considered when operating a wireless powered hand-held terminal connected to an infrastructure network that can handle a less critical latency for optimal performance.

RoamAbout PC Cards with Station Firmware lower than Version 2.00 do NOT support power management. Enabling power management for such cards can cause unpredictable computer behavior and a loss of the network connection.

The RoamAbout Access Point automatically supports power management. The only settable power management parameter is the DTIM period, which should not be changed.

To view or modify the Access Point DTIM period using the AP Manager, select the Access Point from the **Managed List** field and click the **Wireless Parameters** button. In the Wireless Parameters window, click the **Advanced** button.

To modify the DTIM period using the console port, choose **Module-Specific Options** RoamAbout Access Point Installation Menu, then choose **Set Wireless Configuration**. If you do not want to change the value, press <Enter> to go back to the previous menu.

Setting Default Rate Limiting (Multicast Traffic)

By default, the Access Point is configured to limit multicast traffic to 100 Kb/sec. This parameter is not available on the RoamAbout client.

To enable or disable this parameter using the AP Manager, click the **Operating Modes** button in the main window.

To enable or disable this parameter using the console port, select the **Module-Specific Options** in the RoamAbout Access Point Installation Menu.

To change the value of this setting (instead of enabling or disabling the 100 Kb/sec value), you need to manage the Access Point from a Network Management Station.

Configuring Security

To have the most amount of security in your wireless infrastructure network:

- Set up your networking protocols to require user names and passwords. Refer to the documentation that came with the networking software or operating system.
- Enable Secure Access at the Access Points.
- Enable encryption and configure clients that you want to be in the network with the proper encryption keys.
- Configure the Access Points to not communicate with unencrypted clients.

You can also use encryption in a LAN-to-LAN configuration and ad-hoc networks to enhance security.

Setting Secure Access

Secure Access only applies in a wireless infrastructure network. This parameter is only available at the Access Point.

When Secure Access is enabled, the Access Point denies access to wireless clients that do not use the correct wireless network name. When Secure Access is disabled, the Access Point allows access to wireless clients that use **ANY** (all uppercase) as the wireless network name or have a blank wireless network name.

To enable or disable Secure Access using the AP Manager, click the **Wireless Parameters** button. Use the **Help** button for detailed information.

To enable or disable Secure Access using the console port, choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu, then choose **Set Wireless Configuration**. If you do not want to change the value, press <Enter> to go back to the previous menu.

Setting Encryption

Perform the following steps to configure encryption for the wireless network.

1. Create up to four keys, where the keys can be:

   — 5 printable characters or 10 hexadecimal digits if the RoamAbout PC Card supports 40-bit WEP encryption.

   — 13 printable characters or 26 hexadecimal digits if the RoamAbout PC Card supports 128-bit encryption.

   You must create at least one key. The printable character keys are case sensitive.

   A hexadecimal digit key must start with 0x, which is not counted in the number of digits. For example, 0xABCDEF0123 is a valid 40-bit encryption hexadecimal key (10 hexadecimal digits).

2. Determine the positions for each key. There are four positions, Key 1, Key 2, Key 3, and Key 4. The position of each key is important since all the wireless devices must enter the same key in the same position to decipher encrypted data.

3. If using the AP Manager, click the **Encryption** button. In the Encryption dialog box, enable encryption, enter the keys, choose a transmit key, and enable or disable **Deny Non-encrypted Data**. Click the **Help** button for detailed information.

4. Perform the following steps to configure encryption on an Access Point if using the console port:

   a) Select **Set Encryption Configuration** from the RoamAbout Access Point Installation Menu.

   b) Enter the keys using the **Set Encryption Key** menu options.

   c) Choose one key to be the transmit key using the **Set Transmit Key** option. Each Access Point can use a different transmission key as long as the other devices have that key entered in the same position.

d) Choose one of the following options if the Access Point is configured for a wireless infrastructure network:

— Enable **Set Exclude Unencrypted** to only accept encrypted data from clients. Only clients that have the correct keys can participate in this network.

— Disable **Set Exclude Unencrypted** to accept both encrypted and unencrypted data from different clients. This allows clients who require security to use encryption without preventing other clients from using the network.

e) Enable encryption using the **Set Encryption State** menu option.

f) To prevent any management tool using SNMP, including the AP Manager, from changing the encryption parameters, enable the **Set Exclude SNMP** menu option.

5. Reset the Access Point as follows. You do not need to reset the Access Point if you only add, delete, or modify keys, or change the transmit key.

— If using the AP Manager, select **Reset** from the main window, then select **Reset with Current Settings**.

— If using the console port, select **Reset with Current Settings** from the RoamAbout Access Point Installation Menu.

Allow approximately one minute for the Access Point to reset and complete its self-test.

6. To configure encryption on the RoamAbout clients:

a) Open the RoamAbout Driver Properties window as described in the "Showing Current Client Settings" section on page 5-21.

b) Click the **Encryption** tab. Press <F1> on your keyboard for detailed information about the Encryption window.

c) Place a check mark in the **Enable Encryption** check box.

d) Enter the keys in the correct **Encryption Key** fields. Make sure that the keys are in the same positions as the other wireless devices.

After you leave the Encryption window, the characters in each Key field are replaced by asterisks (*) that fill the field.

e) In **Encrypt Data Transmissions using**, select the key you want the client to use when transmitting data. Each wireless device can use a different transmission key as long as the other devices have that key entered in the same key position.

f) Click **OK** to close the RoamAbout Driver Properties window. Restart the computer when prompted.

Configuring the Access Point Console Port for Security

The following security settings are exclusive to the console port on the Access Point:

- To prevent other users from using the console port, enable **Enable/Disable Console Password** from the RoamAbout Access Point Installation Menu. Then choose **Set SNMP Read/Write Community** from the Installation Menu and enter a new community name (4 to 31 printable ASCII characters). Afterwards, users must enter the community name to access the menu.
- To prevent any management tool using SNMP, including the AP Manager, from changing the Encryption parameters, enable **Set Exclude SNMP** from the Encryption menu.

Setting Spanning Tree

By default, Spanning Tree is disabled when in Workgroup bridge mode and enabled in LAN-to-LAN Multipoint bridge mode. You can enable or disable Spanning Tree while the Access Point is in LAN-to-LAN Endpoint bridge mode only. This parameter is only available on the Access Point with the V6.0 or later firmware release.

To enable or disable Spanning Tree using the AP Manager, select the Access Point from the **Managed List** field and click the **Wireless Parameters** button. In the Wireless Parameters window, click the **Advanced** button. Select **LAN-to-LAN Endpoint**.

To enable or disable Spanning Tree using the console port, choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu, then choose **Bridge Mode Options**. If you do not want to change the value, press <Enter> to go back to the previous menu.

It is important to avoid Point-to-Multipoint configurations that will cause bridge loops. A bridge loop occurs when two parallel network paths are created between any two LANs, causing packets to be continuously regenerated through both parallel paths. This situation eventually renders the network unusable due to the excessive traffic that is being generated by the loop. The Access Point spanning tree function corrects this type of problem by shutting down the bridge and possibly shutting down a segment of the network.

Checking the Configuration on Multiple Access Points

The AP Manager provides integrity tests that check for consistent settings across all the Access Points in a single group. Use the integrity tests to make sure that the Access Points in a single wireless network are configured correctly. To access the tests, click **Integrity** on the AP Manager menu bar.

The **Parameters** option tests that all Access Points are configured with the following:

- Same bridge mode
- Same wireless network name
- Different station name
- Same AP Density setting
- Same transmit rate
- Same Secure Access setting
- Same RTS Threshold
- Same rate limiting setting
- Same upline dump setting
- Same forwarding setting

Values not used in LAN-to-LAN mode are not checked when the Access Point is in LAN-to-LAN mode.

The **Firmware Revisions** option verifies that all Access Points have the same version of the firmware.

The additional menu item, **Link Test**, is used to test the communications quality between the Access Point and another wireless device.

Resetting the RoamAbout Access Point

There are two ways to reset the Access Point:

- **Reset with Current Settings**

  If you change any wireless configuration parameter, such as the wireless network name or channel, you must select this option to reset the Access Point to implement your changes.

  From the AP Manager, select **Reset** then select **Reset with Current Settings**.

  From a device attached to the console port, select **Reset with Current Settings** from the RoamAbout Access Point Installation Menu.

  Allow approximately one minute for the Access Point to reset and complete its self-test.

- **Reset with Factory Defaults**

  This option reboots the Access Point, causing the Access Point's configured parameters to be initialized to factory default values.

  This action deletes all configuration settings and replaces them with factory default values. All configuration settings are lost, including the IP address.

  From the AP Manager, select the Access Point from the **Managed List** field, click the **Reset** button, then click the **Reset with Factory Defaults** button.

  From a device attached to the console port, select **Reset with Factory Defaults** from the RoamAbout Access Point Installation Menu.

  The Access Point hardware has a reload/reset button that forces the Access Point to download a new firmware image from a BootP/TFTP server and reset to factory default values. If a new image is not available, the Access Point resets to factory default values after approximately three minutes. Make sure that you do not have multiple BootP/TFTP servers configured to load the Access Point; you might load an incorrect image.

  Allow approximately one minute for the Access Point to reset and complete its self-test.

Modifying the Access Point SNMP Settings

For the AP Manager or any Network Management Station to remotely manage the Access Point, the Access Point must have:

- A valid IP address and subnet mask.
- An SNMP read/write community name (default is **public**).

The following sections describe how to modify these parameters.

Changing the IP Address

To change or delete the Access Point's current IP address from the AP Manager, the Access Point must be currently managed by the AP Manager. If you do not know the Access Point IP address, use the Access Point console port to view or change the address.

1. Select the Access Point from the **Managed List** field.
2. Click the **Network Parameters** button.
3. Set the **Address State** to **Volatile**, then click **OK**.
4. In the main AP Manager window, click the **Reset** button. Then click **Reset with Current Settings**. This sets the IP address to 0.0.0.0. The Access Point is no longer manageable by the AP Manager.
5. Use the **Setup/Add New Access Point** button to give the Access Point a new IP address and add it back to the list of managed Access Points. You can use the procedures to configure Access Points listed earlier in this chapter.

To modify only the subnet mask or default gateway using the AP Manager, select the Access Point from the **Managed List** field and click the **Network Parameters** button.

To change the Access Point's IP parameters using the console port:

1. Choose **Set IP Address** from the RoamAbout Access Point Installation Menu.
2. Enter the new IP address, subnet mask, or default gateway. You do not need to reset the Access Point.

Changing the SNMP Read/Write Community Name

The AP Manager and any other SNMP Manager must have the correct read/write community name associated with the Access Point; otherwise, the tool cannot make any changes to the Access Point.

