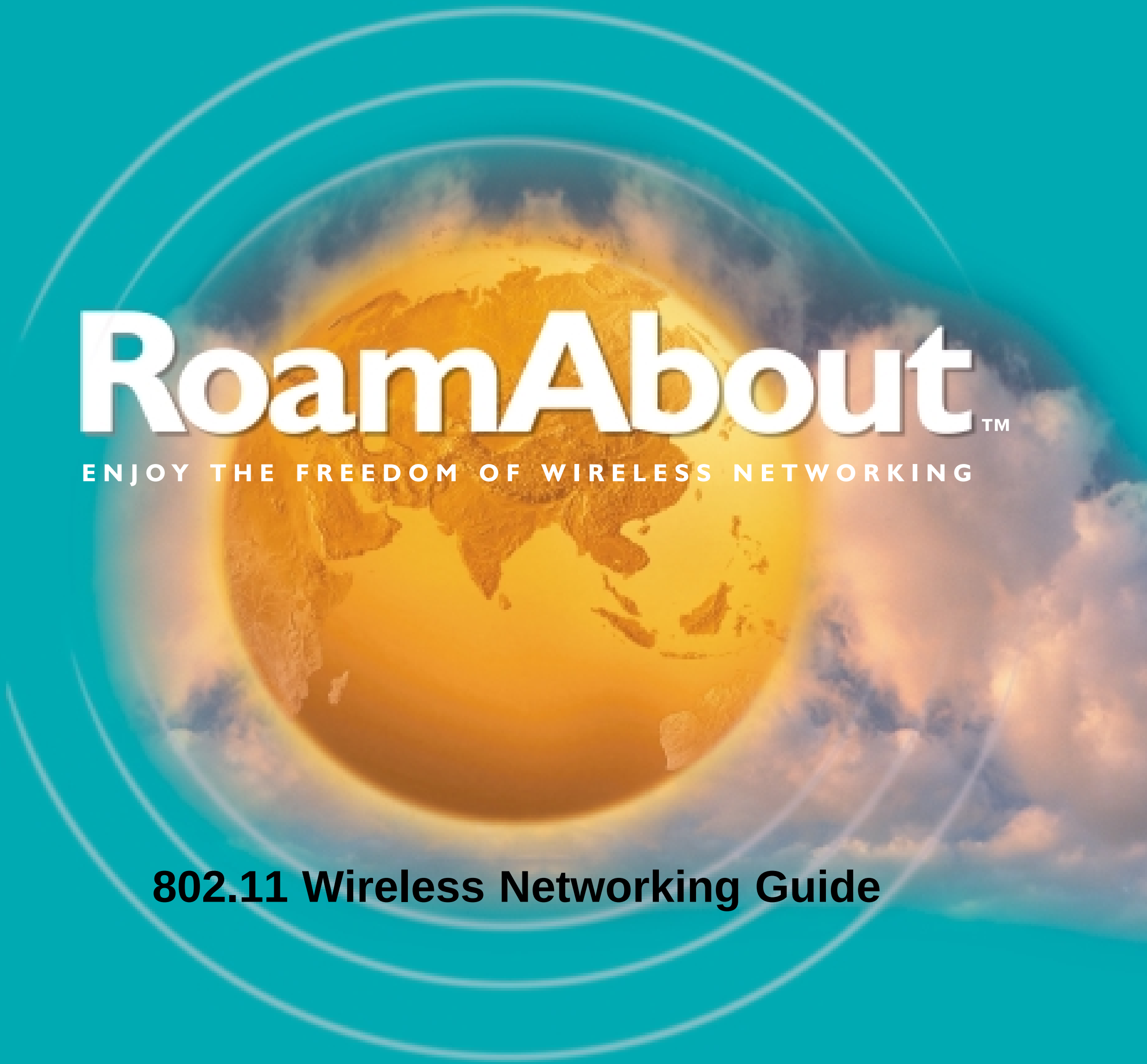


RoamAbout™

ENJOY THE FREEDOM OF WIRELESS NETWORKING

802.11 Wireless Networking Guide

ENTERASYS NETWORKS™

ENTERASYS.COM

P/N 9034042-08

NOTICE

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

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

IN NO EVENT SHALL ENTERASYS NETWORKS 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 DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
500 Spaulding Turnpike
Portsmouth, NH 03801

Part Number: 9034042-08

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

Enterasys, Enterasys Networks, RoamAbout, and the RoamAbout logo are trademarks of Enterasys Networks, Inc.

Apple, the Apple logo, Macintosh, and PowerBook are trademarks or registered trademarks of Apple Computer, Inc.

IPX/SPX is a trademark of Novell, Inc.

LINUX is a trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Novell and NetWare are registered trademarks of Novell, Inc.

PC Card is a trademark of PCMCIA.

All other trademarks and registered trademarks are the property of their respective holders.

Contents

Preface

1 Wireless Network Configurations

2 Understanding Wireless Network Characteristics

3 Designing and Implementing a Wireless Network

4 Wireless Network Tools

5 Configuring the Wireless Network

6 Maintaining the Wireless Network

7 Problem Solving

A PC Card Information

Preface

A RoamAbout wireless network consists of RoamAbout wireless products, such as the RoamAbout R2 Wireless Access Platform, RoamAbout Access Point 2000, RoamAbout PC Card, 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.

***NOTE**: AP refers to the Access Point and the RoamAbout R2 unless otherwise specified in this document.*

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

You can download the documentation, drivers, and utilities from the RoamAbout Wireless web site. Check the RoamAbout Wireless web site regularly for product upgrades:

http://www.enterasys.com/wireless

Component	Information Location
RoamAbout AP Manager	*RoamAbout 802.11 Wireless Networking Guide* and online help
RoamAbout R2 Wireless Access Platform	*RoamAbout R2 Wireless Access Platform Hardware Installation Guide* and online help
RoamAbout Access Point 2000	*RoamAbout Access Point 2000 Hardware Installation Guide* and online help
RoamAbout 802.11 PC Card	*RoamAbout 802.11 PC Card Drivers and Utilities Client CD-ROM Kit* *RoamAbout 802.11 PC Card Installation Guide*
RoamAbout 802.11 PC Card Drivers	*RoamAbout 802.11 PC Card Drivers and Utilities CD-ROM Kit* *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* and online help
RoamAbout Client Utility	*RoamAbout 802.11 PC Card Drivers and Utilities CD-ROM Kit* *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* and online help
RoamAbout Outdoor Solution	*RoamAbout Outdoor Antenna Site Preparation and Installation Guide*
RoamAbout ISA Adapter Card	*RoamAbout ISA Adapter Installation*
RoamAbout PCI Adapter Card	*RoamAbout PCI Adapter Installation*

Document Conventions

The following icons are used in this document:

Icon	Meaning
⚠	***CAUTION:*** *Contains information essential to avoid personal injury or damage to the equipment.*
NOTE	***NOTE:*** *Calls the reader's attention to any item of information that may be of special importance.*

Getting Help

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

World Wide Web:	http://www.enterasys.com/wireless
Phone:	North America: (603) 332-9400 Europe: 353 61 701 910 Asia: +800 8827-2878
Internet mail:	support@enterasys.com

To send comments or suggestions concerning this document, contact the Enterasys Networks Technical Writing Department via the following e-mail address: **TechWriting@enterasys.com**

Make sure you include the document Part Number in the e-mail message.

Before calling Enterasys Networks, please have the following information ready:

- Your Enterasys Networks 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 Enterasys Networks products in the network
- A description of your network environment (for example, layout, cable type)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, have you returned the device before, is this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Chapter 1

Wireless Network Configurations

There are three basic RoamAbout wireless network configurations:

- One or more APs 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 APs 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.

In This Chapter

Information in this chapter is presented as follows:

RoamAbout AP

This guide addresses the different RoamAbout AP hardware platforms: RoamAbout Access Point (sometimes referred to as Classic), RoamAbout Access Point 2000, and RoamAbout R2 Wireless Access Platform. Unless otherwise specified, **AP** refers to all the RoamAbout AP platforms.

The RoamAbout Access Point Classic is no longer available; however, a number of the Access Point 2000 reference information and procedures apply to the Classic platform.

The RoamAbout Access Point 2000 is a wired to wireless 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.

The RoamAbout R2 is an expandable wireless access platform designed to support existing, and future, radio technologies and networking requirements.

The RoamAbout AP provides the following basic bridging services. See Chapter 2 for descriptions of wireless LAN, security and management features.

- **Store-and-forward capability**

  The AP 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 AP isolates traffic that does not need to be forwarded to, or should not be allowed on, other LANs. This action reduces the total data traffic on an extended LAN and thus increases bandwidth efficiency.

- **Data Link layer relay**

  The AP operates at the Data Link layer of the Open System Interconnection (OSI) model. Operation at this layer makes the AP 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 AP is operating. This reverse learning of the address and port association allows automatic network configuration without prior downline loading of configuration data to the AP. 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 AP communicates with wireless clients. The AP only forwards packets to multicast addresses, broadcast addresses, and known addresses on the wireless LAN.

  The RoamAbout Access Point 2000 learns addresses only from the wireless side of the network. The default Aging Timer interval is 32 minutes.

  The RoamAbout R2 learns addresses from both the wired and wireless side. The default Aging Timer interval is approximately 7 minutes.

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

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

  In this mode, the AP 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 APs are configured as dedicated wireless links between LANs in a Point-to-Multipoint configuration. One AP must be designated as the Central AP. The Central AP can communicate with up to six other APs configured as Endpoints.

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

  NOTE*: You must purchase a valid activation key to enable Multipoint bridge mode. Contact your Enterasys Representative.*

Refer to the *Release Notes* that shipped with your AP for a complete list of product features.

RoamAbout PC Card

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 fits into any PC card type II slot and includes the following features:

- The ability to support desktop PCs, via one of the following adapters:
  - 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.
  - RoamAbout PCI Adapter Card option, which allows installation into computers that do not have a PC Card slot or an ISA bus slot. The PCI Adapter works with Microsoft Windows PC99-compliant PCs (PCI-slot-only PCs) that have BIOS-supported PCI 2.2 or higher.
- An 802.11 DS compliant radio.
- The ability to communicate with 802.11 DS compliant APs or other 802.11 clients.
- The RoamAbout Client Utility, which allows you to monitor the quality of wireless communication.
- Support for Windows 95, Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP, MS-DOS, Windows 3.x, Windows CE, Linux, and Apple PowerBook computers. Refer to the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* for more information.
- 802.11 power management.
- Wired Equivalent Privacy (WEP) security.
- Roaming, where the client can move from one AP 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 AP.
- The RoamAbout PC Card is also the means by which a RoamAbout AP communicates with a wireless network. This manual considers an AP and its installed PC Card(s) as one unit.

Operating System Support

You can have clients with various operating systems in the same wireless network. Refer to the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* for setup and installation information. For the latest version of the RoamAbout drivers, see the RoamAbout web site: **http://www.enterasys.com/wireless**.

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.

Wireless Infrastructure Network

In a wireless infrastructure network, wireless clients communicate with an AP to connect to a wired LAN. A RoamAbout wireless infrastructure network can support clients with various operating systems.

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

Single AP

A single AP supports a single wireless infrastructure network. Each wireless client must communicate with the AP to connect to the wired network.

NOTE

***NOTE**: The RoamAbout R2 with the Mezzanine option can support two separate wireless infrastructure networks. Refer to* **"RoamAbout R2 Configuration Examples" on page 1-13**.

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

Multiple APs

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

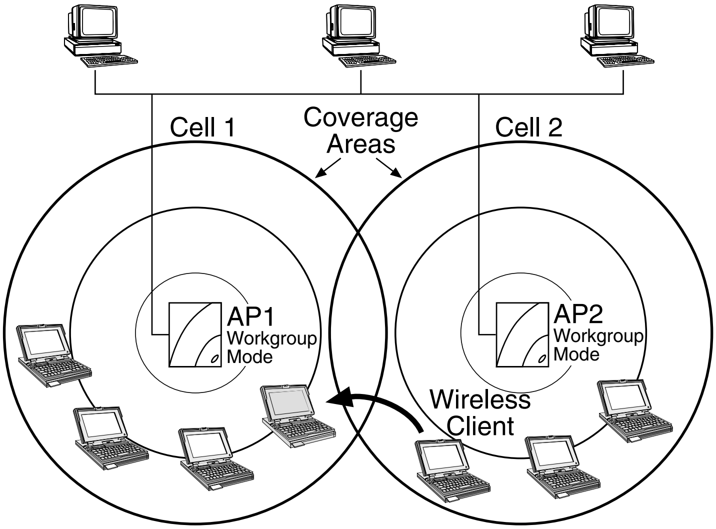
NOTE

***NOTE**: The RoamAbout R2 with the Mezzanine option can effectively be configured as two APs supporting the same wireless infrastructure network. Refer to* **"RoamAbout R2 Configuration Examples" on page 1-13**.

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

Figure 1-1 shows two APs 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 AP2 to AP1 while maintaining LAN connectivity. The capability of moving from one AP 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 AP using the same Wireless Network Name is providing a better quality signal. The client then automatically switches to the other AP. If the other AP 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 AP in the specified wireless network that provides the best communications quality. APs 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 AP that provides the best communications quality. Be aware that if there are multiple wireless networks, the client could connect to an AP that is not in the network you want to join.

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

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 APs to communicate with each other. This is called a LAN-to-LAN configuration.

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

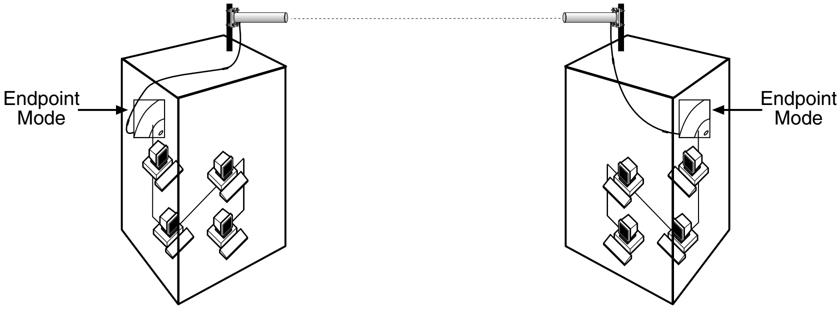
- Point-to-Point, using the LAN-to-LAN Endpoint Bridge mode, which connects two wired networks.
- Point-to-Multipoint, using the LAN-to-LAN Multipoint Bridge mode, which can connect multiple wired networks.

Typically, the APs are configured with outdoor antennas. If you use an outdoor antenna, you should have a professional antenna installation company perform the installation. Contact your Enterasys sales representative or visit the RoamAbout web site, www.enterasys.com/wireless, for more information about the outdoor antenna kits.

Point-to-Point

Figure 1-2 shows two APs, 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 APs use a directional antenna. You can also configure the APs 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 APs is configured as a Multipoint AP, called the Central AP. The Central AP can communicate directly with up to six APs. The six APs are configured as Endpoints, which can only communicate directly to the Central AP. The Central AP allows the Endpoint APs to communicate with each other through the Central AP.

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

NOTE

NOTE*: The RoamAbout R2 Mezzanine option (slot 2) does not support LAN-to-LAN Multipoint. This means that an R2 can use its Slot 2 radio to participate as an Endpoint AP in a Point-to-Multipoint configuration, but cannot use its Slot 2 radio to act as a Central AP.*

Configuration Examples

Figure 1-3 provides an example of a Central AP with six Endpoint APs. The Endpoint APs can only communicate with the Central AP and not directly with each other. Therefore, the Central AP should be connected to the main wired LAN.

Figure 1-3: Point-to-Multipoint Configuration

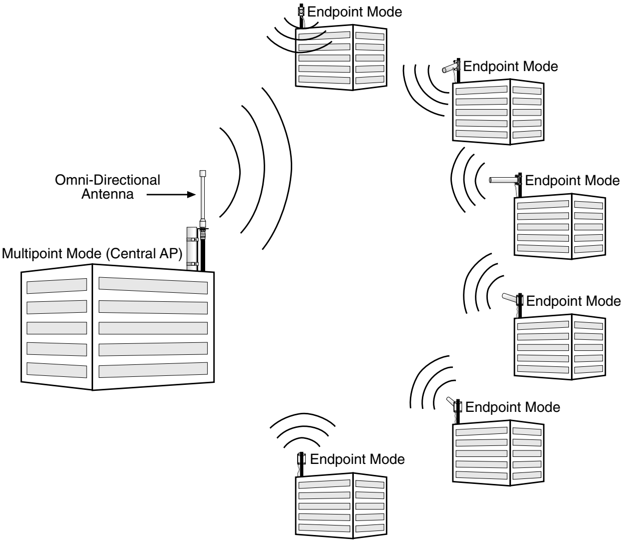
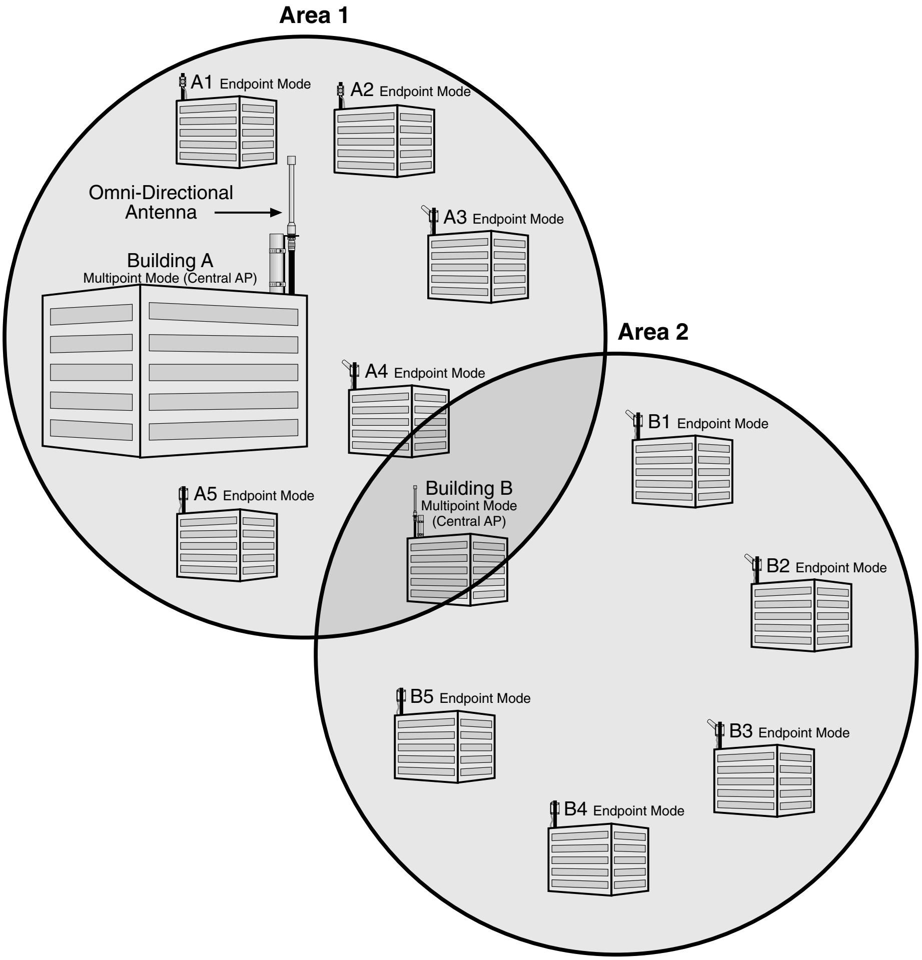


Figure 1-4 provides an example of two Central APs in the same Point-to-Multipoint configuration. In this configuration, six APs are configured to communicate with the same Central AP. You can configure one or more of those six APs as a Central AP to communicate with up to five additional APs. If using an Access Point 2000, this configuration requires the Wireless Relay parameter to be enabled.