If using the AP Manager to change the Access Point read/write community name, the read/write community name currently entered in the AP Manager must be the same as the read/write community name in the selected Access Point. Otherwise, you will see a message when attempting to change a parameter.

To use the AP Manager to change the read/write community name in the Access Point and in the AP Manager, click on the **Options** menu and select **Community Strings**. Click the **Help** button for detailed information.

To change the read/write community name for the Access Point using the console port:

1. Choose **Set SNMP Read/Write Community** from the RoamAbout Access Point Installation Menu.
2. Enter the community name (4 to 31 printable ASCII characters).

Using a Local MAC Addressing Scheme

All RoamAbout PC Cards have a unique universal MAC address that is used to identify the computer on the network. For most network operating systems, you do not need to change the MAC address.

If your network system uses a local MAC addressing scheme, you may need to assign a local MAC address value to the PC Card as follows:

1. Open the RoamAbout Driver Properties window as described in the “Showing Current Client Settings” section on page 5-21.
2. Click the **Advanced** tab.
3. In the MAC Address field, enter the local MAC Address value. Valid address values are 12-digit hexadecimal values, where the second digit must be 2, 6, A, or E.
4. Click **OK** to close the RoamAbout Driver Properties window. Restart the computer when prompted.

The RoamAbout PC Card in an Access Point cannot be changed to a local MAC address.

Chapter 6

Maintaining the Wireless Network

To maintain the wireless network, you should regularly check the wireless coverage area, communications quality, and data throughput efficiency.

As your environment changes, you may need to adjust wireless parameters or move Access Points to account for new obstructions or new sources of radio interference. You may also need to add Access Points should the number of users increase.

In addition, you should regularly check the RoamAbout web site for product updates. This chapter contains the procedures to upgrade the RoamAbout products.

Testing Radio Communications Quality

You can test the radio communications quality from the Access Point to another wireless device using the AP Manager, or from a client to another wireless device using the RoamAbout Client Utility.

Using the Access Point Manager

The RoamAbout AP Manager provides a Link Test tool that tests the signal quality from the Access Point to a client or another Access Point.

1. Select the Access Point from the **Managed List** field in the AP Manager main window.
2. Click **Integrity** in the menu bar.
3. Select **Link Test**.
4. Under **Remote Station Info** in the Link Test window, click the down arrow to list the available clients in the wireless network or the remote Access Points in a LAN-to-LAN configuration.
5. Choose the client or Access Point to test the signal quality, then click the **Start Sampling** button to start the test. To stop the test, click the **Stop Sampling** button.
6. Check the signal level and noise level if the SNR is low between the Access Point and the other wireless device.

   If the signal level is low, the devices may be too far apart or there are obstructions between them. If possible, remove the obstructions, move the devices closer, or use the optional Range Extender antenna described on page 1-15.

   If the noise level is high, you may have one or more devices emitting radio signals in the same frequency band as the client. Determine the source of interference by selecting other clients. If available, use the RoamAbout Client Utility Link Test tool at a mobile client to determine the extent of the noise. The source of the noise may be closest to the device that has the highest noise level. Try to eliminate or move the source of the noise.

Using the Client Utility

This procedure requires the RoamAbout Client Utility on a RoamAbout client. For information about a client utility window, press <F1> while in that window.

1. Start the RoamAbout Client Utility by clicking **Start** from the Taskbar then selecting **Programs→RoamAbout→RoamAbout Client Utility**. Click the **More** button if the Status/Functions window is not displayed.

2. Select **Link Test** from the Status/Functions window.

   If connected to an infrastructure network, the test partner is the associated Access Point. If configured for an ad-hoc network, select another client in the network to be the test partner then select the **Test Results** tab.

3. Check the Signal-to-Noise (SNR) indicator, which changes color according to the communications quality as follows:

   — Green. Communications quality is good.

   — Yellow. Communications quality is adequate. Optionally, click the **Advice** button in the Link Test window for tips on improving communications quality.

   — Red. Communications quality is poor and requires user intervention.

4. Check the Signal Level and Noise Level indicators if the SNR indicator is red.

   A high noise level indicates that you may have one or more devices emitting radio signals in the same frequency band as the client. Run the Link Test on other clients to determine the extent of the noise. The source of the noise may be closest to the device that has the highest noise level. Try to eliminate or move the source of the noise.

   A low signal level indicates that the client and the test partner may be too far apart or there may be obstructions between them. If possible, remove the obstructions, move the devices closer, or use the optional Range Extender antenna described on page 1-15.

The Link Test window has an **Advice** button. Click this button for specific troubleshooting suggestions.

Testing Data Throughput Efficiency

This procedure requires the RoamAbout Client Utility on a RoamAbout client. For information about a client utility window, press <F1> while in that window.

1. Start the RoamAbout Client Utility by clicking **Start** from the Taskbar then selecting **Programs→RoamAbout→RoamAbout Client Utility**. Click the **More** button if the Status/Functions window is not displayed.
2. Select **Link Test** from the Status/Functions window.

   If connected to an infrastructure network, the test partner is the associated Access Point. If configured for an ad-hoc network, select another client in the network to be the test partner then select the **Test Results** tab.
3. Check the **Total Messages** column. Data throughput efficiency is measured in messages sent, lost, or received.
4. Divide the number of **Messages Lost** by the number of **Messages Sent**. The Messages Sent number must be greater than 200.

   Typically, the number of Messages Lost is less than 1 percent of the number of Messages Sent. If this number increases to 5 percent, you may have communication problems. If necessary, click the **Reset** button to observe only the current data throughput.

If the SNR is low and the number of messages lost is high, the problem is likely due to a poor communications quality. For example, the client and the test partner are too far apart or the connection suffers from a source of noise interference. Check the communications quality as described in “Testing Radio Communications Quality” section on page 6-2.

If the SNR is adequate or good but there is a relatively large number of messages lost or received after a retry, the problem might indicate:

- A very busy network where many clients try to access the medium at the same time.
- A microwave oven in close vicinity (7 to 10 feet) to the client or Access Point is causing short bursts of interference. This noise might not be displayed by the noise level indicator, but could still be forcing the clients to retransmit frames.
- Another client is suffering from a poor communications quality and is consequently sending many retransmissions.
- Numerous frame collisions are occurring due to a hidden station problem.

Run the RoamAbout Client Utility link test from multiple clients to determine if the problem is local (one client only) or experienced by all clients.

If all clients suffer from poor data throughput efficiency despite a good SNR value, the traffic load could be caused by the following:

- Many wireless clients are trying to communicate simultaneously.
- Clients are deferring data transmissions to avoid frame collisions.
- Clients are retransmitting frames repeatedly because initial transmissions failed, which can be due to frame collisions.

If one or more clients are transmitting simultaneously with the Access Point in an infrastructure network, you may need to lower the RTS Threshold on the Access Point as described in the "RTS Threshold on Access Points" section on page 5-24.

If the concentration of users per Access Point is high, you may need to place the Access Points closer together to distribute the load, or add Access Points to the wireless network.

To measure values over time, click the **Test History** tab. For example, you have a performance problem during the mid-afternoon but not at other times. Use Test History to measure wireless performance between 2:00 pm to 3:00 pm. You can save the test results to a log file, as described in the "Logging Measurement Data" section on page 6-9.

Optimizing RoamAbout Access Point Placement

The RoamAbout AP Manager and RoamAbout Client Utility provide diagnostic tools to determine the coverage area of an Access Point. If you have multiple Access Points in a wireless network, the client utility can help determine where the coverage areas overlap.

You may need to use these tools after you initially install the Access Points, and on a regular basis to determine if the coverage areas change due to new obstructions or new sources of radio interference.

Using Site Monitor

This procedure requires the RoamAbout Client Utility on a RoamAbout client. For information about a client utility window, press <F1> while in that window.

This procedure is best performed on a mobile client that you can use to walk through the coverage area of the Access Point.

1. Start the RoamAbout Client Utility by clicking **Start** from the Taskbar then selecting **Programs→RoamAbout→RoamAbout Client Utility**. Click the **More** button if the Status/Functions window is not displayed.
2. Select **Site Monitor** from the Status/Functions window. If the **Site Monitor** button is not available, click the **Options** button and enable **Enhanced mode**.
3. Select the network in the **Selection** tab if you have multiple wireless networks.
4. For best results, display the **AP Name**, **MAC Address**, **SNR**, and **Channel** in the Site Monitor window.
5. Walk through the wireless network environment with Site Monitor running. Watch the Site Monitor display to verify that each location is covered by at least one Access Point that provides an Adequate (Yellow) or Good (Green) communications quality.

If you see a poor SNR in any area that you want to be covered, change the columns to display the **AP Name**, **Signal Level**, and **Noise Level**.

A low signal level indicates that the Access Points may be too far apart. Relocate or add Access Points to create a contiguous wireless coverage area, where communications quality is Adequate or better.

If the noise level is high, walk through the area monitoring the Noise Level indicator to determine the location of the source of interference. If possible, switch off the source of interference or relocate it to minimize the impact of interference on the wireless network.

Using Link Test

The RoamAbout AP Manager provides a Link Test diagnostic tool that tests the signal quality from the Access Point to a client or another Access Point.

1. Select the Access Point from the **Managed List** field in the AP Manager main window.
2. Click **Integrity** in the menu bar.
3. Select **Link Test**.
4. Under **Remote Station Info** in the Link Test window, click the down arrow to list the available clients in the wireless network or the remote Access Points in a LAN-to-LAN configuration.
5. Choose the client or Access Point to test the signal quality, then click the **Start Sampling** button to start the test. To stop the test, click the **Stop Sampling** button.
6. Check the signal level and noise level if the SNR is low between the Access Point and the other wireless device.

   If the signal level is low, the devices may be too far apart or there are obstructions between them.

   If the noise level is high, determine the source of interference by selecting other clients. If available, use the RoamAbout Client Utility Site Monitor tool at a mobile client to better determine the location of the interference.

Optimizing RoamAbout Outdoor Antenna Placement

If an Access Point in a LAN-to-LAN configuration is connected to an outdoor directional antenna, the antenna must be pointed directly at the antenna for the other Access Point. A misaligned antenna can decrease the signal level or prevent communications.

The RoamAbout AP Manager provides a Point-to-Point diagnostic tool that can help you adjust the directional antenna to optimize the signal between Access Points. If you are testing the link between two Access Points that both use directional antennas, you may need one person at each antenna and a method to communicate with those people.