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



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

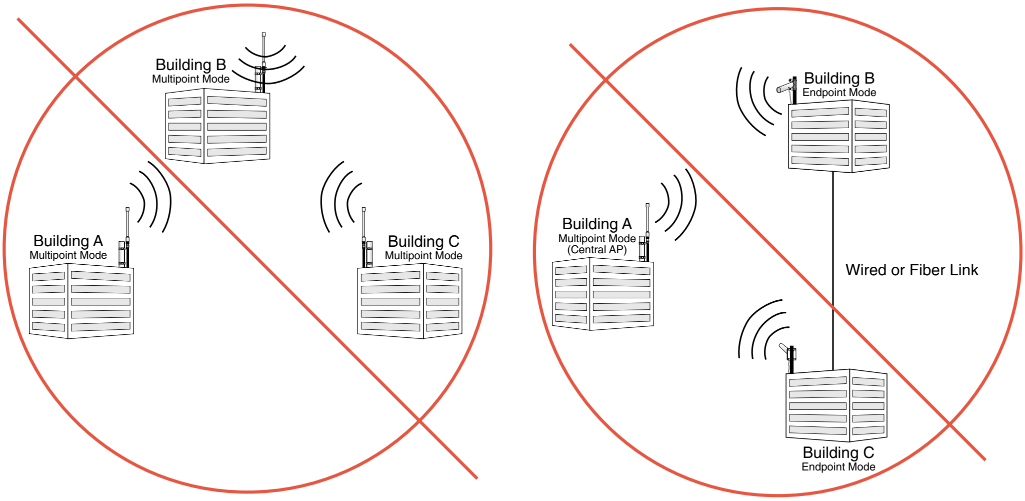
To avoid bridging problems, do not configure an AP as an Endpoint for more than one Central AP. In **Figure 1-4**, you would not configure Building B1 as an Endpoint to communicate directly to Building A.

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 AP Spanning Tree function corrects this type of problem by shutting down the port 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



RoamAbout R2 Configuration Examples

This section provides configuration examples using the RoamAbout R2 (with the two-slot option).

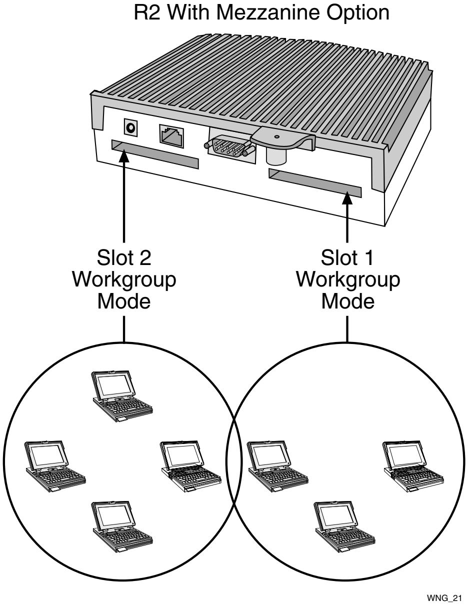
Restrictions

- The RoamAbout R2 slot 2 does not support LAN-to-LAN Multipoint.
- If two 802.11b PC Cards are installed in the RoamAbout R2 Wireless Access Platform, one of the PC Cards must be connected to the Range Extender Antenna to prevent radio interference between the two cards. The antenna must be placed at least two feet away from the RoamAbout R2.
- The 802.11 PC Cards must be at least 5 channels apart from each other.

Workgroup Mode (both slots) Example

Figure 1-6 shows a RoamAbout R2 with both slots configured in Workgroup mode.

Figure 1-6: Workgroup Configuration

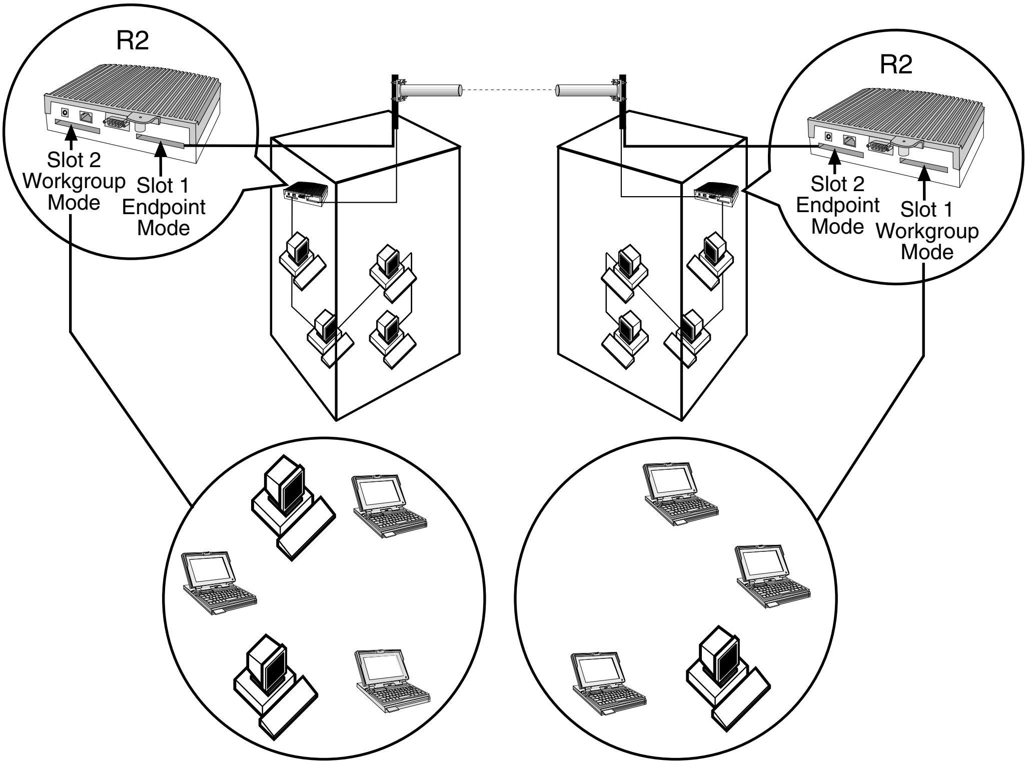


Workgroup Mode and LAN-to-LAN Example

Figure 1-7 shows two RoamAbout R2s in different buildings using an outdoor directional antenna to connect the LANs in those buildings. Each RoamAbout R2 contains two radio slots; one slot configured in Workgroup mode, and one slot configured in LAN-to-LAN Endpoint Bridge mode.

In addition, a RoamAbout R2 can be configured for multipoint mode (slot 1 only), connect to an omni-directional antenna, and connect to other APs.

Figure 1-7: Workgroup and LAN-to-LAN Endpoint Configuration



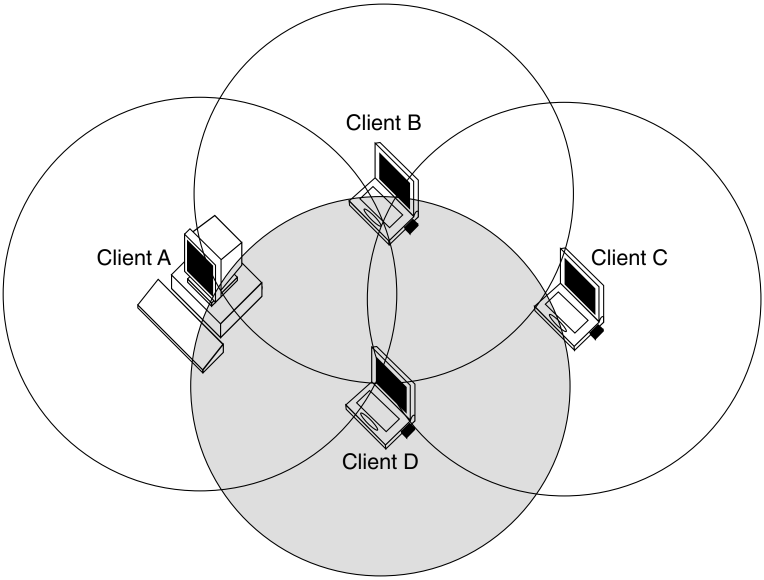
Ad-Hoc Network

Wireless ad-hoc networks do not include APs. 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 1-8** 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 1-8**, 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 1-8: 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.

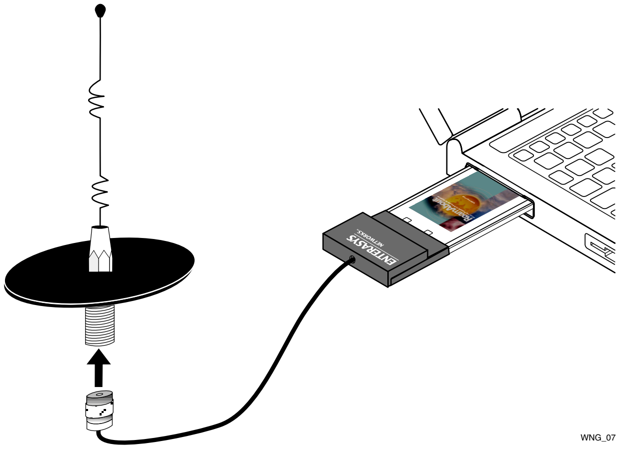
The following sections describe the types of optional antennas available with the RoamAbout products.

Vehicle-Mount Antenna

The RoamAbout Vehicle-Mount antenna (**Figure 1-9**) 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. For mounting and installation instructions, see the *RoamAbout Outdoor Antenna Site Preparation and Installation Guide*.

Figure 1-9: Vehicle-Mount Antenna



Range Extender Antenna

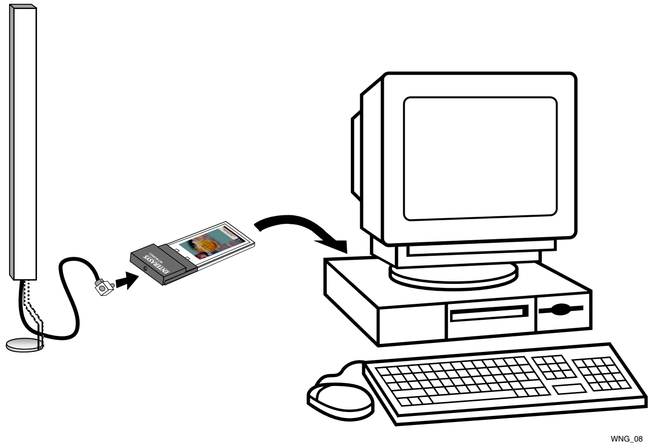
Use the Range Extender Antenna (**Figure 1-10**) to ensure optimal transmission and reception quality for situations where the integrated antennas are shielded, such as:

- The wireless device, such as a desktop client, is close to metal surfaces.
- The wireless device is installed in a hidden location, such as in a cabinet.
- Objects shield the wireless device.
- Using the RoamAbout R2 Mezzanine slot upgrade option, where two 802.11b PC Cards are installed in the RoamAbout R2 Wireless Access Platform. One of the PC Cards must be connected to the Range Extender Antenna to prevent radio interference between the two cards. In this case, the antenna must be placed at least two feet away from the RoamAbout R2.

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.

⚠ ***CAUTION**: 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 1-10: 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: **http://www.enterasys.com/wireless**.

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.

Some of the features listed are not available with earlier versions of the AP and the PC Card driver. Review the Release Notes to determine if a feature is supported by your AP version and client version.

In This Chapter

Information in this chapter is presented as follows:

Wireless Network Name

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

The AP has a Secure Access feature. When enabled, the AP does not broadcast its network name, and it only accepts connections from clients configured with the correct name. Users of operating systems like Windows XP will not see the name show up automatically in wireless LAN configuration dialogs.

When Secure Access is disabled, users can configure clients without a network name by leaving the network name field blank or using **ANY** (all uppercase) as the wireless network name, and still connect to the network. Users of operating systems like Windows XP will be able to view the network name in wireless LAN configuration dialogs.

The AP does not use a wireless network name in a LAN-to-LAN configuration.

Access Point MAC Addresses

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:

- One MAC address for the wired Ethernet interface, which is printed on the AP.
- One MAC address for the RoamAbout PC Card installed in the AP, 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.

RoamAbout R2 MAC Addresses

The RoamAbout R2 has the following MAC Addresses allocated to it:

- One MAC address for the wired Ethernet interface, which is printed on the AP.
- One MAC address for each RoamAbout PC Card installed in the AP, which is printed on a label on the back side of the card.
- One MAC address for the Spanning Tree. This MAC address is the wired MAC address plus 10 hex. For example, if the RoamAbout R2 MAC Address is *xx-xx-xx-xx-xx-40*, the Spanning Tree MAC Address will be *xx-xx-xx-xx-xx-50*.

If using SNMP, you may see additional MAC Addresses, starting with the MAC address printed on the AP. These additional 30 MAC Addresses are used internally and do not generate network traffic.

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.

- APs within the same wireless infrastructure network can be set to different channels. You can change the channel in an AP. The client automatically uses the same channel as the AP.
- Wireless clients automatically switch to the AP’s channel when roaming between APs in a wireless network; for example, there are two APs in a wireless network where AP 1 uses channel 1 and AP 2 uses channel 6. When connected to AP 1, the client automatically uses channel 1. When roaming to AP 2, the client automatically changes to channel 6.
- To avoid radio interference, adjacent APs should be set to different channels that are at least five channels apart. The APs do not necessarily have to be in the same wireless network. For example, you have three APs 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.

  NOTE

  ***NOTE**: If you have two 802.11b PC Cards installed in the RoamAbout R2, the channels between the PC Cards must be at least 5 channels apart from each other.*
- In a LAN-to-LAN configuration, the APs must be set to the same channel.
- In an Ad-Hoc network, all clients must use the same channel to communicate. The client uses a default channel which cannot be changed, with the exception of Mac and Windows XP clients. You can set the channel on Mac and Windows XP operating systems.

See **“Supported Frequency Sub-Bands” on page A-3** for a list of channels supported by country.

Transmit Rate

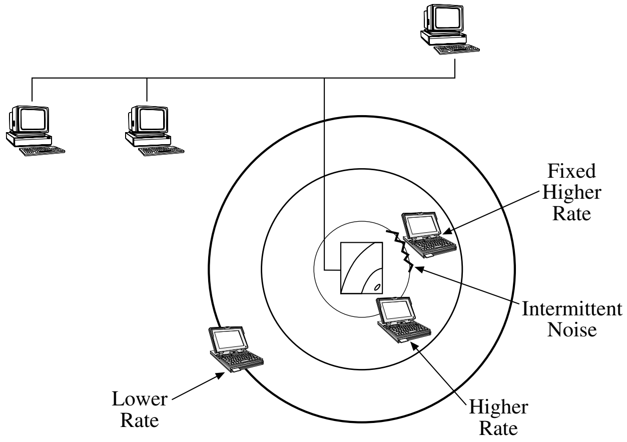
The transmit rate identifies the preferred data transmission speed of the AP. The actual data transmission speed is subject to the type of PC Cards at both ends of the wireless link and the communications quality of the link.

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 when 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.

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

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

Figure 2-1: Using Various Transmit Rates



Auto Rate

With the auto rate option, the PC Card in a client or AP automatically switches to the next 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 sporadic noise interference.

Also use Auto Rate if you have APs with 11 Mbit/s PC Cards and a mix of clients with 11 Mbit/s and 2 Mbit/s PC Cards. The AP 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.

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 AP.

After a transmission fails more than once, the AP 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 AP cannot retransmit at a lower rate.

Using a fixed low rate is useful in networks where range is more important than speed, especially when network response times are affected by numerous retransmissions and the communications quality is low due to a low signal level. Setting the transmit rate to a low rate prevents the AP from slowing network response times by transmitting data unsuccessfully at a higher rate then retransmitting at a lower rate.

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

You should not set the AP 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 AP. 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.

The RoamAbout Client Utility allows you to monitor the SNR, signal level, and noise level at the client. The Client Utility is provided on the RoamAbout 802.11 PC Card Drivers and Utilities CD-ROM, or you can download it from the RoamAbout Wireless web site.

For the AP, the RoamAbout AP Manager provides a Link Test diagnostic tool that monitors the SNR, signal level, and noise level between the AP and a remote wireless device.

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 AP. 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 number 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

The AP Density is an advanced value that changes the sensitivity of the roaming client. The distance range between RoamAbout APs listed below are estimated, and may differ depending on your operating environment.

- **Low** (default). The Low setting provides maximum coverage using a minimum number of APs. 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. The coverage area ranges up to approximately 60+ meters.
- **Medium**. The Medium setting can be used for environments where you desire clients to disassociate sooner and roam to communicate at shorter distances/higher speeds than the Low setting. The coverage area ranges approximately 40 to 60 meters.
- **High**. The High setting should only be used when you are designing a wireless infrastructure that includes a high concentration of AP devices. The coverage area ranges approximately 20 to 40 meters.
- **Minicell**. The Minicell setting should be used when you want to create small coverage areas. The coverage area distance range is approximately 10 to 20 meters.
- **Microcell**. The Microcell setting should be used when you want to create extremely small coverage areas. The distance range is approximately 5 to 10 meters.

The AP has a Medium Density Distribution parameter that automatically distributes the AP density setting to the RoamAbout wireless clients with the V7.44, or higher, driver. This parameter is enabled by default.

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 AP.

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.

The RoamAbout AP allows you to set the RTS Threshold on the AP, and to set a Remote RTS Threshold for clients to avoid a hidden station problem.

RTS Threshold

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

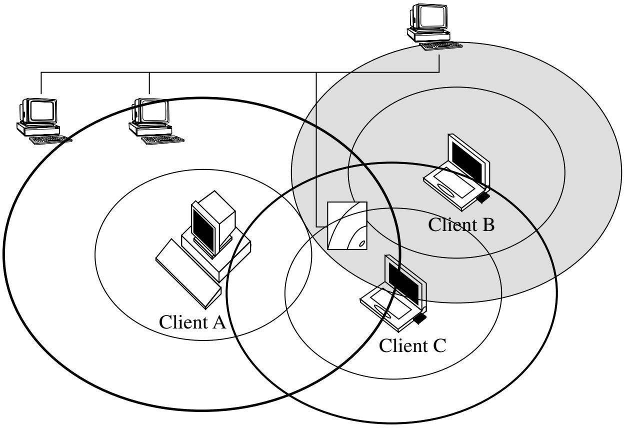
Lowering the RTS Threshold imposes additional network overhead that could negatively affect the throughput performance. You should only lower the RTS Threshold when the wireless network experiences frame collisions and lost messages.

Hidden Station

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 AP coverage area.

Figure 2-2 illustrates a hidden station example. Clients A and B are within range of the AP. 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 AP. 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 AP if possible so that the devices can sense each other's transmissions. Otherwise, enable Remote RTS Threshold on the AP. Do not change the RTS Threshold on the AP.

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

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 AP.

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 AP

The RoamAbout AP 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 AP that the client uses to connect to the network.

The client checks for network traffic addressed to the client at regular intervals. If there is no traffic addressed to the client, the client returns to sleep mode. If traffic is buffered at the AP, 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.

- Power management causes little or no difference in network performance when using transaction processing applications, such as 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 AP could cause longer network response times if a number of clients use the same AP for buffering messages while in sleep mode.

Security

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

- Network operating system security
- RoamAbout AP Secure Access
- Wired Equivalent Privacy (WEP) Encryption
- Simple Network Management Protocol (SNMP) community names
- SNMPv3 (RoamAbout R2 only)
- Device Authentication, which requires a RADIUS (Remote Authentication Dial-In User Service) server. Authentication can be based on:
    - — MAC address
    - — 802.1X
    - — Both MAC address and 802.1X
- 802.1X Rapid Rekeying
- Console port password
- Address Filtering (see **“Filters” on page 2-21**)

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 AP Secure Access

When Secure Access is enabled, the AP denies access to wireless clients that do not use the correct wireless network name. In addition, the AP does not broadcast its network name, so that clients with operating systems like Windows XP do not see the name show up in wireless LAN configuration dialogs.

When disabled, users can configure clients by leaving the network name field blank or using **ANY** (all uppercase) as the wireless network name, and still connect to the network. Clients will be able to view the network name in wireless LAN configuration dialogs.

Wired Equivalent Privacy (WEP) Encryption

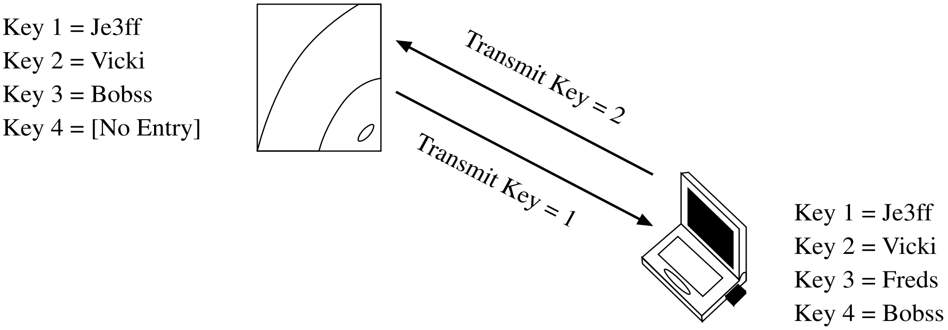
The WEP feature encrypts all data transmitted within the wireless network. The encryption uses the RC4 algorithm as defined in the IEEE 802.11 Wired Equivalent Privacy standard.

NOTE*: Broadcast and multicast messages are not encrypted.*

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 AP uses Key 1 to encrypt transmitted data, which the client can decipher. The client uses Key 2 to encrypt transmitted data, which the AP can decipher. If the AP uses Key 3 to encrypt transmitted data, it cannot be deciphered by the client. The Bobss key is Key 3 on the AP but Key 4 on the client.

Figure 2-3: Using Encryption



In a wireless infrastructure network, you can configure the APs to:

- Only accept encrypted data from clients. Only clients that have the correct encryption keys can participate in this network.
- 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.

Authentication

The RoamAbout AP supports authentication of wireless workgroup clients. An AP can authenticate clients based on:

- MAC address
- 802.1X
- Both MAC address and 802.1X (Hybrid authentication)

When using any of these types of authentication, you must configure the AP as a RADIUS client.

RADIUS Client

RADIUS (Remote Authentication Dial In User Service) is a protocol that the AP uses to communicate with a remote Authentication Server. Separating the Authentication Server from the AP means that several APs can share the same centralized authorization database. However, it also means that to successfully authenticate wireless clients, you must configure the AP as a RADIUS client.

When configured as a RADIUS client, the AP passes user authentication information to a designated RADIUS Server. The RADIUS Server receives inbound user connection requests, processes the requests to authenticate the user, then responds to the AP with the necessary information to deliver service to the user. The AP acts on the response that is returned by the RADIUS Server to allow or deny the user’s access to the network.

The AP and RADIUS Server authenticate transactions through the use of a shared secret, which is never sent over the network. They use the shared secret to encrypt RADIUS attributes containing passwords or other sensitive data. This network security greatly reduces the possibility of disclosed passwords or divulged secrets.

If you enable authentication on the AP without configuring it as a RADIUS client, the AP will be unable to contact the Authentication Server. Therefore, the AP will assume that all of the clients on the controlled ports are unauthorized and will prevent access to the LAN.

MAC Address Authentication

MAC address authentication is a form of authentication that does not place any special requirements upon clients. The RADIUS Server is configured with the MAC addresses of the wireless clients. When a client associates with the wireless LAN, the AP uses the client’s MAC address as the user name. The client is unaware that a MAC address authentication is taking place, except to the extent that the AP blocks LAN access as a result.

802.1X Authentication

IEEE 802.1X authentication allows logins based on user name, password, user certificates, and other methods that may be mutually supported by the authentication server and the clients. Only clients that support 802.1X can participate in a wireless network that uses this type of authentication.

IEEE 802.1X authentication also imposes more requirements on the RADIUS server. For MAC address authentication, a RADIUS server only needs to handle RADIUS. For 802.1X, the server must also handle EAP (Extensible Authentication Protocol) and one or more protocols, such as MD5 (Message Digest 5) or TLS (Transport Layer Security). Microsoft Windows 2000 Advanced Server is one example of a product that supports all of the protocols needed for 802.1X.

Some login methods associated with IEEE 802.1X provide a way by which an AP can securely distribute radio keys. When all of the clients on a wireless LAN use such login methods, it becomes practical to use Rapid Rekeying. Rapid Rekeying enhances security by frequently changing radio encryption keys, reducing the time to decode and use an encryption key.

Hybrid Authentication

Hybrid authentication is a special authentication mode for sites undergoing a transition to IEEE 802.1X. The AP uses both MAC address and 802.1X authentication. 802.1X takes precedence, but in the absence of 802.1X replies from a client, the AP grants access based on the MAC address. This allows you to introduce IEEE 802.1X clients without disrupting non-802.1X clients' access to the LAN. However, this prohibits the use of the Rapid Rekeying feature.

Rapid Rekeying is not available in this authentication mode. The MAC address clients would not be able to keep up with the radio key changes, and would lose connectivity to the LAN.

802.1X Rapid Rekeying

Rapid Rekeying, also known as Key Tumbling, provides automatic IEEE 802.11 WEP encryption key generation and frequent redistribution of WEP keys.

The following information applies to using Rapid Rekeying:

- Rapid Rekeying requires the use of 802.1X authentication. Unauthenticated clients and MAC address authentication clients cannot receive updated WEP keys, and would soon lose connectivity to the LAN.
- Rapid Rekeying automatically disables user-specified WEP encryption keys.
- Rapid Rekeying requires the use of an EAP login method that generates session keys, and the use of a RADIUS server that will distribute those keys to the AP. The AP uses the session keys to encrypt the WEP key distribution messages. Clients without session keys do not get new WEP keys.
- EAP-TLS authentication using X.509 certificates on the clients will work with Rapid Rekeying.
- EAP-MD5 password authentication will not work with Rapid Rekeying. EAP-MD5 does not negotiate session keys.
- Token based authentication will work with Rapid Rekeying if the token based authentication uses a TLS based method, such as TTLS or PEAP. The requirement is that there are TLS session keys negotiated and retained by the client and the AP.

The following describes how the AP introduces new key pairs.

1. The AP and clients are using the existing keys at the beginning of the Rapid Rekeying encryption cycle.

AP				Client	
Key #	**Encryption**	**TX/RX**	**State**	**TX/RX**	**Encryption**
Key1	aaaaaaaaaaaaaa	RX	Active	TX	aaaaaaaaaaaaaa
Key2	bbbbbbbbbbbbb	TX	Active	RX	bbbbbbbbbbbbb
Key3	xxxxxxxxxxxxx		Inactive		xxxxxxxxxxxxx
Key4	xxxxxxxxxxxxx		Inactive		xxxxxxxxxxxxx

2. The key period expires. The AP creates two new random keys and loads them into the inactive authenticator key indexes (Keys 3 and 4 in this example). The keys are not yet used for transmission or reception.

AP				Client	
Key #	**Encryption**	**TX/RX**	**State**	**TX/RX**	**Encryption**
Key1	aaaaaaaaaaaaaa	RX	Active	TX	aaaaaaaaaaaaaa
Key2	bbbbbbbbbbbbb	TX	Active	RX	bbbbbbbbbbbbb
Key3	**cccccccccccccc**		Inactive		xxxxxxxxxxxxxx
Key4	**ddddddddddddd**		Inactive		xxxxxxxxxxxxxx

3. The AP begins transmitting the new key pair to the authenticated clients in the supplicant list. When a client receives the new keys, it immediately begins transmitting using the new TX key. The AP does not use the new TX key until the message has been transmitted to all clients. During this time, the AP accepts transmissions on both the old and new RX keys. Note that a client can only have one TX key. The following table shows that some clients use Key1 as the TX key while other clients use Key 3.

AP				Client	
Key #	**Encryption**	**TX/RX**	**State**	**TX/RX**	**Encryption**
Key1	aaaaaaaaaaaaaa	RX	Active	TX	aaaaaaaaaaaaaa
Key2	bbbbbbbbbbbbb	TX	Active	RX	bbbbbbbbbbbbb
Key3	cccccccccccccc	RX	Active	TX	**cccccccccccccc**
Key4	ddddddddddddd		Inactive		**ddddddddddddd**

4. Once the AP transmits the new keys to all clients in the supplicant list, it begins using the new TX key (Key4). At this time all supplicants are using Key3 as their TX key.

AP				**Client**	
Key #	**Encryption**	**TX/RX**	**State**	**TX/RX**	**Encryption**
Key1	aaaaaaaaaaaaaa		Inactive		aaaaaaaaaaaaaa
Key2	bbbbbbbbbbbbb		Inactive		bbbbbbbbbbbbb
Key3	cccccccccccccc	RX	Active	TX	cccccccccccccc
Key4	ddddddddddddd	TX	Active	RX	ddddddddddddd

5. The key period expires. The AP creates two new random keys, loads them into the inactive authenticator key indexes (Keys 1 and 2 in this example), and repeats the process (starting at step 3).

AP				**Client**	
Key #	**Encryption**	**TX/RX**	**State**	**TX/RX**	**Encryption**
Key1	**eeeeeeeeeeeee**		Inactive		aaaaaaaaaaaaaa
Key2	**fffffffffffff**		Inactive		bbbbbbbbbbbbb
Key3	cccccccccccccc	RX	Active	TX	cccccccccccccc
Key4	ddddddddddddd	TX	Active	RX	ddddddddddddd

SNMP Community Names

The SNMP community name allows management tools using SNMP to display or modify AP parameters remotely.

The RoamAbout R2 supports SNMPv3. To access the RoamAbout R2 parameters via SNMP, the management tool must know the Authentication Password and Privacy Password. To support management tools using SNMPv2 or SNMPv1, the R2 provides four community names that allow SNMPv1 and SNMPv2c read-only and read-write access. The names are disabled by default with the exception of Community Name #1, which is set to **public**. The community names are only accessible from the R2 console port.

The AP 2000 supports a read/write community name and a read-only community name. By default, the AP uses **public** as the default read/write community name. This allows any management tool using SNMP to access the AP and change parameters. By changing the read/write community name, users must enter the correct community name to modify the AP parameters. The read-only community name allows the management tools to view but not change the AP parameters. You can change the read-only name so that users must enter the correct name before they can view the AP parameters.

Console Port Security

RoamAbout Access Point 2000

The RoamAbout Access Point 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.

RoamAbout R2

The RoamAbout R2 console port supports SNMPv3, and has the following security features:

- Access to the console requires a password. The username is “admin” and the default password is “password”. The password must be a minimum of eight ASCII characters, and is case-sensitive.
- The ability to enable or disable Web management and Telnet.

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 APs 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 AP 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 **"Transmit Rate" on page 2-5**. 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.
- 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 **"Transmit Rate" on page 2-5**. If the transmit rate is fixed, the broadcast and multicast messages are transmitted at the fixed rate.

Filters

The following filters are only available using the RoamAbout AP Manager, or a Network Management Station that uses SNMP.

The RoamAbout AP has three types of filters:

- Protocol

  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.

- Address

  This filter forwards or does not forward traffic based on the client's MAC address.

  — Addresses Denied: A client in the Addresses Denied list cannot access the LAN, even if the client has been authenticated.

  — Addresses Allowed: Clients in the Addresses Allowed list can access the LAN. Clients must supply their MAC address to the Network Administrator. This filter is essentially ineffective when also using authentication.

- Rate Limiting (AP 2000 only)

  Use rate limiting to enable/disable the default rate limiting, and to enter the maximum number of rate-limited frames forwarded per second.

  By default, the AP 2000 limits multicast traffic to 100 Kbit/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. The R2 does not support the multicast rate limiting function.

Spanning Tree Protocol

The RoamAbout AP uses 802.1d Spanning Tree Protocol to prevent network loops. A loop occurs when there are alternate routes between networks, as described in **“Preventing Network Loops” on page 1-12**. A loop can cause bridges to continually forward multicast traffic and degrade network performance.

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.

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 AP Spanning Tree function corrects this type of problem by shutting down the port and possibly shutting down a segment of the network.

Using the Access Point 2000

You can enable or disable the Spanning Tree when in Endpoint bridge mode. Spanning Tree is disabled when in Workgroup bridge mode and enabled in Multipoint bridge mode.

Using the RoamAbout R2

You can enable or disable the Spanning Tree in all bridge modes. The default setting is disabled.

VLANs

A VLAN is a logical partition of one or more physical networks. A single VLAN can span multiple LANs, and multiple VLANs can reside within a single LAN. One major benefit of a VLAN is that traffic is restricted to a subset of the physical LAN or LANs. Multicasts are only sent to the VLAN member ports. Therefore, a VLAN can conserve network bandwidth and improve security.

All the devices in a designated VLAN need not necessarily support VLANs. Devices that receive or generate data, such as a user's laptop or desktop computer, do not need to support VLANs to be part of a VLAN. Instead, a network device, such as a switch, can insert the VLAN ID into the data received from a device in a VLAN. Data containing the VLAN ID is considered "tagged."

Access Point 2000

The RoamAbout Access Point 2000 only allows or disallows the forwarding of tagged VLAN data in LAN-to-LAN bridge mode. The AP 2000 does not support configuring the ports as VLAN members.

The AP does not forward VLAN data while in workgroup bridge mode.

R2 Access Platform

The RoamAbout R2 supports the forwarding of tagged VLAN data. It does **NOT** support the following:

- Insertion of VLAN IDs into untagged frames.
- Spanning Trees on a per VLAN basis.
- GARP Multicast Registration Protocol (GMRP).
- VLAN IDs higher than 2047. The R2 supports VLANs numbered 2-2047.
- Forwarding of VLAN data while the R2 is in workgroup mode. The R2 does not support VLANs when either slot of the R2 is in workgroup mode.

NOTE*: VLAN 1 is a default VLAN used by the R2 to allow pass-through of untagged data. Changing the VLAN 1 default settings could prevent the R2 from forwarding untagged data.*

Network Configurations

Both the RoamAbout Access Point 2000 and the R2 can be used as a wireless bridge to an existing VLAN. For example, two APs can connect VLANs residing in different buildings, as illustrated in **Figure 2-4**. The wired side of each AP is connected to a switch that supports VLAN IDs. Switch 1 connects to VLANs Red, Blue, and Green, but only forwards data from VLANs Red and Green. Switch 2, in a different building, connects to VLANs Red and Green. The AP is configured to forward VLAN data.