1. Select the Access Point from the **Managed List** field in the AP Manager main window.
2. Click **Integrity** in the menu bar.
3. Select **Link Test**.
4. Under **Remote Station Info** in the Link Test window, click the down arrow to list the available Access Points in the LAN-to-LAN configuration.
5. Choose the Access Point to test the signal quality, then click the **Start Sampling** button to start the test.
6. To improve the signal strength, watch the SNR indicator and slowly move the antenna in the direction that improves SNR. You may need to have a person at the remote location move the antenna while monitoring the SNR.
7. To stop the test, click the **Stop Sampling** button.

Logging Measurement Data

You can save the results of your RoamAbout Client Utility Link Test or Site Monitor session in a log file. To enable logging, set the client utility to enhanced mode by clicking the **Options** button in the Status/Functions window. For information about a client utility window, press <F1> while in that window.

You can use this log file to:

- Evaluate the results at a later time.
- Compare the results with previous measurements, which may help you investigate the performance of your wireless LAN over a period of time.
- Send the measurement results to your RoamAbout support representative when troubleshooting a specific problem.

The client utility allows you to log measurement data manually or automatically at regular intervals.

To set the logging options, click the **Log Settings** tab in the Site Monitor or Link Test window. You can choose to append data to an existing log file or create a new file.

The log files are saved in a Comma Separated Value (CSV) file format. You can read the files with an ASCII editor or import the data into a spreadsheet or database application.

Checking the Client RoamAbout PC Card

The RoamAbout Client Utility has a Diagnose Card tool that checks the hardware and firmware of the RoamAbout PC Card.

Run the card test only in situations where the Status/Functions window reports a card failure or when you suspect a configuration mismatch. When contacting RoamAbout technical support, the card test results may help the support representative determine the cause of a malfunctioning device.

To access the card test, select **Diagnose Card** from the Status/Functions window. For information about the Diagnose Card tool, press <F1> while in the Card Check window.

Running the card test may temporarily disrupt the communication of your client with the network. In exceptional cases, you may lose your network connection. If this occurs on a Windows NT system, restart your system. If this occurs on a Windows 95 or 98 system:

1. Close the client utility program.
2. Remove the PC Card.
3. Wait several seconds then reinsert the card.

Monitoring the Access Point Using RMON

The Access Point supports four of the nine Remote Network Monitoring MIB (RMON) groups:

- **Statistics** - Contains statistics measured by the probe for the wired LAN and the wireless LAN interfaces.
- **History** - Records periodic statistical samples from a network and stores them for later retrieval.
- **Alarm** - Periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.
- **Event** - Controls the generation and notification of events from this device.

The settings for these groups can only be accessed with a Network Management System. The console port and AP Manager cannot change or view the RMON group settings.

When the Access Point is initialized, two statistics groups are generated. One group is for the wired interface and one is for the wireless interface. Also, two History groups are generated for each interface. One group has a short term polling period of 30 seconds and one has a long term polling period of 30 minutes.

The Access Point has the following limits for the RMON MIB because of memory limitations:

- A maximum of six Statistics groups.
- A maximum of four History groups, with a maximum of 200 “buckets”, also called samples, for all groups. You can reconfigure each group. For example, you could assign 80 buckets each to the long and short term History groups assigned to the wired interface, and 20 buckets each to the long and short term History groups assigned to the wireless interface. This example does not exceed the maximum of 200 buckets.
- A maximum of ten Alarm groups.
- A maximum of ten Event groups.

Checking RoamAbout Product Version Numbers

To check the RoamAbout Access Point firmware version, run the RoamAbout AP Manager, choose the **Hardware** button and check the software version (SW=Vx.x). Refer to the AP Manager on-line help for additional information.

To check the RoamAbout Access Point firmware version using the console port, select **Show Current Settings** from the Installation Menu. The top line contains the firmware version (SW=Vx.x).

To check the versions of the RoamAbout PC Card Driver and Station Firmware in a RoamAbout client, run the RoamAbout Client Utility, choose **Diagnose Card** then choose the **Version Info** tab. The version of the client utility is also displayed.

If the client utility is not available, you can also check the driver version as follows:

1. Open Windows Explorer.
2. Find the WVLAN41.SYS file. Typically, this is located in the C:\WINDOWS\SYSTEM folder for Windows 95 and 98, or the C:\WINNT\SYSTEM folder for Windows NT.
3. Right click on the WVLAN41.SYS file then select **Properties** on the menu.
4. In the Properties window, click the **Version** tab. The **File Version** number near the top of the window is the driver version number.

For information about the latest available versions, check the RoamAbout web site.

Upgrading the RoamAbout Access Point Firmware and ROM

The Access Point firmware, also called embedded software, can be easily upgraded. Regularly check the RoamAbout web site for the latest information concerning RoamAbout updates. To upgrade the Access Point, copy the image file (*.BIN) from the web site to the same directory as the AP Manager or BootP/TFTP server. The Access Point 2000 (hardware release V2) requires an N*.BIN file. The previous release of the Access Point hardware (V1) requires a V*.BIN file. The Access Point ROM upgrade (hardware release V2) requires a R*.Bin file.

To view the Access Point hardware version click the **Hardware** button on the AP Manager main window.

If the power is interrupted during the ROM upgrade process, the image in your device will become corrupt. Do not turn off or perform any action that can cause power loss during a ROM upgrade.

The AP Manager includes a BootP/TFTP loader, called NetRider Loader, that upgrades the Access Point. If not using the AP Manager, you need to configure a BootP/TFTP server. Make sure that you do not have multiple BootP/TFTP servers configured to load the Access Point; you might load an incorrect image.You can only upgrade one Access Point at a time. When you start the upgrade, the Access Point immediately stops its operation.

Using the AP Manager

To upgrade the Access Point using the AP Manager, click the **Reload Now** button and follow the on-line instructions. The NetRider Loader utility loads the new firmware. The upgrade takes a few minutes, during which the Access Point is unavailable. You can determine when the upgrade is complete by looking at the Access Point LEDs or by trying to view parameters using the AP Manager.

Using the Access Point Console Port

To upgrade the Access Point using the console port:

1. Make sure that you have properly configured a BootP/TFTP server.
2. Choose **Module-Specific Options** from the Access Point Installation Menu.
3. Choose **Upgrade Flash** from the next menu. You are asked to confirm the upgrade.

Using the Access Point Hardware Reset Button

The Reset button on the Access Point hardware forces the Access Point to download a firmware image and reset to factory default values.

If the power is interrupted during the ROM upgrade process, the image in your device will become corrupt. Do not turn off or perform any action that can cause power loss during a ROM upgrade.

To use the Reset button:

1. Remove AC power from the Access Point.
2. Restore AC power then press the Reset button on the Access Point. If an image is not available, the Access Point waits approximately three minutes then resets to factory default values.

Replacing the PC Card in an Access Point

You may need to replace a defective PC Card or upgrade the PC Card in an Access Point. If upgrading the Access Point from a 2 Mbit/s PC Card to an 11 Mbit/s PC Card, make sure that the Access Point firmware version is V5.0 or greater, as described in the "Checking RoamAbout Product Version Numbers" section on page 6-12.

Also, you should disable encryption before replacing a PC Card with one does not support encryption.

To change the PC Card in an Access Point configured for a wireless infrastructure network, you only need to remove AC power, replace the PC Card, and power on the Access Point.

To change the PC Card in an Access Point configured for a LAN-to-LAN network, perform the following:

1. Remove AC power.
2. Replace the PC Card.
3. Power on the Access Point.
4. Change the wireless MAC address on each remote Access Point configured to communicate with this Access Point. The wireless MAC address for an Access Point is printed on the back of its PC Card.

Upgrading the RoamAbout Miniport Driver

The RoamAbout Miniport driver is used on Windows 95, 98, and NT systems. Upgrading the installed RoamAbout driver may be required if:

- You want to use new features that have become available for your RoamAbout PC Card.
- You installed a newer version of the RoamAbout Client Utility.
- The RoamAbout Client Utility reported a driver or firmware mismatch.

The procedure to upgrade drivers differs between the various Windows operating systems:

- Windows 98, Windows NT, and later versions of Windows 95 (OSR2) have an Update Driver function that allows you to easily upgrade the current driver.
- Early versions of the Windows 95 system require you to completely remove the driver from your computer before installing the latest driver.

Upgrading the Driver for Windows 95 (OSR2) and Windows 98

Use the following procedure to upgrade the RoamAbout driver on Windows 95 and Windows 98 systems. Early releases of Windows 95 do not have the Update Driver feature.

1. From the Taskbar on the Windows desktop, click **Start** then select **Settings→Control Panel**.
2. In the Control Panel window, double-click the **System** icon.
3. In the System Properties window, select the **Device Manager** tab.
4. In the top section of the Device Manager tab, select **View devices by type**.
5. In the list of computer devices, double-click **Network Adapters**.
6. Select “RoamAbout PC Card” and click the **Properties** button.
7. In the RoamAbout Properties window, select the **Driver** tab. If there is no Driver tab, you may be using an early version of Windows 95.

   For information about the installed driver, click the **Driver File Details** button.
8. To upgrade the driver, click the **Update Driver** button and follow the instructions displayed on the screen. If there is no **Update Driver** button, go to the “Upgrading the Driver for Windows 95 (Early Version)” section on page 6-17.
9. Restart the computer to finish the upgrade procedure and to load the new driver.

Upgrading the Driver for Windows NT

Use the following procedure to upgrade the RoamAbout driver on Windows NT systems.

1. From the Taskbar on the Windows desktop, click **Start** then select **Settings→Control Panel**.
2. In the Control Panel, double-click **Network**.
3. Select the **Adapters** tab.
4. Select **RoamAbout Adapter** and click **Update**.
5. Follow the instructions as they appear on your screen.

Upgrading the Driver for Windows 95 (Early Version)

Upgrading to a new driver on early versions of Windows 95 usually requires deleting the old driver file from your hard disk before installing the new driver.

The early versions of Windows 95 associate a specific driver with specific hardware. When you select the Remove Driver option from the Network Control Panel, the operating system disables the driver but does not delete the driver from your hard disk. Therefore, when you upgrade a driver, Windows recognizes your RoamAbout PC Card as hardware that had been installed before and attempts to reinstall the old driver.

To upgrade your RoamAbout driver on an early version of Windows 95, follow the procedure in “Deleting the RoamAbout Driver Files” section on page 6-18. Then, follow the instructions that came with the RoamAbout PC Card to install the driver.

Removing the RoamAbout Miniport Driver

If you have Version 1.0 of the RoamAbout Miniport driver, you need to perform extra steps. Check the driver version number as described in the "Checking RoamAbout Product Version Numbers" section on page 6-12, before performing this procedure.

1. Remove the PC Card from the PC Card slot.
2. Close all open applications.
3. From the Taskbar on the Windows desktop, click **Start** then select **Settings→Control Panel**.
4. In the Control Panel window, double-click the **Network** icon.
5. Select the RoamAbout PC Card and click the **Remove** button. Then click **OK**.

   The Windows operating system disables the Miniport driver and updates the driver configuration files.
6. Do NOT restart the computer if you have V1.0 of the miniport driver. Instead, perform the procedure in next section to delete the driver and its information and configuration files from your hard disk.
7. If the driver version is later than V1.0, restart the computer.

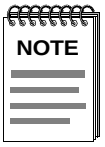
Deleting the RoamAbout Driver Files

The procedure to remove the RoamAbout Miniport Driver files from the hard disk is similar for all Windows operating systems.

1. If not already done, remove the RoamAbout driver as described in the previous section. Otherwise, the Windows Registry is not "cleaned", which can lead to complications when installing the RoamAbout driver in the future.
2. Open Windows Explorer.
3. In the Explorer menu, click on **View** and select **Options**.
4. From the View tab, select **Show all files** and clear the **Hide MS-DOS file extensions** check box.
5. Click the **Apply** button to return to the Explorer window.
6. In Explorer, open the Windows operating system folder:
   - C:\WINDOWS\SYSTEM for Windows 95 and 98
   - C:\WINNT\SYSTEM32\DRIVERS for Windows NT

7. For Windows 95 and 98 systems, delete these RoamAbout driver files:
   - WVLAN41.SYS
   - WVLANUIF.VXD
   - WV41INST.DLL (if present)
   - WVLAN41.HLP
   - WVLAN41.CNT
   - WVLAN41.FTS (if present)
   - WVLAN41.GID (if present)
   - RMABT41.HLP (if present)
   - RMABT41.CNT (if present)
   - RMABT41.GID (if present)

8. Also for Windows 95 and 98, open C:\WINDOWS\INF and delete the RMABT41.INF file.



In Windows 98, this file might be located in C:\WINDOWS\INF\OTHER.

9. For Windows NT systems, delete these files:
   - WVLAN41.SYS
   - WVLAN41.DLL
   - WVLAN41.HLP
   - WVLAN41.CNT
   - WVLAN41.FTS (if present)
   - WVLAN41.GID (if present)
   - RMABT41.HLP
   - RMABT41.CNT (if present)
   - RMABT41.FTS (if present)
   - RMABT41.GID (if present)

10. Close Windows Explorer and restart your computer.

If deleting the driver files was part of an upgrade procedure, install the new driver as described in the RoamAbout PC Card documentation.

Removing the Apple Driver

Removing a previously installed Apple driver is mandatory to:

- Upgrade a driver.
- Change the type of driver. For example, you would change the type of driver when migrating from Apple Classic to Apple Open Transport.

To remove the driver, proceed as follows:

1. Insert the RoamAbout diskette for the MAC operating system into your Apple PowerBook. This should be the same diskette that you used to install the driver.
2. Double-click the diskette icon on the desktop of your computer to display the contents of this diskette.
3. Double-click **RoamAbout Installer** to start the installation program.
4. In the Welcome window, click **Continue**.
5. From the list of options, select **Custom Remove**. Click all boxes to completely remove the driver. If you have any open applications, you are prompted to close them.
6. Follow the on-line instructions. When completed, restart your computer.

Upgrading the RoamAbout PC Card Firmware

You can use the RoamAbout Work Station Update (WSU) tool to update the firmware (also called embedded software) of your RoamAbout PC Cards.

When new features for your RoamAbout PC Card become available, they are typically distributed as a new version of the RoamAbout Work Station Update tool via the RoamAbout web site.

To identify whether you need to update the firmware of the PC Card, verify the current version of the Secondary Card Firmware loaded into the card using the **Version Info** tab on the **Diagnose Card** panel of your RoamAbout Client Utility.

If you update your RoamAbout PC Card firmware, you may need to update the RoamAbout driver as well. In most cases, the WSU tool prompts you to do so, prior to updating the card; therefore, when browsing the RoamAbout web site to download newer versions of the WSU tool, you should download the latest driver as well.

Chapter 7

Problem Solving

This chapter contains problem solving information for the RoamAbout wireless network.

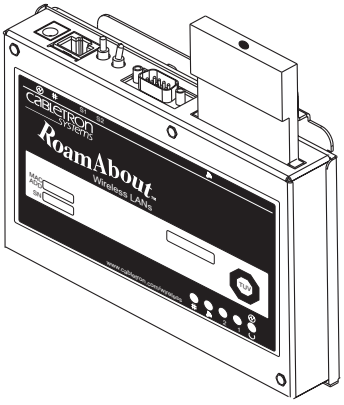
If the problem appears to be with an Access Point or a specific client, check the LEDs first. The Access Point LEDs are described in the next section. The client LEDs are described on page 7-20.

Using the Access Point LEDs to Determine the Problem

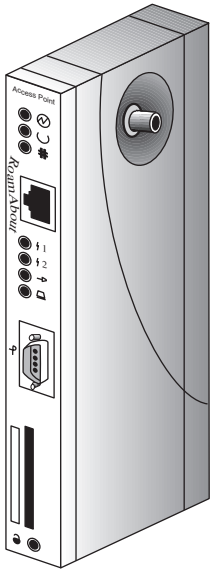
The Access Point LEDs show status and help diagnose problems. The following sections describe the LEDs on the Access Point 2000 and the original release of the Access Point.

The following figure shows the two Access Points.

Figure 7-1: RoamAbout Access Points



Access Point 2000



Original Access Point

Access Point 2000 LEDs

Table 7-1 describes the function of each of the LEDs. Error conditions cause the LEDs to turn on, off, or blink in a pattern. Table 7-2 describes the patterns, the most likely causes, and possible corrective actions. Table 7-3 describes the LED patterns during an Access Point firmware upgrade. If you suspect an Access Point failure, run the self-test by removing then reapplying AC power.

Table 7-1: RoamAbout Access Point 2000 LED Summary Table

Name	Description
Power/ System OK 	Lights when the Access Point has power and has passed the self-test. If the Access Point fails the test, the LED blinks at a steady rate.
Bridge State 	Lights when the Access Point is forwarding packets.
Access Point Saturated 	Lights when the Access Point is saturated. Saturation occurs when the Access Point cannot forward packets from the Ethernet to the wireless side due to the lower throughput of the wireless network. The degree of LED brightness indicates the level of saturation. The LED dims (and eventually extinguishes) as the network congestion is processed.
Wireless LAN Activity 	Lights when packets are: • Received on the wireless port and forwarded to the Ethernet port. • Received on the Ethernet port and forwarded to the wireless port. • Addressed to or generated by the Access Point using the wireless port. Packets received and filtered are not shown. The average brightness of the LED indicates the level of activity on the wireless port. If the LED blinks in unison with the **Power/ System OK** and the **Bridge State** LEDs, the wireless port has a fault that prevents the Access Point from establishing a connection to the network.
Wired LAN Activity 	Lights when data is received on the Ethernet port. Data transmitted by the Access Point is not shown. Data traffic forwarded to the Ethernet port from the wireless port is not shown.

Table 7-2: RoamAbout Access Point 2000 LED Patterns

Wired LAN	Wireless LAN	Access Point Saturated	Bridge State	Power/ System OK	Meaning of LED Pattern
					
○	○	○	○	○	No power. Check the power connections.
○	●	●	○	●	Diagnostics failed. The Access Point automatically resets after one minute. If the pattern continues to display, contact technical support.
⊕	⊕	○	●	●	Normal operating mode.
⊕	⊕	○	○	●	• Access Point is waiting for the spanning tree. No action is required. **or** • Spanning tree detected a bridge loop and disconnected the port. Remove the loop.
⊕	⊕	⊕	●	●	Access Point is occasionally saturated. No action is required.
⊕	●	○	●	●	Cannot communicate with the wireless network. Verify that the PC Card is properly inserted.

Table 7-2: RoamAbout Access Point 2000 LED Patterns (Cont'd)

Wired LAN	Wireless LAN	Access Point Saturated	Bridge State	Power/ System OK	Meaning of LED Pattern
					
					Cannot communicate with the wired network. Verify that the Ethernet cable is properly connected.
					Cannot communicate with the wireless or wired network.

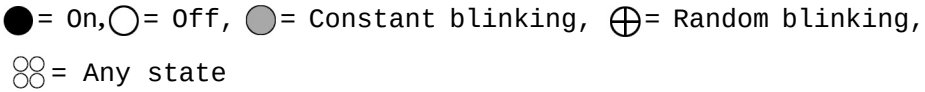


Table 7-3: Network Loading LED Patterns

Wired LAN	Wireless LAN	Access Point Saturated	Bridge State	Power/ System OK	Meaning of LED Pattern
					
					Downline loading image from load host.
					TFTP file not found or other TFTP error. (LEDs blink 10 times.)
					Upgrading Flash. (LEDs blink then turn on one at a time starting with Wireless LAN.) All LEDs, except Wired LAN, are on when the Flash upgrade is successful.
					Invalid load image. Wrong image, image too large, or CRC check error. (LEDs blink 10 times.)
					Unsuccessful Flash upgrade. (LEDs blink 10 times.)
					Firmware error or number of retries exceeded. (LEDs blink 10 times.)

● = On, ○ = Off, ◍ = Constant blinking, ⊕ = Random blinking, ⁘ = Any state

Access Point (Original) LEDs

Table 7-4 describes the LED functions. Table 7-5 describes the patterns, likely causes, and possible corrective actions. Table 7-6 describes the patterns during a firmware upgrade.

Table 7-4: RoamAbout Access Point (Original) LED Summary Table

Name	Description
Power OK	Lights (green) when the Access Point has power.
Module OK	Lights (green) when the Access Point passes its power-up self-test. The LED is off if the Access Point fails the test. If flashing, the Ethernet or wireless port (or both) has a fault, preventing connection to the network.
Wired LAN Activity	Indicates the status of the wired Ethernet segment. The LED lights (green) when packets are: • Received on the Ethernet port and forwarded to the wireless port. • Addressed to or generated by the Access Point using the Ethernet port. Packets received and filtered are not shown. Data traffic forwarded to the Ethernet port is not shown. The average brightness of the LED indicates the level of activity on the Ethernet port. If the LED is flashing together with the Bridge State LED, the Ethernet port has a fault that prevents the Access Point from establishing a connection to the network.
Bridge State 1	Lights (green) when the Access Point is forwarding packets.
Access Point Saturated 2	Lights (yellow) when the Access Point is saturated. Saturation occurs when the Access Point cannot forward packets from the Ethernet to the wireless side due to the lower throughput of the wireless network. The degree of LED brightness indicates the level of saturation. The LED dims (and eventually extinguishes) as the network congestion is processed.