Figure 2-4: Wireless Bridge Between VLANs

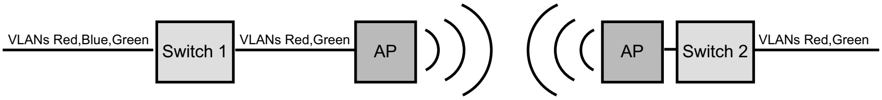
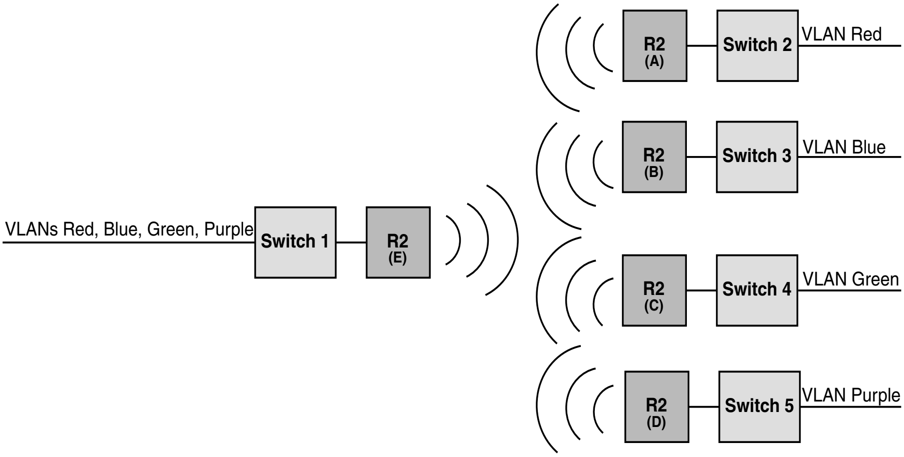


Figure 2-5 shows a point-to-multipoint configuration. Switch 1 connects to VLANs Red, Blue, Green, and Purple. R2(E) is configured to forward data from VLAN Red to wireless endpoint R2(A), VLAN Blue to R2(B), VLAN Green to R2(C), and VLAN Purple to R2(D). This example is only valid for the RoamAbout R2.

Figure 2-5: VLAN Support in Point-to-Multipoint Configuration



Ingress Filtering is always enabled on the RoamAbout R2. That is, the R2 does NOT forward data from a VLAN defined on other ports if it is received on a port that is not configured for that VLAN. In **Figure 2-5**, should R2(A) be configured incorrectly and forward VLAN Green data from Switch 2 to R2(E), R2 (E) would not forward the data. Although other R2(E) ports are configured for VLAN Green, the port receiving the data is not configured for VLAN Green. It is only configured for VLAN Red. Ingress Filtering cannot be disabled.

Static and Dynamic VLANs

A static VLAN is created when a user manually configures the ports to be Tagged, Untagged, or Forbidden. A dynamic VLAN is created when the ports are configured via the GARP VLAN Registration Protocol (GVRP), which allows network devices to share their statically configured VLANs. Dynamically configured VLANs are not saved. A reset to the device causes the device to relearn the dynamic VLANs via GVRP. The RoamAbout R2 supports both statically-configured VLAN settings and GVRP-configured settings.

GVRP only distributes statically configured VLAN information to an adjacent device. In **Figure 2-5**, should the Switch 1 port connected to R2(E) be statically configured for VLAN Gray, GVRP would configure the R2(E) wired port dynamically for VLAN Gray. The wireless ports would not be configured for VLAN Gray since they are not directly connected to Switch 1. By default, GVRP is disabled on the R2.

RoamAbout SNMP Management

Access Point 2000

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 Access Point 2000 supports the following MIB objects:

- DEC ELAN Vendor MIB
- DEC Extended LAN Bridge MIB
- DEC Hub900 Common MIB
- DEC RoamAbout MIB
- Enterasys 802.1X Extensions MIB
- Enterasys Encrypted 802.1X Configuration MIB
- Enterasys Encrypted 802.1X Rapid Rekeying MIB
- EnterasysPrivate Enterprise MIB
- Enterasys-RADIUS-AUTH-Client-MIB
- HUB PCOM MIB
- IEEE 802.11 MIB
- IEEE 8021-PAE-MIB (Port Access Entity)
- RFC1157 (SNMP Management)
- RFC1213 (MIB II)
- RFC1286 (Bridge MIB)
- RFC1398 (Ethernet Interface MIB)
- RFC1493 (IETF Bridge MIB)
- RFC1757 (RMON MIB)
- RFC2618 (RADIUS Authentication Client MIB)

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

Refer to the Release Notes for a complete list of supported MIB objects.

RoamAbout R2

The RoamAbout R2 supports SNMPv3. If your Network Management Station (NMS) does not support SNMPv3, use the RoamAbout R2 console port to configure the Communities Views for SNMPv1 and SNMPv2c access.

The RoamAbout R2 supports the following MIBs:

- Enterasys-802.11 Extensions MIB
- Enterasys Extended Switch MIB
- Enterasys Encrypted 802.1X Rapid Rekeying MIB
- EnterasysPrivate Enterprise MIB
- Enterasys-R2Management.mi2
- Enterasys-RADIUS-AUTH-Client-MIB
- IANAifType-MIB
- IEEE 802.11 MIB
- IEEE 802.1X MIB
- IEEE 8021-PAE-MIB (Port Access Entity)
- RFC1157 (SNMP Management)
- RFC1213 (MIB II)
- RFC1493 (IETF Bridge MIB)
- RFC1757 (RMON MIB)
- RFC1907 (SNMPv3)
- RFC2233 (IF-MIB)
- RFC2571 (SNMP Management Framework)
- RFC2572 (SNMP MPD)
- RFC2573n (SNMP Notification MIB)
- RFC2573t (SNMP Target MIB)
- RFC2574 (SNMP USM)
- RFC2575 (SNMP VACM)
- RFC2618 (RADIUS Auth. Client MIB)
- RFC2665 (Ether-Like MIB)
- RFC2674p (P-Bridge-MIB)
- RFC2674q (Q-Bridge-MIB)
- TMSCommonMib
- TMSL3Mib

Refer to the Release Notes for a complete list of supported MIB objects.

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.

Some of the features listed are not available with earlier versions of the AP and the PC Card driver. Review the Release Notes to determine if a feature is supported by your AP version and client version.

In This Chapter

Information in this chapter is presented as follows:

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 number of APs needed. Afterwards, you need to examine the AP hardware requirements and the wireless client system requirements.

When designing a wireless network, consider the security issues for your environment. Security can include the following:

- Keeping the AP in a locked closet.
- Using the security cover. A security cover is not included with the Access Point 2000 (contact your Enterasys Representative for more information).
- Preventing unauthorized users from joining the wireless network.
- Using authentication and data encryption to ensure that sensitive data is kept private.

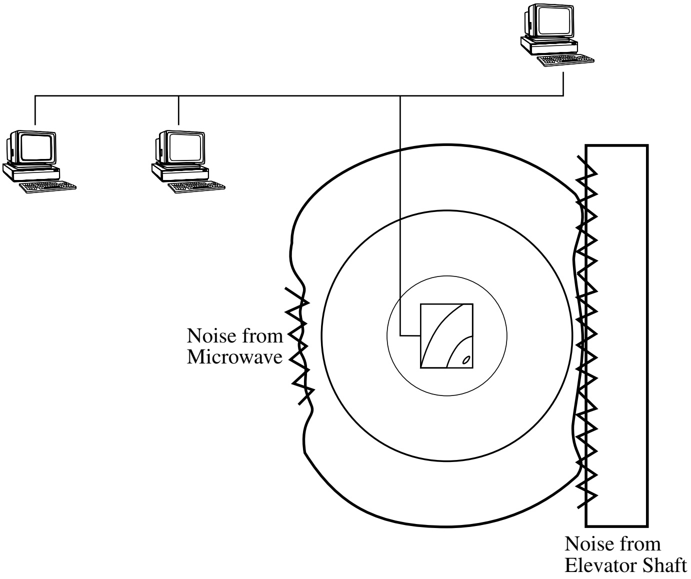
Determining the Coverage Area and Supported Users

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)

Figure 3-1: Coverage Area



The faster the transmit speed, the shorter the coverage area at that speed. An AP 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. Increasing the AP Density will also reduce the coverage area of a single AP.

A RoamAbout Access Point can support up to 250 users within its coverage area. The RoamAbout R2 supports up to 250 users per slot. 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 APs.

Be aware of potential hidden station problems, as described in **"Hidden Station" on page 2-10**. If possible, arrange the coverage area to minimize or prevent any two clients from being within range of the AP, but out of range from each other.

Selecting the Location for a Single AP

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

For best placement, configure the AP and a client and use the procedure in the **"Optimizing RoamAbout AP Placement" on page 6-5** before permanently mounting the AP.

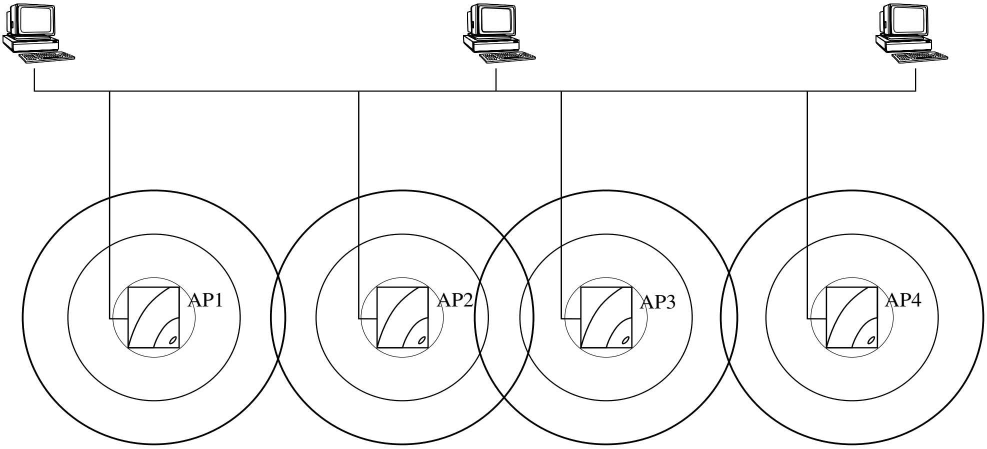
Selecting the Locations for Multiple APs

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 APs closer together (see **Figure 3-2**).

Figure 3-2: Overlapping Coverage Areas



- If possible, have the adjacent APs whose coverage areas overlap use different channels that are at least five channels apart.

NOTE

***NOTE**: If you are using two PC cards in the RoamAbout R2, they must be 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 AP but out of range with each other.

For best placement, configure the AP and a client and use the procedure in the **“Optimizing RoamAbout AP Placement” on page 6-5** before permanently mounting the AP.

Before mounting the AP, review the hardware requirements described in the installation documentation that shipped with the RoamAbout AP.

RoamAbout R2 Mezzanine Special Considerations

The following information pertains to the RoamAbout R2 with the Mezzanine option installed:

- Slot 2 does not support LAN-to-LAN Multipoint.
- If two 802.11b PC Cards are installed in the RoamAbout R2, one of the PC Cards must be connected to the Range Extender Antenna to prevent radio interference between the two cards. The antenna must be placed at least two feet away from the RoamAbout R2. This is not necessary if one of the cards is connected to an outdoor antenna.
- If you have two 802.11b PC Cards installed in the RoamAbout R2, the channels between the PC Cards must be at least 5 channels apart from each other.

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 APs in different networks can overlap without interference as long as they use different channels. If possible, have the APs 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 AP.

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.

NOTE*: If you are planning to use an outdoor antenna refer to the* RoamAbout Outdoor Antenna Site Preparation and Installation Guide *for regulatory information, FCC requirements, and detailed procedures to install outdoor antennas.*

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 AP and the outdoor antenna must use the same earth ground.
- Connecting of the outdoor antenna to the AP, and connecting the AP 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 APs should be within each other’s coverage area. The speed you want to use for your wireless link is one factor that determines the distance between the APs. 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.

- 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 AP, review the hardware requirements described in the installation documentation that came with the RoamAbout AP.

NOTE*: Using the AP Density feature will change the coverage area. See* **AP Density and Roaming on page 2-8** *for more information.*

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. Default channels are listed in **Table A-3 on page A-3**.
- 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.

  — 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 **“Wireless Network Hardware Installation Overview” on page 3-9**.

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 AP in the location you have chosen. Refer to the RoamAbout documentation to install the hardware.
2. Install a tool to configure the AP as described in **Chapter 4**.
3. Configure the APs using the procedures in **Chapter 5**. You should configure the APs before configuring clients. A number of client settings depend on the AP 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), see the **“RoamAbout Client Utility” on page 4-7**.
6. Configure the wireless clients using the procedures described in the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide.*

LAN-to-LAN Configuration

The following is an overview of the steps to install the APs 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 APs in the locations you have chosen. Refer to the RoamAbout AP documentation to install the AP hardware.
3. Choose and install a tool to configure the AP as described in **Chapter 4**.
4. Configure the APs using the procedure in the **“Configuring APs in a Point-to-Point Network” on page 5-8** or **“Configuring the AP for Point-to-Multipoint” 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), see the **"RoamAbout Client Utility" on page 4-7**.
3. Configure the wireless clients, as described in the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide*.

Chapter 4

Wireless Network Tools

This chapter describes the configuration tools.

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

- RoamAbout AP Manager
- RoamAbout console port
- Telnet (RoamAbout R2 only)
- Web Management (RoamAbout R2 only)
- Network Management Station (NMS)

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

In This Chapter

Information in this chapter is presented as follows:

RoamAbout AP Manager

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

The AP Manager has the following features:

- Ability to manage multiple APs remotely, including changing parameters on multiple APs in a wireless network with a single command.
- Ability to group APs. For example, you can group together all the APs in one wireless network and have a second group for APs in another wireless network.
- Ability to view AP parameters such as statistics, firmware version number, MAC addresses, amount of memory, and card type.
- Integrity checking for many wireless parameter changes. This warns 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 AP firmware upgrades, also called flash upgrades.
- Support for 802.11 radio technology.
- Ability to manage current and previous releases of the AP firmware. The AP Manager only allows access to those features supported by the selected AP.

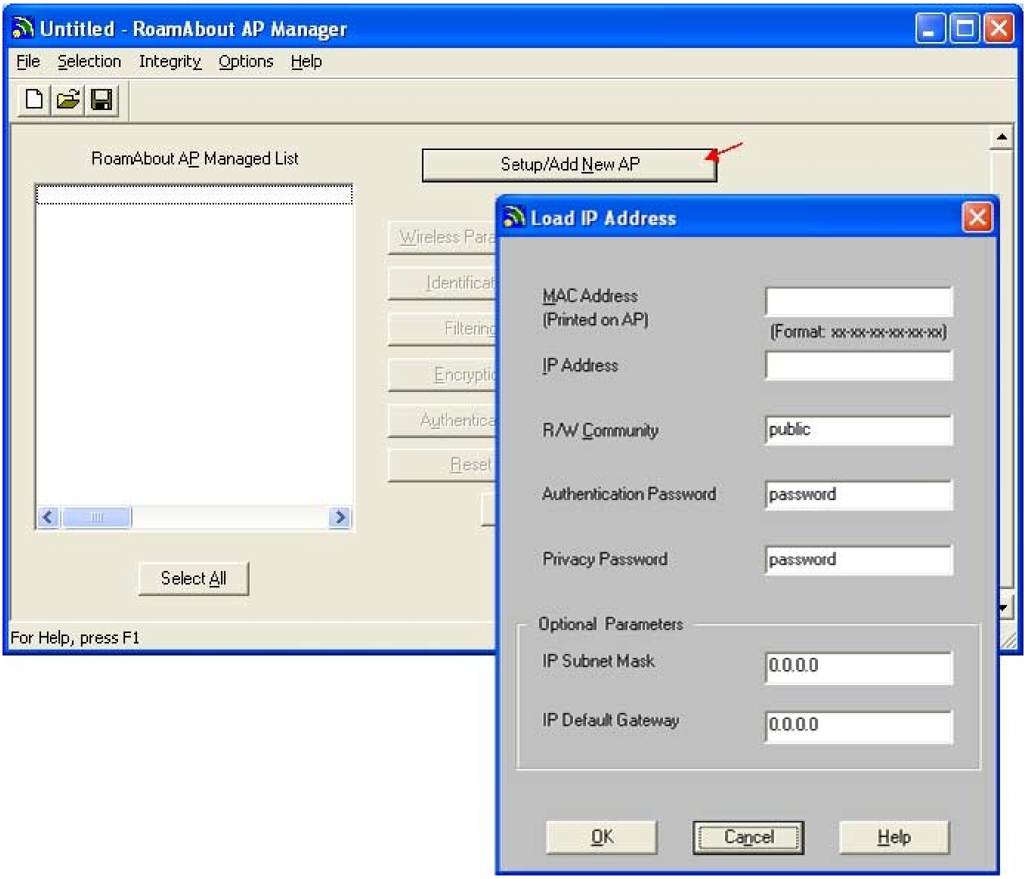
Installing the RoamAbout AP Manager

The AP Manager supports Windows 95, Windows 98, Windows 2000, Windows Me, Windows NT (V4.0 or later), and Windows XP.

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

The AP Manager is included on the CD-ROM in the RoamAbout AP kit, and can also be downloaded from the enterasys.com/wireless web site. To install the AP Manager, follow the installation instructions. After the installation, you can open the AP Manager main window, shown in **Figure 4-1**, by clicking the **Start** button on the Windows desktop and selecting **Programs→RoamAbout→RoamAbout AP Manager**.

Figure 4-1: RoamAbout AP Manager Main Window



MAC Address (Printed on AP)

(Format: xx-xx-xx-xx-xx-xx)

IP Address

R/W Community: public

Authentication Password: password

Privacy Password: password

Optional Parameters

IP Subnet Mask: 0.0.0.0

IP Default Gateway: 0.0.0.0

Using the AP Manager

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

- All APs 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 APs in an infrastructure network and APs in a LAN-to-LAN configuration. APs in these configurations are managed differently.
- If you have earlier releases of the RoamAbout AP, you can group non-802.11 compliant APs together, separate from the 802.11 APs.

The AP Manager saves each group in a configuration file (*.CFG). When you create a group, give the file a meaningful name that represents the group, such as Campus for APs used outside on a college campus, or Engineering if all the APs are used for the Engineering wireless network.

When you open a configuration file, the APs in the group are displayed in the Managed List field on the main window (see **Figure 4-1**). You can add or remove APs from the configuration file. The following lists some of the actions you can perform from the AP Manager main window:

- Each time you open the AP Manager, the **RoamAbout AP 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 APs in that group are displayed in the Managed List field.
- If there is a RoamAbout R2 in the list, you are prompted for a password. The password is the password that you entered when you created the configuration file.
- To display the settings that the AP is currently using, select the AP in the Managed List field and click the various buttons, such as **Wireless Parameters**, **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 AP and another device in the same wireless network, select **Integrity** in the menu bar and select **Link Test**.
- To discover all APs in your network, select **Selection** in the menu bar and **Discover**.

Chapter 5 contains the procedures to configure APs using the AP Manager.

Other SNMP Management Tools

The AP 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.

- To manage the AP with an NMS, you must first use the console port or AP Manager to configure the AP with a valid IP address.
- The RoamAbout R2 supports SNMPv3. If your NMS does not support SNMPv3 and you want to use SNMPv1 or SNMPv2c, use the RoamAbout R2 console to access the community names. The RoamAbout R2 Community screen contains four community names that allow SNMPv1 and SNMPv2c read-only and read-write access to an NMS. The names are disabled by default with the exception of Community Name #1, which is set to **public**. If using SNMPv3, you should leave names 2 through 4 disabled.
- The following AP settings are only accessible from an NMS:
  - RMON parameters
  - Aging timer

RoamAbout Console Port

You can manage the AP 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. Typically, you do not need to use the console port if you use the AP Manager to manage the AP. However, the R2 SNMP community names are only modifiable from the R2 console port.

Refer to **Appendix B** for the procedure to connect a device to the AP console port.

Telnet

You can manage the RoamAbout R2 through Telnet. However, you must first assign the R2 an IP address.

Perform the following steps to access the R2 through Telnet:

1. Open a DOS Prompt.
2. Telnet to the IP Address that you assigned to the RoamAbout R2.

   For example: `telnet 10.0.0.00`

   You are prompted for a username and password. The default username is **admin** and the default password is **password**. The Main Menu appears.
3. Ensure that your preferences are set to use the arrow keys.

Web Management

You can manage the RoamAbout R2 through your web browser. However, you must first assign the R2 an IP address. Refer to **Appendix B** for the procedure to connect a device to the AP console port.

The RoamAbout R2 web management runs on the following browsers:

- Netscape Communicator V4.5, V4.6, V4.7 and V6.0 (and later)
- Microsoft Internet Explorer V4.0 and V5.0 (and later)

You must set the browser proxy to Direct Internet Connection. Then enter the IP address that you assigned to the RoamAbout R2 in the browser window. You are prompted for a username and password. The default username is **admin** and the default password is **password**.

RoamAbout Client Utility

The RoamAbout Client Utility is a diagnostic tool for RoamAbout wireless networks. The RoamAbout Client Utility is included on the RoamAbout 802.11 PC Card Drivers and Utilities CD-ROM, or you can download it from the RoamAbout Wireless web site. Refer to the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* for setup and installation information.

Use the Client Utility to:

- Perform a radio Link Test with a single AP or computer. The Link Test mode allows you to verify the communications quality of the RoamAbout PC Card in more detail. It allows you to investigate the performance of the RoamAbout radio link between:
  - — Your computer and another wireless computer
  - — Your computer and the current AP
- Perform a Site Survey running the Site Monitor option. Use the Site Monitor mode to display the communications quality of your computer with multiple APs in its vicinity. The Site Monitor mode allows you to conduct a site survey to:
  - — Determine the overall wireless coverage of your LAN network.
  - — Determine or optimize placement of your APs, to provide seamless connectivity to mobile stations.

For detailed information about each Client Utility window, consult the RoamAbout Client Utility on-line help by clicking the **Help** button in each 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**.

- To install the drivers and utilities on the clients, refer to the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide*.
- If you are configuring a wireless infrastructure network, configure the APs first. Many of the wireless client parameters are based on the AP settings.
- For infrastructure and ad-hoc networks, document the common settings for any clients that join the network at a future date.

In This Chapter

Information in this chapter is presented as follows:

Configuring APs in an Infrastructure Network

After installing the AP, you can configure its network and wireless parameters using the AP Manager, the console port, or the R2 Web Management. To configure the RoamAbout R2 for management by an NMS using SNMPv2 or SNMPv1, see **"Configuring the R2 for SNMPv1 or SNMPv2" on page 5-29**.

Required Information

When configuring an AP, have the following information available:

- If the AP has been configured with an IP address, you need to know that IP address. If the AP has not been assigned an IP address, you need the following:
  - — The AP wired MAC address, which is printed on the front of the Access Point 2000 and on the side of the RoamAbout R2.
  - — Valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway.
- The AP SNMP read/write community name (default is **public**). If you do not enter the correct community name, you cannot modify the AP or add it to an AP Manager group.
- For a RoamAbout R2, the SNMPv3 Authentication and Privacy Passwords (default for both is **password**).
- Identification information, such as a unique name for the AP, its location, and the name of the person responsible for the AP.

Wireless Parameters Used in an Infrastructure Network

If adding APs to an existing wireless network, write down the wireless parameter settings. If creating a wireless infrastructure network, you can enter the Channel, Wireless Network Name, and Station Name, and use the default settings for the other parameters. The following describes the settings used in an infrastructure network:

- **Slot 1/Slot 2**: (RoamAbout R2 only): Select the slot to be configured.
- **Channel**: Set adjacent APs to different channels that are at least five channels apart if possible. See **Appendix A** for channel information.
- **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

- **Station name**: Select a unique name that helps identify the location of the AP. Each AP should have a unique station name.
- **Bridge Mode**: Set to **Workgroup**.
- **AP Density**: See **AP Density and Roaming on page 2-8** for more information.
- **Transmit Rate**: The default setting works well in most environments. See **"Transmit Rate" on page 2-5**.
- **RTS Threshold**: The default setting works well in most environments. See **"RTS/CTS Protocol" on page 2-9**.
- **Remote RTS Threshold**: The default setting works well in most environments. See **"RTS/CTS Protocol" on page 2-9**. This setting is only available on a RoamAbout R2 managed by the AP Manager.
- **DTIM**: In nearly all environments, you should not change the default DTIM of 1. See **"802.11 Power Management" on page 2-11**.
- **Secure Access**: Enable to prevent clients without the correct wireless network name from connecting to this AP.
- **Multicast Transmit Rate**: Identifies the desired transmission speed for the broadcast and multicast traffic as forwarded by the AP to the wireless LAN. You should use the lowest speed that you want to support. If using applications that use multicast traffic (for example, IGMP), you can increase this rate from the default of 2 Mbit/s Fixed.
- **IntraBSS Relay**:
  - — **Enable**: Allows wireless users associated with an AP to see and communicate between each other. This is accomplished by taking a multicast packet from one wireless user and rebroadcasting it so that all wireless users see it.
  - — **Disable**: Prevents communication between users associated with an AP. This mode is intended for use in the ISP market where the ISP does not want separate households to browse the Network Neighborhood and see other customers and their hard drives.
- **Medium Density Distribution**: Enable it to have the AP distribute its AP Density (low, medium, high, minicell, microcell) to the clients. This setting is not available from the console ports.
- **Load Balancing**: Forces wireless clients to associate with APs that are least busy, resulting in a more even distribution of client associations between APs. Load balancing increases the network's overall throughput. Load balancing is enabled by default. This setting is not available from the console ports.

Using the AP Manager

Use the **Help** button in the AP Manager for a description of any field.

1. If you are currently managing APs with the AP Manager, determine if the new AP belongs to an existing group. Refer to **"RoamAbout AP Manager" on page 4-2** for a description of configuration groups.

   File→Open (adds the AP to an existing group)

   File→New (starts a new group)

2. Click **Setup/Add New AP**.

3. If the AP has been assigned an IP address, click **No** when asked if you need to load an IP address on the AP. If the AP does not have an IP address, click **Yes**.

4. Enter a new IP address or the AP's existing IP address and other network parameters as prompted.

   You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager displays the Identification and Wireless Parameter dialog boxes.

5. **Identification**: Enter information that will help administrators identify the AP.

6. **Wireless Parameters**: Enter the wireless parameters for your wireless network. If your wireless network requires additional settings, click the **Advanced** button.

7. Click **OK**.

8. To implement your changes:

   R2 AP: Select **Reset** from the main window. Select **Reset Slot x**, where x is the slot (1 or 2) you configured.

   AP 2000: Select **Reset** from the main window. Select **Reset with Current Settings**. Allow approximately one minute for the AP to reset and complete its self-test.

9. Repeat this procedure to add additional APs to this or other configuration groups.

10. When configuring wireless clients, enter the Wireless network name especially if Secure Access is enabled.

Refer to the other sections in this chapter to configure features such as authentication, encryption, and filters.

Using the RoamAbout R2 Console Port

To use the console port, follow the instructions in **"Connecting a Device to the Console Port" in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Network Configuration** from the Main Menu and enter the following parameters:

   IP address: Enter the IP address you wish to assign to the AP.

   Subnet mask: Enter the subnet mask you wish to assign to the AP.

   Default gateway: Enter the IP address of the default gateway.

   Spanning Tree: Set to **Disable**.

   IP Address Mode: Set to **Manual** when configuring an AP for the first time. For more information, see **"Modifying the IP Address" on page 5-19**.

   Ethernet Speed: This sets the speed of the wired Ethernet connection. The default setting, **autonegotiate**, works well in most environments.

   GVRP: Set to **Disabled** unless you are configuring the AP to support VLANs, as described in **"Configuring for VLANs" on page 5-40**.

   CDP: This setting is Disabled by default in Workgroup mode. To change this setting, refer to **"Setting the Cabletron Discovery Protocol" on page 5-21**.

2. Choose **Save**.

3. Choose **Wireless Configuration** from the Main Menu, then choose **Set/Show Wireless Configuration**.

4. At the top of screen, select the radio slot (1 or 2) to configure.

5. Enter the wireless parameters.

6. Set the **Reset Option** to **Reset Radio if necessary** (default setting).

7. Choose **Save**.

8. To configure the RoamAbout clients, write down the Wireless Network Name, especially if Secure Access is enabled.

Refer to the other sections in this chapter to configure features such as authentication, encryption, and filters.

Using the Access Point 2000 Console Port

To use the console port, follow the instructions in **"Connecting a Device to the Console Port" in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Set IP Address** from the Installation Menu.
2. Enter the IP address, subnet mask, and default gateway.
3. Choose **Module-Specific Options** from the Installation Menu.
4. Choose **Set Wireless Configuration**. Enter the wireless parameters for your wireless network.
5. Select **Module-Specific Options** from the Installation Menu and set the following parameters:

   Bridge Mode Options: Set to **Workgroup**.

   Enable/Disable Default Rate Limiting: Set to Disabled to disable the 100 Kbit/sec limitation on multicast traffic.
6. Optionally, you can enable console security as follows:
   a) Choose **Enable/Disable Console Password** from the Installation Menu. Enable Console Password to prevent other users from using the console port to view or modify settings.

   b) Select **Set SNMP Read/Write Community** from the Installation Menu. Enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.
7. To implement your changes, select **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the AP to reset and complete its self-test.
8. When configuring wireless clients, enter the Wireless network name especially if Secure Access is enabled.

Refer to the other sections in this chapter to configure features such as authentication, encryption, and filters.

Configuring APs in a Point-to-Point Network

You can configure two APs 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. To configure the RoamAbout R2 for management by an NMS using SNMPv2 or SNMPv1, see **"Configuring the R2 for SNMPv1 or SNMPv2" on page 5-29**.

Required Information

When configuring an AP, have the following information available:

- If the AP has been configured with an IP address, you need to know that IP address. If the AP has not been assigned an IP address, you need the following:
  - — The AP wired MAC address, which is printed on the front of the Access Point 2000 and on the side of the RoamAbout R2.
  - — Valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway.
- The AP SNMP read/write community name (default is **public**). If you do not enter the correct community name, you cannot modify the AP or add it to an AP Manager group.
- For a RoamAbout R2, the SNMPv3 Authentication and Privacy Passwords (default for both is **password**).
- Wireless MAC address of each AP. The wireless MAC address is NOT the same as the wired MAC address printed on the AP. Perform one of the following to see the wireless MAC address:
  - — AP Manager: Select each AP from the **Managed List** field and click the **Hardware** button.
  - — Access Point 2000 console port: **Show Current Settings** from the Installation Menu.
  - — R2 console port: **Current Configuration** from the Main Menu.
  - — Back of the PC Card used in the AP. The MAC address of the PC Card is the AP's wireless MAC address.
- Identification information, such as a unique name for the AP, its location, and the name of the person responsible for the AP.

Wireless Parameters Used in a Point-to-Point Network

The following AP parameters are not used in this configuration:

- Wireless Network Name
- Secure Access
- IntraBSS Relay
- AP Density
- Power Management (DTIM Period)
- Multicast Transmit Rate

The following describes the settings used in a point-to-point network:

- **Slot 1/Slot 2**: (RoamAbout R2 only): Select the slot to be configured.
- **Channel**: Both APs must use the same channel.
- **Station name**: Select a unique name that helps identify the location of the AP. Each AP should have a unique station name.
- **Bridge Mode**: Set to **LAN-to-LAN Endpoint**.
- **Remote Wireless MAC Address**: Enter the wireless MAC address of the remote AP.
- **Transmit Rate**: A fixed rate is recommended for most environments. See **"Transmit Rate" on page 2-5**.
- **RTS Threshold**: The default setting works well in most environments. See **"RTS/CTS Protocol" on page 2-9**.
- **Spanning Tree**: Set to Enabled or Disabled. For more information, see **"Spanning Tree Protocol" on page 2-22**.

Using the AP Manager

Use the **Help** button in the AP Manager for a description of any field.

1. If you are currently managing APs with the AP Manager, determine if the new AP belongs to an existing group. Refer to **“RoamAbout AP Manager” on page 4-2** for a description of configuration groups.

   File→Open (adds the AP to an existing group)

   File→New (starts a new group)

2. Click **Setup/Add New AP**.

3. If the AP has been assigned an IP address, click **No** when asked if you need to load an IP address on the AP. If the AP does not have an IP address, click **Yes**.

4. Enter a new IP address or the AP’s existing IP address and other network parameters as prompted.

   You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager displays the Identification and Wireless Parameter dialog boxes.

5. **Identification**: Enter information that will help administrators identify the AP.

6. **Wireless Parameters**: Enter the wireless parameters for your wireless network. Click the **Advanced** button to view all wireless parameters.

7. Click **OK**.

8. To implement your changes:

   R2 AP: Select **Reset** from the main window. If changing the bridge mode, select **Reset with Current Settings**. Otherwise, select **Reset Slot x**, where x is the slot (1 or 2) you configured.

   AP 2000: Select **Reset** from the main window. Select **Reset with Current Settings**. Allow approximately one minute for the AP to reset and complete its self-test.

9. Repeat this procedure at the other AP.

Refer to the other sections in this chapter to configure features such as encryption and filters.

Using the RoamAbout R2 Console Port

To use the console port, follow the instructions in **"Connecting a Device to the Console Port" in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Network Configuration** from the Main Menu and enter the following parameters:

   IP address: Enter the IP address you wish to assign to the AP.

   Subnet mask: Enter the subnet mask you wish to assign to the AP.

   Default gateway: Enter the IP address of the default gateway.

   Spanning Tree: Set to Enabled or Disabled. For more information, see **"Spanning Tree Protocol" on page 2-22**.

   IP Address Mode: Set to **Manual** when configuring an AP for the first time. For more information, see **"Modifying the IP Address" on page 5-19**.

   Ethernet Speed: This sets the speed of the wired Ethernet connection. The default setting, **autonegotiate**, works well in most environments.

   GVRP: Set to **Disabled** unless you are configuring the AP to support VLANs, as described in **"Configuring for VLANs" on page 5-40**.

   CDP: This setting is Auto Enabled by default in LAN-to-LAN mode. To change this setting, refer to **"Setting the Cabletron Discovery Protocol" on page 5-21**.

2. Choose **Save**.

3. Choose **Wireless Configuration** from the Main Menu, then choose **Set/Show Wireless Configuration**.

4. At the top of screen, select the radio slot (1 or 2) to configure.

5. Enter the wireless parameters.

6. Set the **Reset Option** to **Reset Radio if necessary** (default setting).

7. Choose **Save**.

8. If changing the bridge mode, you need to implement your changes by choosing **Reset/Upgrade** in the Main Menu then choosing **Reset Switch**. Allow approximately one minute for the AP to reset and complete its self-test.

9. Perform this procedure on the other AP.

Refer to the other sections in this chapter to configure features such as encryption and filters.

Using the Access Point 2000 Console Port

To use the console port, follow the instructions in **"Connecting a Device to the Console Port" in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Set IP Address** from the Installation Menu.
2. Enter the IP address, subnet mask, and default gateway.
3. Choose **Module-Specific Options** from the Installation Menu.
4. Choose **Set Wireless Configuration**. Enter the parameters for your wireless network.
5. Select **Bridge Mode Options** in the Module-Specific Options menu.

   Bridge Mode: Set to **LAN-to-LAN End-Point**.

   Remote Wireless MAC Address: Enter the wireless MAC address of the remote AP.

   Spanning Tree Mode: Set to Enabled or Disabled. For more information, see **Spanning Tree Protocol on page 2-22**.
6. Optionally, you can enable console security as follows:

   a) From the Installation Menu, choose **Enable/Disable Console Password**. Set to Enable.

   b) Select **Set SNMP Read/Write Community** from the Installation Menu. Enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.
7. To implement your changes, select **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the AP to reset and complete its self-test.
8. Perform this procedure on the other AP.

Refer to the other sections in this chapter to configure features such as encryption and filters.

Configuring the AP for Point-to-Multipoint

You can configure up to seven APs in a point-to-multipoint configuration. At least one AP must be configured as a Central AP. The other APs are configured as endpoint APs, as described in **"Point-to-Multipoint" on page 1-10**. To configure the RoamAbout R2 for management by an NMS using SNMPv2 or SNMPv1, see **"Configuring the R2 for SNMPv1 or SNMPv2" on page 5-29**.

Required Information

When configuring an AP, have the following information available:

- Valid Multipoint Activation Key (16 characters) to enable Multipoint bridge mode (purchased separately). Contact your Enterasys Representative.
- If the AP has been configured with an IP address, you need to know that IP address. If the AP has not been assigned an IP address, you need the following:
  - — The AP wired MAC address, which is printed on the front of the Access Point 2000 and on the side of the RoamAbout R2.
  - — Valid, unused IP address. Depending on your network configuration, you may also need to provide the subnet mask and default gateway.
- The AP SNMP read/write community name (default is **public**). If you do not enter the correct community name, you cannot modify the AP or add it to the AP Manager group.
- For a RoamAbout R2, the SNMPv3 Authentication and Privacy Passwords (default for both is **password**).
- Wireless MAC address of each AP. The wireless MAC address is NOT the same as the wired MAC address printed on the AP. Perform one of the following to see the wireless MAC address:
  - — AP Manager: Select each AP from the **Managed List** field and click the **Hardware** button.
  - — Access Point 2000 console port: **Show Current Settings** from the Installation Menu.
  - — R2 console port: **Current Configuration** from the Main Menu.
  - — Back of the PC Card used in the AP. The MAC address of the PC Card is the AP's wireless MAC address.
- Identification information, such as a unique name for the AP, its location, and the name of the person responsible for the AP.