Table 7-4: RoamAbout Access Point (Original) LED Summary Table (Cont'd)

Name	Description
Wireless LAN Activity 	The LED lights (green) when packets are: • Received on the wireless port and forwarded to the Ethernet port. • Addressed to or generated by the Access Point using the wireless port. Packets received and filtered are not shown. Data traffic forwarded to the wireless port is not shown. The average brightness of the LED indicates the level of activity on the wireless port. If the LED is flashing together with the Bridge State LED, the wireless port has a fault that prevents the Access Point from establishing a connection to the network.
Card Present 	Lights (green) when the PC Card is correctly installed at power-up.

Table 7-5: RoamAbout Access Point (Original) LED Patterns

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
○	○	○	○	○	○	○	No power. Check the power connections.
●	⁘	⁘	⁘	⁘	⁘	○	PC Card not inserted properly.
●	○	○	○	●	●	⁘	Diagnostics are running.
●	○	○	◍	◍	◍	⁘	Ethernet connection is not working or there is a hardware failure.
●	○	○	○	◍	○	○	Failure while initializing/ testing the memory.
●	●	⊕	●	○	⊕	●	Normal operating mode.
●	●	⊕	○	○	⊕	●	Waiting for the spanning tree. No action is required.

Table 7-5: RoamAbout Access Point (Original) LED Patterns (Cont'd)

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
●	●	⊕	●	⊕	⊕	●	Access Point is occasionally saturated due to excessive traffic. No action is required.
●	◍	⊕	○	◍	◍	⁘	PC Card is defective.
●	◍	◍	○	◍	⊕	●	Ethernet problem after power-up.
●	◍	⁘	⁘	◍	◍	●	Cannot communicate with the wireless network. Check the wireless parameters and PC Card.
●	◍	◍	⁘	◍	⁘	●	Cannot communicate with the wired network. Check the Ethernet cable.

● = On, ○ = Off, ◍ = Constant blinking, ⊕ = Random blinking, ⁘ = Any state

Table 7-6: Network Loading/Upline Dumping LED Patterns

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
●	●	○	⊕	○	●	◌◌	Waiting for downline load from load host
●	●	⊕	⊕	○	●	◌◌	Downline loading image from load host
●	●	⊕	⊕	○	○	◌◌	Firmware error detected while downline loading image from load host
●	●	⊕	⊕	○	⊕	◌◌	TFTP file not found
●	●	○	○	○	○	◌◌	Waiting for retry of TFTP load
●	●	○	●	●	●	◌◌	Upgrading Flash
●	●	○	◍	◍	●	◌◌	Flash upgrade successful
●	○	◍	○	○	●	◌◌	Invalid (wrong) load image

Table 7-6: Network Loading/Upline Dumping LED Patterns (Cont'd)

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
●	○	○	◍	○	●	⁘	Unsuccessful Flash upgrade
●	○	○	○	◍	●	⁘	Invalid load image: corrupted image
●	○	◍	◍	○	●	⁘	Invalid load image: image too large
●	○	◍	○	◍	●	⁘	TFTP error
●	○	◍	◍	◍	●	⁘	Firmware error or number of retries exceeded
●	○	◍	◍	◍	◍	⁘	Hardware error

Showing Counters

You can display the values of all the counters maintained by the Access Point and the client. This information can help you to monitor the performance of your wireless network or better understand a problem. Typically, this information is used by RoamAbout support personnel to help you diagnose a problem.

At a RoamAbout client, use the client utility to run the **Diagnose Card** option and select the **Card Statistics** tab.

To show a subset of the counters using the AP Manager:

1) Select the Access Point from the Managed List field.

2) Click the **Statistics** button.

To show all the counters using the console port:

1) Choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu.

2) Choose **Show Counters** from the next menu. The following example shows the screens associated with Show Counters. The first screen displays counters specific to the Access Point. The second screen displays counters from the RoamAbout PC Card. These counters are the same for RoamAbout PC Cards in an Access Point or in a client.

The following sections describe the counters shown by the RoamAbout PC Card.

```
Device uptime:    0 00:30:08       ETHERNET Port 0  WIRELESS Port 1
 Individually addressed bytes sent:              0             0
 Multicast bytes sent:                      111446        109406
 Individually addressed bytes received:          0             0
 Multicast bytes received:                       0             0
 Individually addressed frames sent:             0             0
 Multicast frames sent:                       1850          1820
 Individually addressed frames received:         0             0
 Multicast frames received:                      0             0
 Frames deferred:                                0             0
 Single collision:                               0             0
 Multiple collisions:                            0             0
 Excessive collisions:                           0             0
 Carrier check failed:                           0             0
 Transmit Frame too long:                        0             0
 Remote failure to defer:                        0             0
 Block check error:                              0             0
 Frame error:                                    0             0
 Receive Frame too long:                         0             0
 Data Overrun:                                   0             0
 System buffer unavailable:                      0             0
 Collision detect check fail:                    0             0
    Press RETURN to continue
```

```
Wireless PC card counters
    Individually addressed frames sent:              0
    Multicast frames sent:                         156
    Fragments sent:                               1665
    Individually addressed bytes sent:               0
    Multicast bytes sent:                        10380
    Deferred transmissions:                        126
    Single retry frames sent:                        0
    Multiple retry frames sent:                      0
    Transmit retry limit exceeded frames:            0
    Transmit frames discarded:                       0
    Individually addressed frames received:          0
    Multicast frames received:                       3
    Fragments received:                              3
    Individually addressed bytes received:           0
    Multicast bytes received:                      162
    Receive FCS errors:                            220
    Receive buffer not available:                    0
    Wrong station address on transmit:               0
    Receive WEP errors:                              0
    Receive message in message fragments:            0
    Receive message in bad msg fragments:            0
    Receive WEP ICV errors:                          0
    Receive WEP excluded:                            0
                    Press Return for Main Menu ...
```

Individually Addressed Frames Sent (TxUnicastFrames)

This counter displays the number of messages sent by the PC Card that are destined for another wireless device. In most LAN applications, it is normal behavior for this counter to have a high value and is continuously increasing (you can see it run). For example, this counter should increase rapidly when running the Link Test.

Multicast Frames Sent (TxMulticastFrames)

This counter displays the total number of messages sent by the PC Card as broadcast or multicast (destined at multiple other devices). In most LAN applications, multicast messages are regularly sent. Typically, this counter shows a lower value than the TxUnicastFrames counter.

Fragments Sent (TxFragments)

This counter displays the total number of messages or message fragments sent by the PC Card. The running rate of this counter is a general indication of activity at this wireless device. The number within this counter should be greater than the sum of TxUnicastFrames and TxMulticastFrames.

Individually Addressed Bytes Sent (TxUnicastOctets)

This counter displays the total number of bytes transmitted by the PC Card as part of unicast messages. Normal behavior for this counter shows a relatively high value that is increasing rapidly.

Multicast Bytes Sent (TxMulticastOctets)

This counter displays the total number of bytes transmitted by the PC Card as part of multicast messages. This value is expected to be a large number.

Deferred Transmissions (TxDeferredTransmissions)

This counter displays the number of times the PC Card deferred a transmission to avoid collisions with messages transmitted by other devices. Deferral is normal behavior for 802.11 devices. A relatively high value for this counter identifies a wireless network with lots of activity.

Signal Retry Frames Sent (TxSingleRetryFrames)

This counter displays the number of messages that were retransmitted a single time before being acknowledged by the receiving device. Retransmission is a normal behavior for the IEEE 802.11 protocol in order to recover quickly from lost messages. A relatively high value for this counter in comparison with the TxFragments counter identifies a wireless network that suffers from interference (noise) or a heavy load of wireless data traffic.

See also TxMultipleRetryFrames.

Multiple Retry Frames Sent (TxMultipleRetryFrames)

This counter displays the number of messages that were retransmitted multiple times before being acknowledged by the receiving device. Retransmission is a normal behavior for the IEEE 802.11 protocol in order to recover quickly from lost messages. A relatively high value for this counter in comparison with the TxFragments counter identifies a wireless network that suffers from interference (noise) or a heavy load of wireless data traffic.

High values for this counter result in lower throughput for the PC Card as the system falls back to the next lower transmit rate when more than one retransmission retry is needed to transfer a message.

See also TxSingleRetryFrames.

Transmit Retry Limit Exceeded Frames (TxRetryLimitExceeded)

This counter displays the number of messages that could not be delivered after the maximum number of retransmissions. You can use this counter together with TxDiscards to identify a wireless network that is overloaded due to severe interference or excessive load of wireless data traffic. The system drops such messages and depends on the higher communication protocols to recover from this lost message.

Transmit Frames Discarded (TxDiscards)

This counter displays the number messages that could not be transmitted due to congestion at the RoamAbout PC Card. In normal situations, the PC Card can temporarily store messages that are to be transmitted in an internal buffer. When this buffer is full, the PC Card discards any new messages until buffer space becomes available again. When this counter is relatively high, this may identify a wireless network with a heavy load of wireless data traffic.

Individually Addressed Frames Received (RxUnicastFrames)

This counter displays the number of messages sent by other devices to this PC Card. In most LAN applications, it is normal behavior for this counter to have a high value and is continuously increasing (you can see it run). For example, this counter should increase rapidly when running the Link Test.

Multicast Frames Received (RxMulticastFrames)

This counter displays the number of broadcast or multicast messages received by the device. In most LAN applications, it is normal behavior for this counter to have a value that is continuously increasing. Typically, this counter should display a value that is less than the RxUnicastFrames counter.

Fragments Received (RxFragments)

This counter displays the total number of messages or message fragments received by the PC Card. The running rate of this counter is a general indication of the amount of activity at the PC Card. This counter should be greater than the sum of RxUnicastFrames plus RxMulticastFrames.

Individually Addressed Bytes Received (RxUnicastOctets)

This counter displays the total number of bytes received by the PC Card as part of unicast messages. It is normal behavior for this counter to increase rapidly.

Multicast Bytes Received (RxMulticastOctets)

This counter displays the total number of bytes received by the PC Card as part of multicast messages. It is normal behavior for this counter to have a high value.

Receive FCS Errors (RxFCSErrors)

This counter displays the number of received messages or message parts that contained an erroneous value and had to be deleted. In the IEEE 802.11 protocol, such messages are recovered by the ACK (Acknowledgment) protocol and then retransmitted by the sending device.

A high value for this counter identifies a wireless network that suffers from interference or malfunctioning RoamAbout hardware. It is normal behavior for the RoamAbout PC Card to discard these messages.

Receive Buffer Not Available (RxDiscardsNoBuffer)

This counter displays the number of times an incoming message could not be received due to a shortage of receive buffers on the RoamAbout PC Card. A non-zero value identifies heavy data traffic for your RoamAbout PC Card; for example, when your PC Card is receiving large amounts of data.

Wrong Station Address on Transmit (TxDiscardsWrongSA)

This counter displays the number of times a message transmission was not done because a wrong MAC address was used by the protocol stack. A non-zero value indicates an error situation in the communication between your driver and the protocol stack.

Receive WEP Errors (RxDiscardsWEPUndecryptable)

This counter displays the number of times a received message was discarded because it could not be decrypted by your PC Card. This means that:

- Both devices have enabled encryption, but use keys that do not match.
- One of the devices does not support encryption or does not have encryption enabled.

Use RoamAbout Client Utility Link Test, Configuration Info tab, to see the configuration of the client and the Access Point or other client.

Receive Message in Message Fragments (RxMessageInMsgFragments)

This counter displays the number of times messages were received while another transmission was in progress. It is a measure of the amount of overlapped communication in your system. Zero values indicate low to moderate load of your network. Non-zero values identify a wireless medium that is being used simultaneously by multiple users.

Receive Message in Bad Message Fragments (RxMessageInBadMsgFragments)

This counter displays the number of times messages were received while a transmission elsewhere in the wireless network was in progress. This counter is expected to be zero. Non-zero-values indicate a heavily loaded system.

WEP ICV Error

This counter increments when encrypted data has an error that prevents it from being deciphered. A high number indicates a mismatched encryption key. A low number can be caused by drop bits which can be ignored.

WEP Excluded

This counter increments when this device sends unencrypted data to another device which rejects the data. If this is a client in an infrastructure network, this can be caused when the client has encryption disabled and the Access Point is configured to accept encrypted data only (DENY NON-ENCRYPTED DATA is enabled).

Displaying Error Logs

The Access Point can display error logs used by support personnel to analyze system faults. Up to four error log dumps can be stored, and the most recent dump is displayed first. There are two types of error logs: one for Access Point settings and one for wireless settings.

To display the Access Point settings error logs using the console port, choose **Dump Error Log** from the RoamAbout Access Point Installation Menu. This error log displays various information, including current reset count and PC Card present/not present.

To see the reset count from the AP Manager, select the Access Point in the **Managed List** field then click the **Reset** button. To display the wireless settings error logs in the AP Manager, click the **Troubleshooting** button.

To display the wireless settings error logs using the console port:

1) Choose **Module-Specific Options** from the RoamAbout Access Point Installation Menu.

2) Select **Dump Error Log** from the next menu.

The following example shows the screen associated with this option.

```
RoamAbout Access Point
==============================================================

       Product Specific  ERROR LOG
==============================================================



        Entry Number = 58
        Entry Type   = OTHER EXCEPTIONS
        Error Code   = FC000200  Vector offset = 0512
        Error Data   =

                0:0001E8C8   1:00000000   2:20100700   3:C3360200
                4:0000EEAC   5:00050400   6:0001CBAC   7:01001596

   Dump another Log entry [Y]/N ?
```

RoamAbout PC Card LED Activity in a Client

If you encounter difficulty using a RoamAbout client, the error may be related to various causes, such as:

- Out-of range situation, which prevents the PC Card from establishing a wireless connection with the network.
- Configuration mismatch, which prevents the PC Card from establishing a wireless connection with the (correct) network.
- Absence of or conflict of the RoamAbout Driver.
- A problem or conflict with the PC Card slot or ISA Adapter Card that prevents the PC Card from powering on.
- A conflict of the RoamAbout hardware with another device.

If you have a problem, you should first look at the PC Card LEDs (Figure 7-2). Table 7-7 describes the various modes of operation and associated LED activity. The table also includes a number of troubleshooting hints that may help you solve the problem.

Figure 7-2: RoamAbout PC Card

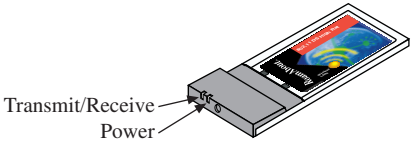


Table 7-7: RoamAbout PC Card LED Description

Power LED	Transmit /Receive LED	Description/Action
Continuous Green	Blinking	Standard operational mode: • Card is powered on. • Sensing/transmitting wireless data.
	Off	• Card is powered on. • A network connection was established but currently there is no wireless activity. This could be a normal situation. Also, the client may have moved out of the range of the wireless network. If in an ad-hoc network, no other clients may be available.
Flicker	Flicker	Power management mode: • Card is powered on. • Power management is enabled. • Flashes indicates that the card wakes up at regular intervals to check if there is wireless data addressed to your client.
Both LEDs blink once every 10 seconds		The PC Card has not established a connection with the wireless network. Actions: • Contact the LAN administrator to verify the wireless network name assigned to the wireless infrastructure network. Be aware that the wireless network name is case sensitive. • If using ANY as the wireless network name, verify that the RoamAbout Access Point does not have Secure Access enabled. • The client may not be within range of an Access Point or ad-hoc network.

Table 7-7: RoamAbout PC Card LED Description (Cont'd)

Power LED	Transmit /Receive LED	Description/Action
Off	Off	Card is not powered on. The cause may be: • No driver loaded or installed. • Card and driver mismatch that prevented the driver from loading. • Device conflict that prevented the driver from loading. Actions: • Verify that a driver has been installed. If not, install the driver. • Determine if there is a conflict with another device as described in the "Device Conflict on a Windows System" section on page 7-26. Typically, this only happens on a Windows NT system. • Verify the versions of the PC Card driver and Station firmware as described in the "Checking RoamAbout Product Version Numbers" section on page 6-12. • Consult the RoamAbout web site to see if newer versions are available and if so, upgrade both the firmware and driver to the latest available version.

Windows Does Not Detect the RoamAbout PC Card

If the RoamAbout PC Card was properly working at one time in the client, then the problem could be one of the following:

- The PC Card was removed and is no longer properly inserted. Reinsert the PC Card into the PC Card slot.
- The PC Card was removed and reinserted but the computer requires a reboot to recognize the PC Card. Restart the computer.
- The RoamAbout PC Card driver was improperly removed or corrupted. Remove the existing driver, as described in the "Removing the RoamAbout Miniport Driver" section on page 6-18. Then reinstall the driver.

Client Cannot Connect to the Network

This situation may occur in one of the following situations:

- The wireless network name is incorrect. Be aware that the wireless network name is case sensitive.
- If using **ANY** as the wireless network name or the field is blank, verify that the RoamAbout Access Point has disabled Secure Access.
- If the wireless network is using encryption, make sure that encryption is enabled and that the correct encryption key is entered in the correct key position (1, 2, 3, or 4).
- The Microsoft Windows workgroup name is incorrect. Follow the procedure in the next section to check the networking protocols.
- The driver is not loaded. Use the RoamAbout installation documentation that came with the PC Card to install the driver.
- There is a device conflict as described in the “Device Conflict on a Windows System” on page 7-26.
- The PC Card is defective.

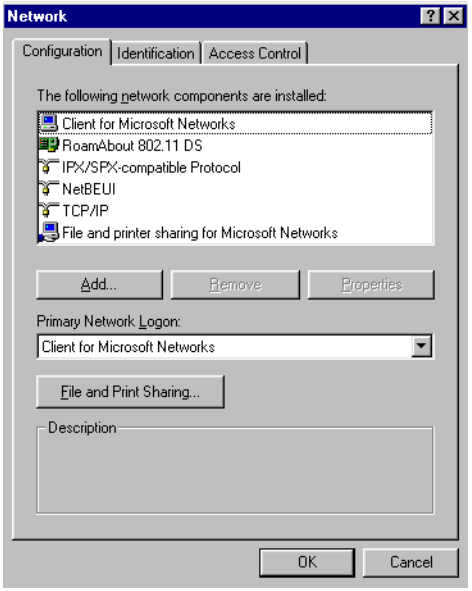
In an ad-hoc configuration, the RoamAbout Client Utility could show the other computers in the ad-hoc network but these computers are not shown in the Network Neighborhood. The most likely cause is that the computers are not using the same workgroup name.

Checking the Network Protocols on a Windows System

To verify that the client is configured for the correct type of networking and networking protocols:

1) From the Windows desktop, click **Start** then select **Settings→Control Panel**.

2) Double-click **Network**. The following dialog box is displayed:



3) Verify that the list of network components includes Client for Microsoft Networks and, optionally, Client for NetWare Networks.

4) If the item you want is available, click **Cancel** and go to the next step. If the items you require are missing, click **Add** and select **Add Client** to add the client software of the networking protocol that you want to install.

5) If the proper client software is installed but you do not see the required protocols, click **Add** then follow the on-line instructions.

If this is the first time that networking support is installed on your computer, Windows prompts you to enter the computer and workgroup names. These names are used to identify your computer on the Microsoft Network Neighborhood.

To enter the computer and workgroup names:

1) If the Network window shown below is not opened, click **Start,** select **Settings→Control Panel**, then double click **Network**.

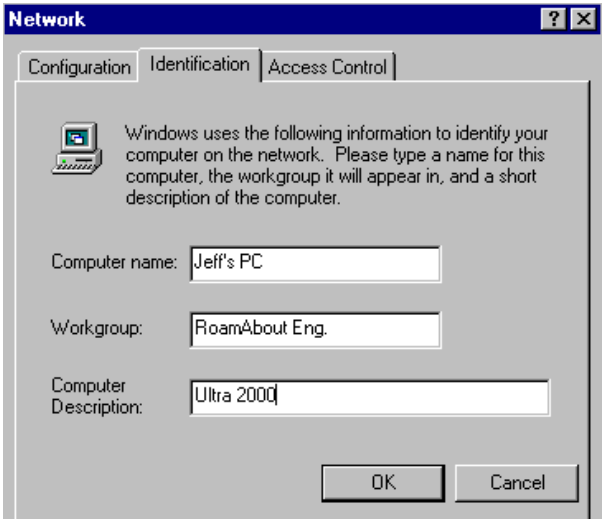
2) Click the **Identification** tab as shown below. The Windows NT version of this window is similar.

3) In the **Computer Name** field, enter a unique name for your computer.

4) In the **Workgroup** field, enter the name of your workgroup. The name must be the same for all computers in the wireless network.

5) Optionally, provide a description of the computer in the **Computer Description** field.

For more information about setting your Windows network properties, consult the Windows documentation or Windows on-line help.



Device Conflict on a Windows System

A device conflict under Windows NT may be related to the RoamAbout ISA card or PC Card. To detect which card is causing the conflict, use the Windows NT diagnostics. This problem can also appear on Windows 98 and the early version of Windows 95 (OSR0).