Wireless Parameters Used in a Point-to-Multipoint Network

The following AP parameters are not used in this configuration:

- Wireless Network Name
- Secure Access
- IntraBSS Relay
- AP Density
- Power Management (DTIM Period)
- Multicast Transmit Rate

The following describes the settings used in a point-to-multipoint network:

- **Slot 1/Slot 2** (RoamAbout R2 only): Select the slot to be configured. For the central AP, Slot 1 must be selected.
- **Channel**. All APs must use the same channel.
- **Station name**. Select a unique name that helps identify the location of the AP. Each AP should have a unique station name.
- **Bridge Mode**:

  Central AP: Set to **LAN-to-LAN Multipoint**.

  Endpoint APs: Set to **LAN-to-LAN Endpoint**.
- **Multipoint Activation Key** (Central AP only): Enter the 16 character alphanumeric activation key.
- Remote Wireless MAC addresses: Central AP: Enter the wireless MAC addresses of the other APs. Any unused fields must be null (contain no characters). Endpoint APs: Enter the wireless MAC address of the Central AP.
- **Wireless Relay** (Central AP, Access Point 2000 only): Enable to allow the endpoint APs to communicate with each other through the Central AP, or Disable to only allow the endpoint APs to communicate with the Central AP and its wired LAN.
- **Transmit Rate**: The default setting works well in most environments. See **“Transmit Rate” on page 2-5**.
- **RTS Threshold**: The default setting works well in most environments. See **“RTS/CTS Protocol” on page 2-9**.
- **Spanning Tree**: Central AP: Set to **Enabled**. Endpoint APs: Enable or disable. For more information, see **“Spanning Tree Protocol” on page 2-22**.

Using the AP Manager

Use the **Help** button in the AP Manager for a description of any field.

1. Determine which AP is the Central AP, as described in **“Point-to-Multipoint” on page 1-10**.

2. If you are currently managing APs with the AP Manager, determine if the new AP belongs to an existing group. Refer to **“RoamAbout AP Manager” on page 4-2** for a description of configuration groups.

   File→**Open** (adds the AP to an existing group)

   File→**New** (starts a new group)

3. Click **Setup/Add New AP**.

4. If the AP has been assigned an IP address, click **No** when asked if you need to load an IP address on the AP. If the AP does not have an IP address, click **Yes**.

5. Enter a new IP address or the AP’s existing IP address and other network parameters as prompted.

   You may need to wait a few minutes for the IP address to load. Afterwards, the AP Manager displays the Identification and Wireless Parameter dialog boxes.

6. **Identification**: Enter information that will help administrators identify the AP.

7. **Wireless Parameters**: Enter the wireless parameters for your wireless network. Click the **Advanced** button to view all the wireless parameters.

   When configuring the Central AP, click the **LAN-to-LAN Multipoint Properties** button to enter the wireless MAC addresses of the other APs. Any unused fields must be null (contain no characters).

8. Click **OK**.

9. To implement your changes:

   R2 AP: Select **Reset** from the main window. If changing the bridge mode, select **Reset with Current Settings**. Otherwise, select **Reset Slot x**, where x is the slot (1 or 2) you configured.

   AP 2000: Select **Reset** from the main window. Select **Reset with Current Settings**. Allow approximately one minute for the AP to reset and complete its self-test.

10. Repeat this procedure at the other APs.

Refer to the other sections in this chapter to configure features such as encryption and filters.

Using the RoamAbout R2 Console Port

To use the console port, follow the instructions in **“Connecting a Device to the Console Port” in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Network Configuration** from the Main Menu and enter the following:

   IP address: Enter the IP address you wish to assign to the AP.

   Subnet mask: Enter the subnet mask you wish to assign to the AP.

   Default gateway: Enter the IP address of the default gateway.

   Spanning Tree: For the Central AP, set to **Enabled**. For the APs in LAN-to-LAN Endpoint bridge mode, you can enable or disable Spanning Tree. For more information, see **“Spanning Tree Protocol” on page 2-22**.

   IP Address Mode: Set to **Manual** when configuring an AP for the first time. For more information, see **“Modifying the IP Address” on page 5-19**.

   Ethernet Speed: This sets the speed of the wired Ethernet connection. The default setting, **autonegotiate**, works well in most environments.

   GVRP: Set to **Disabled** unless you are configuring the AP to support VLANs, as described in **“Configuring for VLANs” on page 5-40**.

   CDP: This setting is Auto Enabled by default in LAN-to-LAN mode. To change this setting, refer to **“Setting the Cabletron Discovery Protocol” on page 5-21**.
2. Choose **Save**.
3. Choose **Wireless Configuration** from the Main Menu, then choose **Set/Show Wireless Configuration**.
4. At the top of screen, select the radio slot (1 or 2) to configure.
5. Enter the wireless parameters.
6. Set the **Reset Option** to **Reset Radio if necessary** (default setting).
7. Choose **Save**.
8. If changing the bridge mode, you need to implement your changes by choosing **Reset/Upgrade** in the Main Menu then choosing **Reset Switch**. Allow approximately one minute for the AP to reset and complete its self-test.

Refer to the other sections in this chapter to configure features such as encryption and filters.

Using the Access Point 2000 Console Port

To use the console port, follow the instructions in **"Connecting a Device to the Console Port" in Appendix B**. Use **Help** in the console screens for a description of any field.

1. Choose **Set IP Address** from the Installation Menu.
2. Enter the IP address, subnet mask, and default gateway.
3. Choose **Module-Specific Options** from the Installation Menu.
4. Choose **Set Wireless Configuration**. Enter the wireless parameters for your wireless network.
5. Select **Bridge Mode Options** from the Module-Specific Options menu and continue entering the wireless parameters.
6. Optionally, you can enable console security as follows:
   - a) From the Installation Menu, choose **Enable/Disable Console Password**. Set to Enable.
   - b) Select **Set SNMP Read/Write Community** from the Installation Menu. Enter a new community name (4 to 31 printable ASCII characters). Users must enter the community name to access the menu.
7. To implement your changes, reset the AP by selecting **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the AP to reset and complete its self-test.
8. Perform this procedure on the other APs.

Refer to the other sections in this chapter to configure features such as authentication and filters.

Viewing Current AP Settings

You can view the current settings before you modify the RoamAbout AP parameters.

Using the AP Manager

Using the AP Manager, select the AP from the **Managed List** field and click the various buttons, such as **Wireless Parameters**, **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 AP, both the operating (current) settings and the settings that take affect after the next reset are displayed.

Using the RoamAbout R2 Console

- Choose **Current Configuration** from the Main Menu to view the network and hardware parameters.
- To display the current wireless settings, choose **Wireless Configuration** in the Main Menu, then choose **Set/Show Wireless Configuration**. If you have changed a wireless parameter but not yet reset the AP, the new setting is NOT reflected in this display.

Using the Access Point 2000 Console

- Choose **Show Current Settings** from the Installation Menu to view the network and hardware parameters.
- 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 AP, the new setting is NOT reflected in this display.

Modifying the IP Address

The AP can obtain an IP address using these methods:

- **BootP** (default): The AP obtains its IP Address from a BootP server when it reboots. A BootP server must be configured in advance to respond with the desired IP address.
- **DHCP**: The AP obtains its IP address from a DHCP server. This option is not recommended for enterprise networks.
- **Manual**: Prevents the AP from issuing BootP or DHCP requests to obtain an IP address. Use this setting if the AP was already assigned an IP address and you do not want to change it.

Using the AP Manager

You can use the AP Manager to change the IP address using a BootP or DHCP server. You also have the option to manually change the IP address of an Access Point or Access Point 2000. To only modify the subnet mask or default gateway, select the AP from the **Managed List** field and click the **Network Parameters** button. A reset is not needed.

To change the AP’s current IP address using BootP or DHCP, perform the following:

1. Select the AP from the **Managed List** field.
2. Click the **Network Parameters** button and set the following parameters:

   Address State: Set to **Volatile**. The address state options are inactive if this parameter was disabled using the console port. This setting is not used on a RoamAbout R2.

   IP Address Initialization: Set to DHCP or BootP to automatically assign an IP Address to the AP after the reset.
3. Click **OK**.
4. In the AP Manager main window, click the **Reset** button. Then click **Reset with Current Settings**. The AP is reset and uses the selected method to obtain an IP address.

When done, you may need to delete the AP with the old IP address from the managed list.

To manage the AP with the new IP address with AP Manager, use the **Setup/Add New AP** button from the main window or use **Selection→Discover** from the menu bar.

To manually change the IP address of an Access Point or Access Point 2000, perform the following. You will need the AP's wired MAC address and an unused IP address.

1. Select the AP in the managed list.
2. Click on the **Network Parameters** button.
3. Set the **Address State** to **Volatile**.
4. Select **Manual** from the IP Address Initialization option.
5. Click **OK**.
6. In the main AP Manager window, click the **Reset** button. Then, click **Reset with Current Settings**.
7. Click the **Setup/Add New AP** button from the main window.
8. Click **Yes** in the Load IP Address message.
9. In the Load IP Address dialog, enter the wired MAC address, new IP Address, and other parameters as necessary.
10. Click **OK**.
11. If a message appears about reloading an R2, click **OK** to close the message and continue loading the new address.

Using the RoamAbout R2 Console Port

1. Choose **Network Configuration** from the Main Menu and enter the following parameters:

   IP address: If manually entering an IP address, enter the IP address you wish to assign to the AP.

   Subnet mask: Enter the subnet mask you wish to assign to the AP.

   Default gateway: Enter the IP address of the default gateway.

   IP Address Mode: Set to Manual, DHCP, or BootP. The AP uses this method to obtain an IP address on the next reset.

2. Choose **Save**. You do not need to reset the AP.

Using the Access Point 2000 Console Port

To manually enter an IP address, and disable both BOOTP and DHCP, go to **Set IP Address** in the Main Menu and enter an IP address. A reset to the AP is not needed.

To change how the IP address is obtained, perform the following:

1. Choose **Module-Specific Options** from the Main Menu.
2. Choose **Choose BOOTP or DHCP to get IP Address**.
3. Enable DHCP or BOOTP. The AP obtains an IP address on the next reset.

__NOTE__: If the AP has an IP address and you wish to enable DHCP or BOOTP, you must first go to __Set IP Address__ and set the IP address to 0.0.0.0.

To modify only the subnet mask or default gateway, go to the **Set IP Address** in the Main Menu.

Setting the Cabletron Discovery Protocol

The Cabletron Discovery Protocol (CDP) allows other devices (Cabletron/Enterasys) with CDP to discover the RoamAbout R2 in the network topology.

- **Auto enabled** (the default setting). The RoamAbout R2 sends out one CDP packet at startup, and only transmits further CDP packets after receiving CDP packets from another device.
- **Enabled**. The RoamAbout R2 always sends out CDP packets.
- **Disabled**. The RoamAbout R2 never sends out a CDP Packet.

__NOTE__: CDP is automatically disabled on the wireless port when the RoamAbout R2 is in Workgroup mode.

Using the AP Manager

Click on the **Network Parameters** button in the main window.

Using the RoamAbout R2 Console Port

Choose **Network Configuration** from the Main Menu.

Modifying Wireless Parameters

The following AP wireless parameters can be modified as necessary:

- **AP Density**: Should only be changed when APs are moved closer or further apart from each other. This parameter is only available when the AP is in Workgroup bridge mode. See **AP Density and Roaming on page 2-8** for more information.
- **Transmit Rate**: The transmit rate can be changed between the auto rate and fixed rate options to accommodate a changing wireless network, such as a larger coverage area or all clients were upgraded to a faster PC card. The transmit rate can also be changed to accommodate the addition or reduction of noise in the coverage area. For more information, see **"Transmit Rate" on page 2-5**.

  ***NOTE**: Enterasys Networks recommends that you use an xx Mbit/s Auto rate setting.*

  If using a fixed rate of 11 or 5.5 Mbit/s on the AP, any clients with 2 Mbit/s PC Cards will not be able to communicate with the AP.

- **RTS Threshold**: Should only be used to address frame collisions and lost messages in the wireless network. If necessary, set the RTS Threshold to **500** to reduce or eliminate collisions at the AP. See **"RTS/CTS Protocol" on page 2-9**.

  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**.

- **Remote RTS Threshold**: Should only be enabled to address a hidden station problem, as described in **"RTS/CTS Protocol" on page 2-9**. This parameter is only available on a RoamAbout R2 in Workgroup bridge mode.
- **DTIM**: This is the only configurable AP Power Management parameter. It is only available when the AP is in Workgroup bridge mode. In nearly all environments, you should not change the default DTIM of 1. See **"802.11 Power Management" on page 2-11**.
- **Secure Access**: When enabled, this prevents clients without the correct wireless network name from connecting to this AP. It is only available when the AP is in Workgroup bridge mode.
- **Multicast Transmit Rate**: Identifies the desired transmission speed for the broadcast and multicast traffic as forwarded by the AP to the wireless LAN. You should use the lowest speed that you want to support. If using applications that use multicast traffic (for example, IGMP), you can increase this rate from the default of 2 Mbit/s Fixed.

- **IntraBSS Relay**: When enabled, it allows wireless users associated with an AP to see and communicate between each other. This is accomplished by taking a multicast packet from one wireless user and rebroadcasting it so that all wireless users see it.

  When disabled, it prevents communication between users associated with an AP. This mode is intended for use in the ISP market where the ISP does not want separate households to browse the Network Neighborhood and see other customers and their hard drives.

- **Medium Density Distribution**: When enabled, the AP distributes its AP Density (low, medium, high, minicell, microcell) to the clients. It is only available when the AP is in Workgroup bridge mode. This setting is always enabled on the AP 2000 (firmware V6.04 or higher).

- **Load Balancing**: This parameter forces wireless clients to associate with APs that are least busy, resulting in a more even distribution of client associations between APs. Load balancing increases the network's overall throughput. Load balancing is enabled by default. It is only available when the AP is in Workgroup bridge mode. This setting is always enabled on the AP 2000 (firmware V6.04 or higher).

- **Wireless Relay**: Enable to allow the endpoint APs to communicate with each other through the Central AP, or Disable to only allow the endpoint APs to communicate with the Central AP and its wired LAN. This feature is only available on an Access Point 2000 managed by the AP Manager when the AP is in Point-to-Multipoint bridge mode.

Using AP Manager

To modify a wireless parameter using the AP Manager, select the AP from the **Managed List** field and click the **Wireless Parameters** button. To see all the wireless parameters, click the **Advanced** button. Use the **Help** button for a detailed description of each parameter.

Using the RoamAbout R2 Console Port

To modify a wireless parameter using the console port, choose **Wireless Configuration** from the Main Menu, then choose **Set/Show Wireless Configuration**. The console port does not support the Remote RTS Threshold, Medium Density, and Load Balancing parameters.

Using the Access Point 2000 Console Port

To modify a wireless parameter using the console port, choose **Module-Specific Options** from the RoamAbout AP Installation Menu. From the module-specific menu, choose **Set Wireless Configuration**. The console port does not support the Medium Density, Load Balancing, and Wireless Relay parameters.

Configuring for 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.
- Create a unique Wireless Network Name and enable Secure Access at the APs.
- Configure the APs to not communicate with unencrypted clients.
- Enable console port security.
- Use the RADIUS authentication services to configure the AP as a RADIUS client.

  For the Access Point 2000, create a custom AP RADIUS Management Authenticator. The R2 uses SNMP v3 and, therefore, does not support the Management Authenticator.
- Use 802.1X Authentication with rapid rekeying.

  If rapid rekeying is not available, enable encryption and configure clients that you want to be in the network with the proper encryption keys. 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 AP. When Secure Access is enabled, the AP denies access to wireless clients that do not use the correct wireless network name. When Secure Access is disabled, the AP allows access to wireless clients that use **ANY** (all uppercase) as the wireless network name or have a blank wireless network name.

Using the AP Manager

Click the **Wireless Parameters** button then click the **Advanced** button. Use the **Help** button for detailed information. A reset is not needed.

Using the RoamAbout R2 Console Port

Choose **Wireless Configuration** from the Main Menu, then select **Set/Show Wireless Configuration**. A reset is not needed.

Using the Access Point 2000 Console Port

Choose **Module-Specific Options** from the RoamAbout AP Installation Menu, then choose **Set Wireless Configuration**. A reset is not needed.

Setting Encryption

Before configuring encryption on the AP, create the encryption keys as follows:

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.

Using the AP Manager

To configure encryption using the AP Manager, perform the following:

1. In the main window, select the AP in the Managed List.

2. Click the **Encryption** button.

   Selected Slot (RoamAbout R2 only): 1 or 2

   Enable Encryption: Enable (add a check to the checkbox).

   Deny Non-encrypted Data: Optionally, enable to prevent the AP from communicating with clients that do not use encryption.

   Keys: Enter up to four encryption keys.

   Encrypt Data Transmissions: Choose a transmit key by selecting that key in the field.

3. Click **OK** to accept the parameters.

4. When prompted, click **OK** to reset the AP. Allow approximately one minute for the AP to reset and complete its self-test. You do not need to reset the AP if you only add, delete, or modify keys, or change the transmit key.

Using the RoamAbout R2 Console Port

To configure encryption using the RoamAbout R2 console port, perform the following:

1. Choose **Wireless Configuration** from the Main Menu.
2. Choose **Encryption Configuration**.

   Radio Slot: 1 or 2

   Encryption State: Enable

   Keys: Enter up to 4 encryption keys.

   Transmit Key ID: Select the Key number that you want the RoamAbout R2 to use when transmitting data.

   Exclude Unencrypted:

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

   — Disable 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.

   Transmit Key ID: Select the Key number that you want the RoamAbout R2 to use when transmitting data.

   Reset Option: Set to **Reset Radio if necessary** (default setting).
3. Choose **Save**.
4. Choose **Reset/Upgrade** from the Main Menu, then choose **Reset Switch**. You do not need to reset the AP if you only add, delete, or modify keys, or change the transmit key. Allow approximately one minute for the AP to reset and complete its self-test.

Using the Access Point 2000 Console Port

To configure encryption using the console port, perform the following:

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.
2. Choose **Set Encryption Configuration**.

   Set Encryption Key: Use these menu options to enter the keys.

   Set Transmit Key ID: Choose one key to be the transmit key. Each AP can use a different transmission key as long as the other devices have that key entered in the same position.