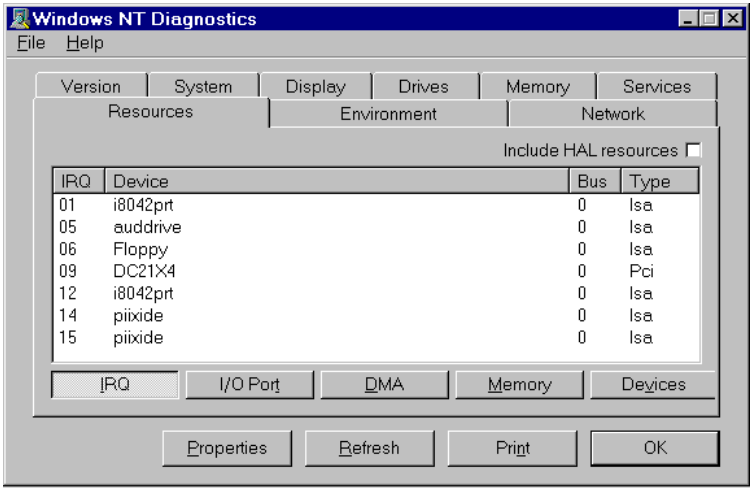
To help determine if a device conflict exists, check the following:

- If there is a conflicting I/O Base setting, the RoamAbout PC Card usually does not work at all and both LEDs are off.
- If there is a conflicting IRQ value, LEDs may flicker but you cannot connect to the network. In a number of cases, the card may succeed in connecting to a wireless device, but fail to connect to the network operating system.
- Another device in the computer no longer works properly.

Windows NT

To check the I/O port and IRQ values, perform the following:

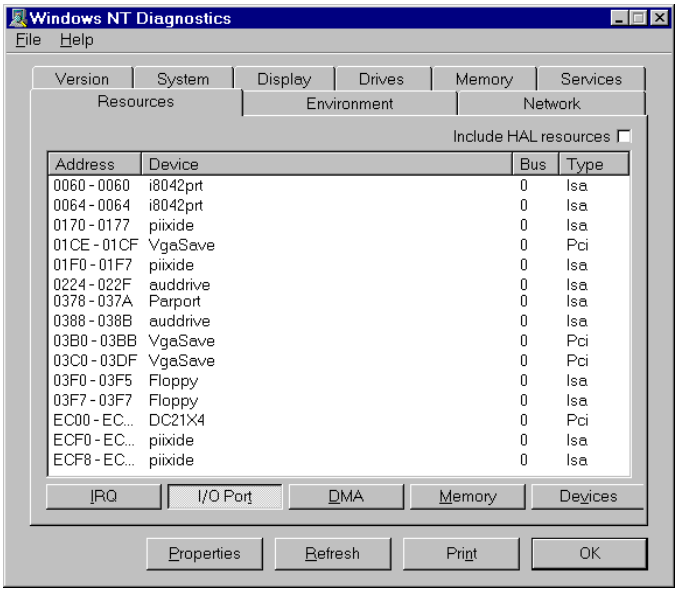
1) From the Taskbar, click **Start**. Select **Programs→Administrative Tools→Windows NT Diagnostics**.
2) Click the **Resources** tab to display the following window:



3) Click the **IRQ** button to display the Interrupt Request (IRQ) vectors currently in use by other devices in your computer.

If IRQ value 10 (default value for the PC Card) is not used, write down IRQ 10. If 10 is used, select a value not listed in the Windows NT Diagnostics window and write it down. Values include: IRQ 15, 12, 07, 05, 04, 03.

4) On the Resources screen, click **I/O Port** to display this window:



If I/O Port value 0400-043F is not used, write down I/O Port 0400-043F. If this value is used, select an unused value and write that down. I/O port values are in the range 0300 to FFC0 with increments of 40. Examples:

0300, 0340, 380, 03C0;
0400, 0440, 0480, 04C0;

.

.

FF00, FF40, FF80, FFC0.

If you need to select an address, start with the first unused address after 0400.

5) Open the driver properties, as described in the “Showing Current Client Settings” section on page 5-21, and click on the **Adapter** tab.

6) Enter the I/O Port and IRQ values that you wrote down.

It is possible that a conflict can still occur even after using the Windows NT Diagnostics program to determine unused I/O port addresses and IRQ values. This can happen when your computer has one or more devices and/or peripherals installed that claimed an I/O Base Address or IRQ value without notifying the Windows NT operating system. Therefore, the Windows NT Diagnostics program does not display these values as used.

If there is a device conflict, select alternative settings for I/O Base Address or IRQ values. You may need to try multiple values before resolving the problem. To isolate the problem, you should change only one parameter at a time. For example, try to resolve a possible conflict with the I/O Base Address. If that does not work, try to resolve a possible IRQ conflict.

If you know which device is conflicting with the PC Card, you have the option of changing that device's I/O address or IRQ instead of changing the RoamAbout PC Card or ISA card.

Depending on the computer, you might need to verify the settings of the BIOS which is loaded when you start your computer.

If the computer previously had a network card installed and the network card was running in 32-bit operation, you may need to set the BIOS to PCIC - 16 bit. You may also need to disable the network card in the Control Panel - Devices.

Windows 95 or 98

To check the I/O and IRQ for a Windows 95 and 98 system:

1) From the Taskbar, click **Start** then select **Settings→Control Panel**.
2) Double-click the **System** icon.
3) Select the **Device Manager** tab.
4) Open (click the + sign) **Network adapters**, select **RoamAbout 802.11 DS**, then click the **Properties** button.
5) Click the **Resources** tab to see the I/O range and IRQ setting.

You can also select a different device and click **Properties** to display its resource settings.

Should you change the I/O address or IRQ value, only change one value at the time to isolate a potential conflict without unintentionally creating another one.

Depending on the computer, you might need to verify the settings of the BIOS which is loaded when you start your computer.

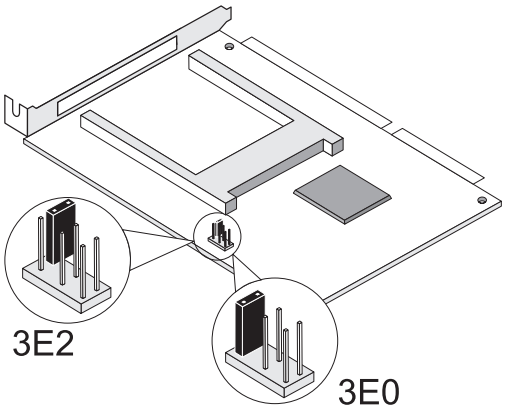
Changing the ISA Adapter Address

If the device conflict is related to the I/O port address of the ISA card, you can change the ISA address by changing the jumper setting on the ISA card (Figure 7-3). The ISA card supports two I/O addresses:

- 3E0-3E1 (factory-set default)
- 3E2-3E3

To change the jumper setting, open your computer according to the documentation that was shipped with your computer and follow the safety precautions described in the RoamAbout installation documentation that came with the ISA adapter.

Figure 7-3: ISA Card I/O Address Strapping



Setting and Removing SNMP Trap Addresses

To have the Access Point send SNMP traps, you need to enter the IP address of the device where the trap is to be sent. A trap is a defined event or condition detected by the RoamAbout Access Point SNMP agent. The Access Point sends an SNMP trap when any of the following events occur:

- Access Point is powered on (coldstart trap).
- Ethernet network connection is established (network link up trap).
- User tried to communicate with the Access Point using an incorrect SNMP community string (authentication trap).

To enter an SNMP trap address using the console port:

1) Choose **Add SNMP Trap Addresses** from the RoamAbout Access Point Installation Menu.

2) Enter the IP address of the system that you want to receive the SNMP traps.

Note: If you do not want to change the existing value, press <Enter> to go back to the previous menu.

To delete an existing trap address using the console port:

1) Choose **Delete SNMP Trap Addresses** from the RoamAbout Access Point Installation Menu.

2) Enter the IP address of the system that you no longer want to send SNMP traps.

Note: If you do not want to change the existing value, press <Enter> to go back to the previous menu.

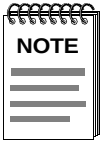
Setting Upline Dump

The Upline Dump mode is disabled by default. This option allows you to specify whether the Access Point uploads diagnostic information bout itself in the event of a crash. This option should be DISABLED unless a support representative tells you otherwise.

The Upline Dump setting is available by clicking the Operating Modes button in the AP Manager, or selecting the **Module-Specific Options** in the console port RoamAbout Access Point Installation Menu.

When enabled, you can select one of the following:

- Use the BootP Server to discover the IP address of the destination TFTP server and the destination directory on that server.
- Upload the image to the specified TFTP server IP address and a destination directory.



You must use the path structure dictated by your operating system.

Depending on the dump host, you may need to create a writable file to accept the dump. The file name should be apxxxxxx.dmp, where xxxxxx is the last 6 digits of the Access Point's wired MAC address.

Appendix A

RoamAbout Product Specifications

This appendix lists the various specifications of the RoamAbout products.

PC Card and ISA Adapter Physical Specifications

Form factor		PC card: PC card type-II extended ISA card: Half-size ISA adapter card
Dimension: PC Card	(LxWxH)	118 x 54 x 8 mm (4.72 x 2.16 x 0.32 in)
Dimension: ISA Adapter	(LxWxH)	170 x 100 x 15 mm[1] (6.8 x 4.0 x 0.6 in)
Weight: PC Card		45 gram (1.58 oz)
Weight: ISA Adapter		110 gram (3.85 oz)
Temperature & humidity		
Operation	0° to 55° C[2] (32° to 131° F)	Maximum humidity 95%
Transit	-20° to 70° C (-4° to 158° F)	15 to 95% (no condensation allowed)
Storage	-10° to 60° C (14° to 140° F)	10 to 90% (no condensation allowed)

[1] As measured without the standard mounting plate for ISA boards.

[2] Although the card may still operate in the range of -20° to 70° C, operation outside the range 0° to 55° C may no longer be according to the RoamAbout or IEEE specifications.

PC Card Power Characteristics

Doze mode	9 mA
Receive mode	185 mA
Transmit mode	285 mA
Power supply	5 V

PC Card Networking Characteristics

Compatibility	IEEE 802.11B standard for wireless LANs (DSSS)
Network operating system	Novell client 3.x & 4.x Microsoft Windows Networking
Host operating system	Microsoft Windows 95, Windows 98, and Windows NT (NDIS Miniport driver)
	Windows 2000 (NDIS 5 driver)
	MS-DOS & Microsoft Windows 3.x: • DOS ODI driver • Packet driver
	Apple Macintosh (RoamAbout driver)
Media access protocol	CSMA/CA (collision avoidance) with acknowledgment (ACK)

PC Card Radio Characteristics

Radio characteristics of RoamAbout PC Cards may vary according to the country where the product was purchased (see Table A-1). If you plan to connect a RoamAbout Access Point to an outdoor antenna installation, additional regulations may apply. You use a different RoamAbout PC Card when connecting to the RoamAbout outdoor 14 dBi directional antenna in countries that adhere to ETSI regulations (see Table A-2).

Table A-1: Radio Characteristics

R-F frequency band	**2.4 GHz** (2400-2483.5 MHz)	
Number of selectable sub-channels	North America (FCC)	11
	Europe (ETSI)	13
	France (FR)	4
	Japan (JP)	14
	Other countries that adhere to:[1] FCC ETSI	 11 13
Modulation technique	Direct sequence spread spectrum (DQPSK, CCK, DBPSK)	
Spreading	11-chip barker sequence	
Bit error rate	Better than 10^{-5}	
Nominal Output Power	15 dBm	

Range (100 bytes user data)	**11 Mbit/s**	**5.5 Mbit/s**	**2 Mbit/s**	**1 Mbit/s**
Open environment	160 m (525 feet)	270 m (885 feet)	400 m (1300 feet)	550 m (1750 feet)
Semi-open environment	50 m (165 feet)	70 m (230 feet)	90 m (300 feet)	115 m (375 feet)
Receiver sensitivity	-82 dBm	-87 dBm	-91 dBm	-94 dBm

[1] Consult your authorized RoamAbout reseller sales office for information about the radio regulations that apply in your country.

Signal strength can be affected by closeness to metal surfaces and solid high-density materials. The ranges listed above provide a general guideline and may vary according to the actual physical environment where the product is used.

- In open environments, there are no physical obstructions between antennas.
- In semi-open environments, work space is divided by shoulder-height, hollow wall elements; antennas are at desktop level.

Table A-2: Radio Characteristics (For Outdoor Antenna Use)

R-F frequency band	**2.4 GHz** (2400-2500 MHz)	
Number of selectable sub-channels	Europe (ETSI)	13
	France (FR)	4
	Japan (JP)	14
	Other countries that adhere to ETSI[1]	13
Modulation technique	Direct sequence spread spectrum (DQPSK, CCK, DBPSK)	
Spreading	11-chip barker sequence	
Bit error rate	Better than 10^{-5}	
Nominal Output Power	8 dBm	
Range	Consult the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide*.	

[1] This variation of the RoamAbout PC Card is not available in FCC regulated countries. This PC Card is used when connecting to an outdoor 14 dBi directional antenna in countries that adhere to radio regulations as defined by the ETSI.

Supported Frequency Sub-Bands

The RoamAbout PC Card supports a number of factory-programmed channels. The number of available frequencies is subject to local radio regulations as defined by local authorities.

In RoamAbout infrastructure environments, the RoamAbout PC Card automatically starts operation at the frequency channel that is used by the RoamAbout Access Point. This frequency is controlled by the LAN administrator who sets the RoamAbout Access Point configuration. Table A-3 shows the factory-set default values, which are printed in bold.

Table A-3: IEEE 802.11 RoamAbout Channel Sets

Frequency range	**2400-2500 MHz**			
Channel ID	**FCC**	**ETSI**	**France**	**Japan**
1	2412	2412	-	2412
2	2417	2417	-	2417
3	**2422**	**2422**	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11	2462	2462	**2462**	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14	-	-	-	**2484**

Range Extender Antenna Specifications

You can connect the RoamAbout Range Extender antenna to a RoamAbout PC Card in either an Access Point or wireless client. Use the Range Extender antenna to ensure optimal transmission and reception quality for situations where the PC Card integrated antennas are shielded.

Table A-4 provides the specifications for the Range Extender antenna.

Table A-4: Range Extender Antenna Specifications

Mechanical	
Size (length x width x height)	18.5 x 2.5 x 0.9 cm (7.2 x 1 x 0.35 in)
Cable Length	150 cm (58.5 in)
Insertion Loss @ 2.4 GHz	1.25 dBm
Connector	RoamAbout special, snap-on type
Electrical	
Frequency Range	2400-2500 MHz
VSWR (Voltage Standing Wave Ratio)	Less than 2:1
Nominal Impedance	50 Ohms
Gain (vertical position)	2-3 dBi
Gain (horizontal position)	-2 dBi
Polarization (vertical position)	Vertical
Polarization (horizontal position)	Not applicable

Vehicle-Mount Antenna Specifications

The RoamAbout Vehicle-Mount antenna can be mounted on vehicles, such as fork-lift trucks, that need continuous access to networked data, whether inside or outside of the building. Table A-5 provides the specifications for the Vehicle-Mount antenna.

Table A-5: Vehicle Mount Antenna Specifications

Mechanical	
Cable Length	250 cm (8 feet)
Insertion Loss @ 2.4 GHz	3.3 dB
Connectors	
FCC Countries	Reverse Polarity-N (Female)
ETSI Countries	Standard-N (Male)
France	Standard-N (Male)
Japan	Standard-N (Male)
Electrical	
Frequency Range	2400-2438 MHz
VSWR (Voltage Standing Wave Ratio)	1.5:1
Nominal Impedance	50 Ohms
Gain	5 dBi
Half-Power Beamwidth	NA
Polarization	Vertical
Power Handling	100 Watts
Antenna Environment	
Operating Temperature	- 40°C (-40°F) to +60°C (140°F)
Relative Humidity Range	0-100%
Wind/survival (mph)	194 km/h (120 mph)[1]
Wind rating	129 km/h (80 mph)
Wind load	202 km/h (125 mph)

[1] 104 km/h (65 mph) with 1.25 cm (0.5 in) ice.

Glossary

Access Point

A 2-port bridge that connects a wireless LAN to a wired Ethernet LAN.

Ad-Hoc network

A group of wireless stations that participate in wireless communication without connection to a **wireless infrastructure network**. An ad-hoc network does not include Access Points.

Ad-hoc networks are also referred to as peer-to-peer networks.

Beacon

A message that is transmitted at regular intervals by the RoamAbout Access Point to all wireless clients in the wireless network.

Beacons are used to maintain and optimize communications by helping mobile clients to automatically connect to the Access Point that provides the best communications quality.

Broadcast Message

A data message that is transmitted by one wireless device to all devices in the wireless network.

Broadcast storm

An occurrence where a large number of broadcast messages are sent through the network, usually degrading network performance.

Cell

A single Access Point and its wireless clients within a wireless infrastructure network containing multiple Access Points.

Channel (Frequency)

The center radio frequency that the wireless device uses to transmit.

The RoamAbout PC Card can support up to 13 radio frequency channels as defined in the IEEE 802.11 Standard. The number of available channels for your PC Card is subject to radio regulations that apply in your country. In most countries, these radio regulations adhere to either the FCC or ETSI Standards.

Directional Antenna

An antenna that radiates RF signals in a specific direction. A directional antenna typically has a higher gain and can cover a greater distance than an omni-directional antenna. A 14 dBi Yagi directional antenna is available as an option for the RoamAbout Access Point.

ETSI

European Telecommunications Standards Institute. Standards body that governs use of radio frequencies, mostly for European countries.

FCC

Federal Communications Commission. Standards body that governs use of radio frequencies, mostly for North America.

IEEE 802.11 Standard

The Institute of Electrical & Electronics Engineers, Inc. (IEEE) is an organization that develops standards for electrical and electronic equipment. IEEE 802.xx Standards define the access technologies for local and metropolitan area networks. The IEEE 802.11 Standard is an interoperability standard for wireless LAN devices that identifies three major distribution systems for wireless data communication:

- Direct Sequence Spread Spectrum (DSSS) Radio Technology
- Frequency Hopping Spread Spectrum (FHSS) Radio Technology
- Infrared Technology

IEEE 802.11 compliant networking products based on the same type of distribution system are interoperable with one another regardless of the device's manufacturer. RoamAbout 802.11 DS products are compliant with the IEEE 802.11 Standard for wireless LAN devices that use the Direct Sequence Spread Spectrum (DSSS) Radio Technology.

ISA adapter

An option for the RoamAbout PC Card for computers that do not have a PCMCIA slot. The ISA adapter installs into a computer's ISA bus and provides a PCMCIA slot for the PC Card.

Endpoint Bridge Mode

An Access Point mode that allows two Access Points to communicate, effectively connecting two wired LANs through a wireless link.

Multipoint Bridge Mode

An Access Point mode that allows up to seven Access Points to communicate, effectively connecting wired LANs through a wireless link.

Multicast Message

A data message that is transmitted by one wireless device to multiple devices in the wireless network. Unlike broadcast messages, multicast messages do not always include all devices in the network.

Omni-Directional Antenna

An antenna that radiates RF signals in all directions. An omni-directional antenna typically has a lower gain and covers less distance than a directional antenna. A 7 dBi omni-directional antenna is available as an option for the RoamAbout Access Point.

PC Card

A network card that installs in an Access Point or wireless client to provide wireless connectivity in a LAN environment.

PCMCIA

The Personal Computer Memory Card International Association (PCMCIA) is the standards body for the type of PC Card used with the RoamAbout products.

Range Extender Antenna

An indoor antenna that extends the coverage area of a RoamAbout wireless device.

RoamAbout Access Point Manager

Software used to manage and configure one or more Access Points. The software is installed on a Windows computer that connects to the Access Point via a wired LAN or wireless LAN.

roaming

The ability for a wireless client to move from one cell to another in a wireless network without losing the network connection.

As the client moves between different wireless cells, the RoamAbout PC Card keeps track of the quality of the radio connection with the Access Points. As the client moves away from its Access Point and the signal level decreases, the RoamAbout PC Card automatically connects to another Access Point in the same network that has a stronger signal level.

SNR

The Signal to Noise Ratio (SNR) is a dynamic indicator that indicates the relative strength of the radio signal (signal level) versus the radio interference (noise level) in the radio signal path.

Unicast Message

A data message that is transmitted by one wireless device to another wireless device.

Vehicle-Mount Antenna

A 5 dBi omni-directional antenna that connects to a PC Card in a client to extend the coverage area. The Vehicle-Mount antenna is designed to be mounted on vehicles, such as fork-lift trucks that need continuous access to networked data while inside or outside of the warehouse.

WEP

Wired Equivalent Privacy. Used to encrypt data transmitted via the wireless medium.

wireless client

A computer such as a PC, laptop, or notebook, that uses the PC card for wireless LAN connectivity. A wireless client is also referred to as a station.

wireless infrastructure network

A wireless network that consists of wireless clients connected by one or more Access Points to a wired Ethernet LAN.

wireless network

A collection of end-user systems connected together using a medium such as radio frequency or infrared technology. The RoamAbout products use radio frequencies.

wireless relay

When enabled, the multipoint Access Point relays messages from one Access Point to another. When disabled, each of the Access Points in the LAN-to-LAN multipoint configuration can only communicate with the multipoint Access Point and its wired LAN.

Index