   Set Exclude Unencrypted: Only valid if the AP is configured for a wireless infrastructure network.

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

   — Disable 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.

   Set Encryption State: Enable encryption.
3. To prevent any management tool using SNMP, including the AP Manager, from changing the encryption parameters, enable the **Set Exclude SNMP** menu option.
4. Select **Reset with Current Settings** from the RoamAbout AP Installation Menu. You do not need to reset the AP if you only add, delete, or modify keys, or change the transmit key. Allow approximately one minute for the AP to reset and complete its self-test.

Configuring the Console Port for Security

For the AP 2000, the AP Manager and any other SNMP Manager must have the correct read/write community name associated with the AP; otherwise, the tool cannot make any changes to the AP.

For the R2, the AP Manager and any other SNMP Manager must have the correct Authentication and Privacy passwords.

AP Manager

For the AP 2000, the AP Manager can change both the read-only and read/write SNMP community names. To change the read-only community name on the AP 2000, select the **Network Parameters** button in the main window. To change the read/write community name on the AP 2000, click on the **Options** menu and select **SNMP Security**. Click the **Help** button for detailed information.

For the R2, the AP Manager can change the SNMPv3 Authentication and Privacy passwords. Click on the **Options** menu and select **SNMP Security**. Click the **Help** button for detailed information.

RoamAbout R2 Console Port

The following security settings are available from the console port:

- Access to the console requires a password. The username is **admin** and the default password is **password**. The password must be a minimum of eight ASCII characters, and is case-sensitive. The same username and password is used for Telnet and web management. To change the password, choose **Serial/Telnet/Web Configuration** from the Main Menu.
- You can disable Telnet and web management from the console port. Choose **Serial/Telnet/Web Configuration** from the Main Menu.

Access Point 2000 Console Port

The following security settings are exclusive to the console port:

- To prevent other users from using the console port, enable **Enable/Disable Console Password** from the Installation Menu. 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.

Configuring the R2 for SNMPv1 or SNMPv2

The RoamAbout R2 supports SNMPv3. To support management tools using SNMPv2 or SNMPv1, the R2 provides four community names that allow SNMPv1 and SNMPv2c read-only and read-write access. The names are disabled by default with the exception of Community Name #1, which is set to **public**. The community names are only accessible from the R2 console port. The community names and descriptions are:

- Community Name #1: Allows access to the read-only MIB II system group.
- Community Name #2: Allows creation of new views, and provides read-write access to tmsCommonCommunityToViewTable.
- Community Name #3: Allows read-only access to the full MIB view.
- Community Name #4: Allows read-write access to the full MIB view.

To disable a Community Name, enter **disable** and the community name number in the field. For example, enter **disable2** in the Community Name #2 field.

NOTE*: It is recommended that Community Name #1 remain at its default setting of* ***public****.*

Perform the following to change the community names:

1. Choose **Security and Policy Configuration** from the Main Menu.
2. Choose **Communities**.
3. To only have the RoamAbout AP Manager manage the R2 using SNMPv3, set Community Name #1 to **public** and disable the other community names.
4. To support systems using SNMPv2 or SNMPv1, choose which access you wish to allow the network management systems. Enter a unique name for each of those Community Names. Disable any Community Name to prevent access to that function.
5. Choose **Save**. You do not need to reset the AP.

Configuring the AP for Authentication

Authentication uses a RADIUS server to authenticate wireless clients in a wireless infrastructure network. Refer to **Authentication on page 2-14** for a description of the types of authentication. The following lists the basic tasks to configure for authentication:

- Configuring a RADIUS server (not described in this document)
- Configuring the AP as a RADIUS client and choosing the type of authentication

  The AP 2000 has the option of using the default RADIUS Management Authenticator or creating a custom authenticator. The R2 uses SNMPv3 instead of a Management Authenticator.
- Configuring for Rapid Rekeying (optional, if MAC address or hybrid authentication is not used)

RADIUS Management Authenticator (AP 2000 Only)

The AP RADIUS Management Authenticator security feature allows you to specify an authenticator that encrypts the SNMP Objects used between the AP Manager and the Access Point 2000 for management of critical RADIUS client parameters. You can enter a custom RADIUS Management Authenticator, or use the AP's default RADIUS Management Authenticator. The Management Authenticator can be changed at anytime.

NOTE*: When you enter a custom authenticator, you are prompted for a password. After you enter the password, only those with the password can access the custom RADIUS Authenticator.*

If you reset to factory defaults, the AP RADIUS Management Authenticator is cleared and reset to the default. To view the AP RADIUS client parameters, you must restore the default RADIUS client management authenticator in the AP.

Using the AP Manager

To enter a custom RADIUS Management Authenticator on the Access Point 2000 using the AP Manager, perform the following steps:

1. Click on the **Authentication** button in the RoamAbout AP Manager main window.
2. Click on the **Change Authenticator** button. The RADIUS Client Management Authenticator dialog box appears.
3. Click on the **Custom** radio button.

4. Enter the Custom Authenticator. The format is 16 printable ASCII characters, or 32 hexadecimal digits preceded by **0x**.

5. Click **OK**.

   After you enter a custom authenticator, you are prompted to enter a password. Once you set the password, only those with the password can access the custom RADIUS authenticator. If this is the first time entering a Custom Authenticator, the RADIUS Client Management Password dialog box appears.

6. Enter the New Password.

7. Enter the password in the **Confirm New Password** field.

8. Click **OK**.

To change the password using AP Manager, perform the following steps:

1. Click on the **Change Password** button in the Authentication dialog box.

2. Enter the RADIUS Management Authenticator password in the **Old Password** field.

3. Enter the new password in the **New Password** field, and in the **Confirm New Password** field.

4. Click **OK**.

Using the Access Point 2000 Console Port

To enter a custom RADIUS Management Authenticator using the console port, perform the following:

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.

2. Choose **RADIUS Client Options**. The RADIUS Client Options menu appears.

3. Choose **Configure RADIUS Client Parameters**.

4. Choose **Enter RADIUS Client Management Authenticator** to enter a custom AP RADIUS Management Authenticator. The format is 16 printable ASCII characters, or 32 hexadecimal digits preceded by 0x.

5. Choose **Save**.

***NOTE**: If you use the AP Manager after you set the Authenticator in the console, you must set the AP RADIUS Management Authenticator to match the Authenticator you set in the console.*

Configuring the AP for Authentication

Before you can configure the AP as a RADIUS client, you must choose the type of authentication to use: MAC address, 802.1X, or both. Also, you need to have the following RADIUS server information available:

- **Primary Server IP Address**: IP Address of the primary RADIUS authentication server. The IP Address must be an IP Version 4 address.
- **Secondary Server IP Address**: IP Address of the secondary RADIUS authentication server, if used. The IP Address must be an IP Version 4 address. If you are not using a secondary RADIUS server (as a backup server), enter 0.0.0.0 or leave it blank.
- **Primary Authentication Port**: A value between 1 and 65535. Standard values are 1812 (default) and 1645. This value must match the primary RADIUS Server configuration.
- **Secondary Authentication Port**: A value between 1 and 65535. Standard values are 1812 (default) and 1645. This value must match the secondary RADIUS Server configuration, if used.
- **Shared Secret**: The text string that ensures that the data exchanged between the server and the AP is valid. The shared secret must match the corresponding entry for the AP in the RADIUS Server database.
- **Retry Limit**: Valid range is 0 to 20 times. Default is 5.
- **Retry Timer**: Number of seconds between retries. Valid range is 2 to 10 seconds. Default is 5 seconds.

If using MAC Address or hybrid authentication, you must provide the MAC address of your wireless client (PC) to the Network Administrator.

NOTES

NOTE**: User names (MAC Addresses) are case-sensitive (lower-case), and in the format:* ***00-e0-63-ab-ce-ef

If possible, configure the RADIUS server to authenticate the user without checking a password. Otherwise, use a password of "NOPASSWORD" for all of the MAC Address based user names.

If using 802.1X or hybrid authentication, you need the following 802.1X parameter settings:

- **Reauthentication**: When enabled, authenticates 802.1X clients at regular intervals. When disabled, clients are only authenticated once.

- **Time Between Reauthentications**: Time, in minutes, between each reauthentication when Reauthentication is enabled. The default is 60 minutes.
- **Hold Period After Failed Login**: Time, in seconds, after a login failure before the device can restart the authentication procedure. The default is 60 seconds. A login failure is when a device tries to log in and fails authentication twice consecutively.
- **Identity Request Timeout**: Time allowed before the client's identity times out. The default is 60 seconds.
- **Challenge Request Timeout**: Time allowed before the client challenge request session is terminated. The default is 30 seconds.
- **Challenge Request Retry Limit**: Number of allowed retries before ending the client session. The default is 2.
- **Server Timeout**: Time for the server to timeout. The default is 30 seconds.
- For an AP 2000 only, you need a valid 802.1X Activation Key to enable 802.1X authentication (purchased separately). Contact your Enterasys Representative.

Using the AP Manager

1. Click on the **Authentication** button in the RoamAbout AP Manager main window.

   Selected AP: Select the AP that you want to configure for authentication.

   Authentication Options: Choose the slot (slot 2 is for RoamAbout R2 only) and the type of authentication, MAC or 802.1X. For hybrid authentication, choose both.

   802.1X Activation Key (AP 2000 only): Enter the alphanumeric activation key (dialog appears when you select 802.1X authentication).

2. Enter the RADIUS client information.

3. If 802.1X authentication was selected, click the **802.1X Parameters** button and enter the 802.1X settings. If Rapid Rekeying was enabled, enter the settings as described in **"Configuring for Rapid Rekeying" on page 5-36**. Click **OK** to apply the changes.

4. Click **OK** in the Authentication dialog.

5. If you enabled MAC or 802.1X authentication, perform the following to implement your changes. If only changing RADIUS or 802.1X parameters, a reset is not needed.

   R2 AP: Select **Reset** from the main window. Select **Reset Slot x**, where x is the slot (1 or 2) you configured.

   AP 2000: If prompted, reset the AP. Otherwise, select **Reset** from the main window. Select **Reset with Current Settings**.

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

Using the RoamAbout R2 Console Port

1. Choose **Security and Policy Configuration** from the Main Menu.
2. Choose **RADIUS Client Configuration**.

   RADIUS: Enable. The RADIUS Client Parameters screen appears.
3. Enter the RADIUS client information.
4. Choose **Save**.
5. Choose **Authentication Configuration** from the **Security and Policy Configuration** menu.

   Authentication Configuration Slot: 1 or 2

   Authentication Mode: Choose **MAC**, **802.1X**, or **Hybrid** (MAC and 802.1X).
6. If 802.1X or hybrid was selected, enter the 802.1X parameters. Optionally, configure **Rapid Rekeying**. See **"Configuring for Rapid Rekeying" on page 5-36**.
7. Choose **Save**.
8. If you enabled MAC or 802.1X authentication, perform the following to implement your changes. If only changing RADIUS or 802.1X parameters, a reset is not needed.

   a) Choose **Reset/Upgrade** from the Main Menu.

   b) Choose **Reset Radio**.

      Slot: Choose Radio 1 or Radio 2.

      Reset Option: Set to **Reset Radio Regardless**.

   c) Choose **Apply**.

To view the RADIUS client statistics, see **"Monitoring RADIUS Client Operations" on page 6-11**.

Using the Access Point 2000 Console Port

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.

2. Choose **Authentication Options**.

3. Choose **Configure RADIUS Client**.

4. Choose **Enable/Disable RADIUS Authentication**. Enable this setting.

5. In the Configure RADIUS Client Parameters menu, choose **Enter All RADIUS Client Parameters**.

6. Enter all the RADIUS client parameters.

   You can use **Change Radius Client Parameters** to change a parameter, or **List RADIUS Client Parameters** to view current RADIUS settings. To view RADIUS client statistics, see **"Monitoring RADIUS Client Operations" on page 6-11**.

7. In **Authentication Options** menu, choose **Configure Wireless Authentication Type**.

8. Choose the type of authentication:

   None: Disables all authentication types.

   MAC address-based Authentication: Enables MAC-address authentication. Disables 802.1X authentication.

   802.1X Authentication: Enables 802.1X authentication. Disables MAC-address authentication and Rapid Rekeying.

   802.1X Authentication with Rapid Rekeying: Enables 802.1X authentication and Rapid Rekeying. Disables MAC-address authentication.

   Hybrid 802.1X/MAC-based Authentication: Enables both 802.1X and MAC-address authentication. Disables Rapid Rekeying.

9. If you enabled any 802.1X authentication option, you are prompted for the activation key. Afterwards, go to the Authentication Options menu and choose **Configure IEEE 802.1X Parameters**. Enter the 802.1X parameters. Optionally, choose **Apply Settings to Current Supplicants** to immediately send the changes to the clients.

10. If Rapid Rekeying was enabled, see **"Configuring for Rapid Rekeying" on page 5-36** to enter the parameters.

11. If you enabled or disabled any authentication, select **Reset with Current Settings** from the Installation Menu to implement your changes. If only changing RADIUS or 802.1X parameters, a reset is not needed.

Configuring for Rapid Rekeying

To use Rapid Rekeying, you must set up the AP for 802.1X authentication, as described in **Configuring the AP for Authentication on page 5-30**. Rapid Rekeying must be configured on the AP and the wireless clients. The following lists the Rapid Rekeying parameters:

- **Time Between Key Changes (or Rekeying Period)**: This is the interval, in minutes, that the AP waits before starting a new key sequence. Time can be 1 to 525600 minutes. Default is 10 minutes.
- **Key Length**: **40** or **128 bit** depending on the WEP encryption supported by the PC Card.
- **Separate Transmit and Receive Keys**: Select **Enabled** to use different encryption keys for transmit and receive, or **Disabled** to use the same encryption key for both transmit and receive.

Using the AP Manager

To set up Rapid Rekeying using the RoamAbout AP Manager, perform the following steps:

1. Click on the **Authentication** button in the AP Manager main window.
2. Select the AP from the drop-down list.
3. Select **Rapid Rekeying** (Slot 1 or 2) (**802.1X** should already be selected.)
4. Click the **802.1X Parameters** button.
5. Enter the Rapid Rekeying parameters.
6. Click **OK** to apply the changes. There is no need to reset the AP.

Using the RoamAbout R2 Console Port

To set up Rapid Rekeying using the RoamAbout R2 console port, perform the following:

1. Choose **Server and Policy Configuration** from the Main Menu.
2. Choose **Authentication Configuration**. (802.1X should already be configured.)
3. Select the **Authentication Configuration Slot** (1 or 2).
4. Set **Rekeying** to **Enabled**.
5. Enter the Rapid Rekeying parameters.
6. Choose **Save**. There is no need to reset the AP.

Using the Access Point 2000 Console Port

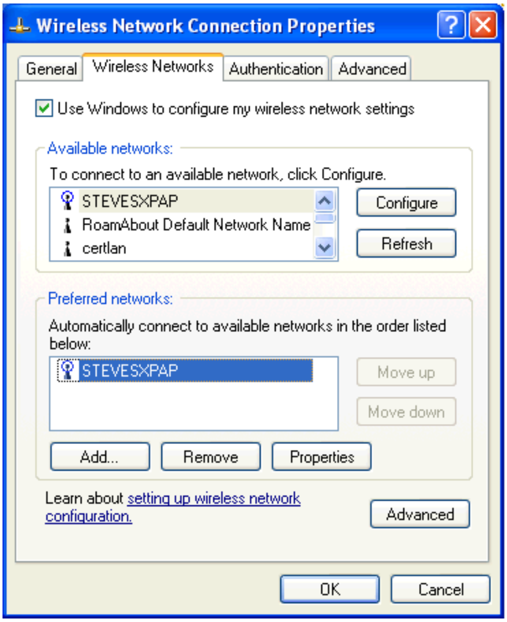
To set up Rapid Rekeying using the console port, perform the following steps:

1. Choose **Module-Specific Options** from the Installation Menu.
2. Choose **Authentication Options**.
3. Choose **Configure Wireless Authentication Type**.
4. Choose **802.1X Authentication with Rapid Rekeying**.
5. Enter the 802.1X activation key, then enter the 802.1X parameters as described in **"Configuring the AP for Authentication" on page 5-32**.
6. Choose **Configure Rapid Rekeying Parameters** from the **Authentication Options** menu.
7. Enter the Rapid Rekeying parameters.
8. Choose **Save**. There is no need to reset the AP.

Set Up Rapid Rekeying on the Clients

This section describes how to set up Rapid Rekeying on a Windows XP client. For more information, refer to the Release Notes or the Readme file that came with the RoamAbout PC Card driver.

1. Open the Control Panel by selecting **Start→Programs→Control Panel**.
2. In the Control Panel, open **Network Connections** then open the **Wireless Network Connection (RoamAbout 802.11 DS)**.
3. In the Wireless Network Connection Status window, click on the **Properties** button.
4. In the Wireless Connection Properties window, click on the **Wireless Networks** tab.
5. If the Wireless Network Name you want to configure is in the **Preferred Networks** field of the Wireless tab (shown below), click on the name then click the **Properties** button. Otherwise, click on the Wireless Network Name in the **Available Networks** field, then click on the **Configure** button.



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

STEVESXPAP
RoamAbout Default Network Name
certlan

Preferred networks:

Automatically connect to available networks in the order listed below:

STEVESXPAP

Learn about setting up wireless network configuration.

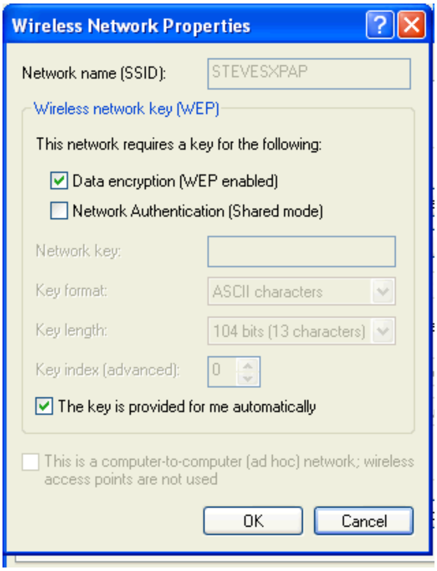
6. In the Wireless Network Properties window (shown below), select the following:

   a) Check the box marked **Data encryption (WEP enabled)**.

   b) Check the box marked **The Key is provided for me automatically**.

   c) Un-check any other checked boxes.

   d) Click **OK** to apply the changes.



Wireless Network Properties

Network name (SSID): STEVESXPAP

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

□ Network Authentication (Shared mode)

Network key:

Key format: ASCII characters

Key length: 104 bits (13 characters)

Key index (advanced): 0

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

7. Click **OK**, or **Close**, to close all open windows.

Configuring for VLANs

The RoamAbout AP supports the forwarding of tagged VLAN data. The RoamAbout R2 can be configured to forward VLAN data to specific endpoints. The Access Point 2000 can only be configured to forward or not forward VLAN data. When forwarding VLAN data, the Access Point 2000 forwards to all endpoints.

NOTE

***NOTE**: VLAN 1 is a default VLAN used by the R2 to allow pass-through of untagged data. Changing the VLAN 1 default settings could prevent the AP from forwarding untagged data.*

To configure a VLAN, define the VLAN and configure each port to handle data as follows:

- **Tagged**: The port forwards all incoming data from a defined VLAN, where the incoming data is tagged.
- **Untagged**: The port forwards all incoming tagged data from a defined VLAN; however, the port removes the VLAN ID from the outgoing frames. This feature should only be used when the transmitting port is connected to a device in the network that does not support VLANs.
- **Forbidden**: The port does not forward any data from a defined VLAN.
- **None**: The port does not forward any data from a defined VLAN (default setting). This setting can only be configured manually and can be overridden by GVRP.

***CAUTION**: If you change the bridge mode to Workgroup after setting up VLANs, all VLAN configurations belonging to that membership will be deleted with the exception of the default VLAN. All tagged ports will be cleared.*

Ports are displayed according to the Remote Wireless MAC addresses you set up for the RoamAbout R2 configuration. In the LAN-to-LAN Multipoint configuration, the ports are assigned according to the wireless MAC Addresses you entered in the Multipoint Properties dialog box. The ports are defined as follows:

- Port 1: The 10/100 Ethernet Port.
- Port 2: R2 Slot 1 if the slot is in LAN-to-LAN Endpoint mode.
- Ports 2 through 7: R2 Slot 1 if the slot is in LAN-to-LAN Multipoint mode. These ports correspond to Remote Wireless MAC Addresses 1 through 6, as displayed in the Multipoint Properties dialog box.
- Port 8 (with the R2 Mezzanine option): R2 Slot 2 if the slot is in LAN-to-LAN Endpoint mode.

Using the AP Manager

Click on the **VLANs** button in the main window. Refer to the RoamAbout AP Manager online help for more information. A reset is not needed to implement VLAN changes.

To create a VLAN (RoamAbout R2 only):

1. Click the **Create VLAN** button.

   VLAN ID: Enter the ID of the VLAN. The R2 supports VLAN IDs 2-2047.

   VLAN Name: Enter the name of the VLAN.

   Port Constraints: Configure each port for Tagged, Untagged, Forbidden, or None.
2. Click **OK**.

To modify a VLAN (RoamAbout R2 only):

1. Select the VLAN ID and click the **Modify Selected VLAN** button.

   VLAN Name: Enter the name of the VLAN.

   Port Constraints: Configure each port for Tagged, Untagged, Forbidden, or None.
2. Click **OK**.

To delete a VLAN (RoamAbout R2 only):

1. Select the VLAN ID and click the **Delete Selected VLANs** button.
2. Confirm the deletion.

To enable or disable GVRP (RoamAbout R2 only):

1. Click the **VLAN Parameters** button.
2. Enable or disable GVRP.
3. Click **OK**.

To enable or disable VLAN compatibility on the AP 2000:

1. Click the **VLAN Parameters** button.
2. Enable or disable **Allow Tagged Packets**.
3. Click **OK**.

Using the RoamAbout R2 Web Management

To access the VLAN configuration pages, click on the **VLANs/Multicast Groups** folder.

Using the RoamAbout R2 Console Port

The R2 console port/Telnet interface does not support configuring VLANs. However, you can enable or disable GVRP as follows. A reset is not needed to implement VLAN changes.

1. Choose **Network Configuration** from the Main Menu.
2. Enable or disable **GVRP**.
3. Choose **Save**.

Using the Access Point 2000 Console Port

A reset is not needed to implement VLAN changes.

1. Choose **Module-Specific Options** from the Installation Menu.
2. Choose **VLAN Options**.

   Set VLAN Compatibility Mode: Enable to forward VLAN data. Disable to not forward VLAN data.
3. Choose **Save**.

Setting Spanning Tree

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 AP Spanning Tree function corrects this type of problem by shutting down the port and possibly shutting down a segment of the network.

Typically, Spanning Tree is disabled when in Workgroup bridge mode and enabled in LAN-to-LAN Multipoint bridge mode.

Using AP Manager

To enable or disable Spanning Tree using the AP Manager, select the AP from the **Managed List** field and click the **Wireless Parameters** button. In the Wireless Parameters window, click the **Advanced** button. To implement your changes:

- **R2 AP**: Select **Reset** from the main window. Select **Reset Slot x**, where x is the slot (1 or 2) you configured.
- **AP 2000**: Select **Reset** from the main window. Select **Reset with Current Settings**.

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

Using the RoamAbout R2 Console Port

Choose **Network Configuration** from the Main Menu. Enable or disable Spanning Tree. To implement the change, select **Reset/Upgrade** from the Main Menu then select **Reset Radio**. Allow approximately one minute for the AP to reset and complete its self-test.

Using the Access Point 2000 Console Port

You can enable or disable the Spanning Tree when in Endpoint bridge mode. Spanning Tree is disabled when in Workgroup bridge mode and enabled in Multipoint bridge mode. To enable or disable Spanning Tree using the console port, perform the following:

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.
2. Choose **Bridge Mode Options**.
3. Select **Set Spanning Tree Mode** and set to Enabled or Disabled.
4. To implement your changes, reset the AP by selecting **Reset with Current Settings** from the Installation Menu. Allow approximately one minute for the AP to reset and complete its self-test.

Filtering Traffic by Protocols

You can configure the AP to NOT forward specific protocol traffic to the wireless network. This could 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.

To select the protocol to filter using the AP Manager, perform the following steps:

1. Click on the **Filtering** button in the main window to access the Filtering Dialog Box.
2. Click on the **Protocol** tab.
3. For a RoamAbout R2, select the slot (1 or 2).
4. Select the protocols to filter, as described in **Table 5-1**. Only the filters supported by the selected AP are available. The filters are enabled when they are checked, meaning that traffic of the protocol specified is NOT forwarded by the AP.
5. Click **OK** to implement your change. The AP does not need to be reset.

If you select one or more protocols, the AP Manager applies those changes to ALL of the APs selected in the Managed List field in the main window. The AP Manager prompts you for confirmation before changing the parameters on multiple APs.

Table 5-1: Protocols to Filter

Protocol	Description
IP V4	Does not forward IP version 4 packets carried in Ethernet V2 frames or IEEE 802.3 frames with Logical Link Control (LLC)/Subnetwork Access Protocol (SNAP) headers. Also, the filter does not forward Address Resolution Protocol (ARP) packets carried in Ethernet V2 frames. IP is used in many environments, most notably UNIX networks and the Internet. When enabled, IP, TCP/IP, and UDP/IP packets are not forwarded. This filter should NOT be set if the AP is to be managed from a wireless node.
IPX Ethernet II	Does not forward IPX packets carried in Ethernet V2 frames. Used primarily in NetWare environments.
IPX - 802.2	Does not forward IPX packets carried in IEEE 802.3 frames with LLC headers. Used primarily in NetWare environments.
NetBEUI	Does not forward NetBEUI packets. Used primarily in Microsoft native networking.

Table 5-1: Protocols to Filter(Cont'd)

Protocol	Description
DECnet	Does not forward DECnet packets carried in Ethernet V2 frames or in IEEE 802.3 frames with LLC/SNAP headers. DECnet packets are used primarily in DEC VMS and related networking. If you do not plan to have DECnet clients, you should filter all DECnet traffic.
LAT	Does not forward Local Area Transport (LAT) packets. Used primarily in terminal/server communication.
AppleTalk Ethernet II	Does not forward AppleTalk packets carried in Ethernet V2 frames. Used primarily in Apple native networking.
AppleTalk AARP	Does not forward AppleTalk AARP packets. Used primarily in Apple native networking. The AppleTalk Address Resolution Protocol (AARP) uses broadcasts to discover the hardware address of a node. It is similar to TCP/IP's ARP.
AppleTalk SNAP	Does not forward AppleTalk packets carried in IEEE 802.3 frames with LLC/SNAP headers. Used primarily in Apple native networking.
VAXcluster	Recommended if there are no VAXclusters on the wireless LAN.
802.3 ISO Connectionless DSAP	Recommended if there are no ISO wireless clients on the wireless LAN.
LAN Traffic Monitor	Recommended if there are no bridges on the wireless LAN.
DECnet End Node Hello	Recommended if there are no DECnet routers on the wireless LAN.
IPX Raw	Does not forward IPX packets carried in IEEE 802.3 frames with no LLC.
IPX SNAP	Does not forward IPX packets carried in IEEE 802.3 frames with LLC/SNAP headers.
SNA	Does not forward SNA packets carried in IEEE 802.3 frames with LLC headers.
NetBIOS	Does not forward NetBIOS packets (DSAP and SSAP bytes) carried in IEEE 802.3 frames with LLC headers. The filter does not prevent NetBIOS packets that are using "tunneling" in other protocols such as TCP.
IP V6	Does not forward IP version 6 carried in Ethernet V2 frames or IEEE 802.3 frames with LLC/SNAP headers.

Filtering Traffic by Addresses

You can filter traffic to the network using Address Denied, or you can restrict access to the network using Addresses Allowed. The device can be on either side of the AP (wired or wireless). You identify the device by its MAC address. The maximum number of entries for each AP in the list is 128 entries.

- **Addresses Denied**

  The AP does not forward traffic from a device with its MAC address in the Addresses Denied field. A client in the Addresses Denied list cannot access the LAN, even if the client has been authenticated.

- **Addresses Allowed**

  The AP forwards messages to and from devices identified in the Addresses Allowed List. This filter is essentially ineffective when also using authentication.

To set the filters using the AP Manager, perform the following steps:

1. Click on the **Filtering** button in the main window to access the Filtering Dialog Box.
2. Click on the **Address** tab.
3. For a RoamAbout R2, select the slot (1 or 2).
4. Select **Addresses Denied** or **Addresses Allowed** from the drop-down list, and click on **Selected**.
5. Add the MAC Addresses to the list by clicking on the **Add** button. A pop-up box prompts you for the MAC address of the device.

To remove a device from a list, select the MAC Address and click on the **Remove** button.

The AP Manager updates the list for ALL the APs selected in the Managed List field in the main window. The AP Manager prompts you for confirmation before changing the parameters on multiple APs. The AP does not need to be reset.

Checking the Configuration on Multiple APs

The AP Manager provides integrity tests that check for consistent settings across all the APs in a single group. Use the integrity tests to make sure that the APs 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 APs 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 (AP 2000 only)
  - Same upline dump setting (AP 2000 only)
  - Same forwarding setting
- Values not used in LAN-to-LAN mode are not checked when the AP is in LAN-to-LAN mode.
- The **Firmware Revisions** option verifies that all APs have the same version of the firmware.
- The additional menu item, **Link Test**, is used to test the communications quality between the AP and another wireless device.

Resetting the RoamAbout AP

This section describes how to reset the AP.

- **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 AP to implement your changes.

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

  — From a device attached to the RoamAbout R2 console port, select **Reset/Upgrade** from the Main Menu and then select **Reset Switch**.

  — From a device attached to the Access Point 2000 console port, select **Reset with Current Settings** from the RoamAbout AP Installation Menu.

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

- **Reset with Factory Defaults**

  This option reboots the AP, causing the AP'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 AP from the **Managed List** field, click the **Reset** button, then click the **Reset with Factory Defaults** button.

  — From a device attached to the RoamAbout R2 console port, select **Reset/Upgrade** from the Main Menu, then select **Reset Switch with Factory Defaults**.

  — From a device attached to the Access Point 2000 console port, select **Reset with Factory Defaults** from the RoamAbout AP Installation Menu.

- **Hardware Reload/Reset button**

  — **RoamAbout R2**. The RoamAbout R2 has a reload/reset button. To reset back to the factory defaults you must download a new firmware image from a TFTP server then reset back to factory default values. If an image is not available to download, the RoamAbout R2 resets to its current configuration settings and not back to the factory default values.

  — **Access Point**. The AP hardware has a reload/reset button that forces the AP 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 AP resets to factory default values after approximately three minutes. Make sure that you do not have multiple BootP/TFTP servers configured to load the AP; you might load an incorrect image. Allow approximately one minute for the AP to reset and complete its self-test.

Using the RoamAbout R2 Web Management

For the RoamAbout R2 web management, AP Manager or any Network Management Station to remotely manage the AP, the AP must have a valid IP address and subnet mask. The RoamAbout R2 web management runs on the following browsers:

- Netscape Communicator V4.5, V4.6, V4.7, V6.0 (and later)
- Microsoft Internet Explorer V4.0 and V5.0 (and later)

To manage the RoamAbout R2 using web management, perform the following steps:

1. Open your web browser. Ensure that your web browser configuration is set to **Direct Internet Connection**.
2. Enter the RoamAbout IP Address into the browser URL path.

   You are prompted for the username and password. The default username is **admin** and the password is **password**. The RoamAbout AP Manager management tree appears.
3. Click on the **Network Configuration** web page, then the **Network Parameters** web page.
4. Enter the IP Address, Subnet Mask and the Default Gateway.
5. Click on **Save**.
6. Click on the **Identification** web page.
7. Enter the text to describe the RoamAbout R2.
8. Click on **Save**.
9. Click on the **Wireless Parameters** web page and the **Slot 1** web page.
   a) Enter the name of the wireless network if in Workgroup bridge mode.
   b) Enter a channel. If there are other RoamAbout R2s whose coverage areas overlap, enter a channel that is at least five channels apart from the adjacent R2s.
   c) Enter a station name. The station name is displayed when clients run the RoamAbout Client Utility. Each RoamAbout R2 should have a unique station name.
10. Click on **Save**.

Refer to the online help for more parameter information.

Configuring Clients

To configure the clients, refer to the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide* and the client online help.

Check the enterasys.com/wireless web site frequently for client upgrades and documentation revisions.

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 APs to account for new obstructions or new sources of radio interference. You may also need to add APs should the number of users increase.

In addition, you should regularly check the RoamAbout Wireless web site for product updates.

In This Chapter

Information in this chapter is presented as follows:

Testing Radio Communications Quality

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

Using the AP Manager

The RoamAbout AP Manager provides a Link Test tool that tests the signal quality from the AP to a client or another AP. Click on the **Help** button in any window for more information.

1. From the Windows Taskbar, click **Start**, then select **Programs→RoamAbout→RoamAbout AP Manager**.
2. Select the AP from the **Managed List** field in the AP Manager main window.
3. Click on the **Integrity** drop-down menu and 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 APs in a LAN-to-LAN configuration.
5. Choose the client or AP 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 Signal to Noise Ratio (SNR) is low between the AP 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 in **"Range Extender Antenna" on page 1-17**.

   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 RoamAbout Client Utility

This procedure requires the RoamAbout Client Utility on a RoamAbout client. The RoamAbout Client Utility Link Test window allows you to investigate the specific link between the RoamAbout client and its test partner. Click on the **Help** button in any window for more information.

1. To start the Client Utility, perform the following:

   — Click on the Client Utility icon 📶 located on the System Tray of your Windows Taskbar.

   or

   — From the Windows Taskbar, click **Start**, then select **Programs→RoamAbout→RoamAbout Client Utility**.

2. Click on the **Advanced** drop-down menu and select **Link Test**. The Link Test window has an **Advice** button. Click this button for specific troubleshooting suggestions.

   If you are connected to an infrastructure network, the test partner is the associated AP. If you are configured for an ad-hoc network, you can 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:

   ***NOTE**: You cannot check the SNR if you are in a peer-to-peer (ad-hoc) configuration, the SNR indicator will remain black or gray.*

   — **Green (green color)**. Communications quality is good.

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

   — **Red (red color)**. Communications quality is poor and requires user intervention.

   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 in **"Range Extender Antenna" on page 1-17**.

4. Check the **Total Messages** column. Data throughput efficiency is measured in messages sent, lost, or received.

5. 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.

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 AP 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 AP in an infrastructure network, you may need to lower the RTS Threshold on the AP as described in the **“RTS/ CTS Protocol” on page 2-9**.

If the concentration of users per AP is high, you may need to place the APs closer together to distribute the load, or add APs 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 6-8**.

Optimizing RoamAbout AP Placement

The RoamAbout AP Manager and RoamAbout Client Utility provide diagnostic tools to determine the coverage area of an AP. If you have multiple APs 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 APs, and on a regular basis to determine if the coverage areas change due to new obstructions or new sources of radio interference.

Using the Client Utility

Use the RoamAbout Client Utility Site Monitor window to monitor the radio communications quality with multiple RoamAbout APs simultaneously.

The Site Monitor window only displays the APs within range of the client. If the Site Monitor window does not display all the APs that you expect, the unlisted AP 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.

This procedure requires the RoamAbout Client Utility on a RoamAbout client. This procedure is best performed on a mobile client that you can use to walk through the coverage area of the AP.

To open the Site Monitor window, perform the following steps:

1. To start the Client Utility, perform the following:

   — Click on the Client Utility icon 📶 located on the System Tray of your Windows Taskbar.

   or

   — From the Windows Taskbar, click **Start**, then select **Programs**→**RoamAbout**→**RoamAbout Client Utility**.

2. Click on the **Advanced** drop-down menu and select **Site Monitor**.
3. Select the network in the **Selection** tab if you have multiple wireless networks.
4. For best results, click on the **Site Monitor tab** 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 AP 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** and add it to the table.

A low signal level indicates that the APs may be too far apart. Relocate or add APs 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 AP Manager

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

1. Select the AP from the **Managed List** field in the AP Manager main window.
2. Click on the **Integrity** drop-down menu option and select **Link Test**.
3. Under **Remote Station Info**, click the down arrow to list the available clients in the wireless network or the remote APs in a LAN-to-LAN configuration.
4. Choose the client or AP to test the signal quality, then click the **Start Sampling** button to start the test. To stop the test, click the **Stop Sampling** button.

5. Check the signal level and noise level if the SNR is low between the AP and the 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 AP 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 AP. 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 APs. If you are testing the link between two APs that both use directional antennas, you may need one person at each antenna and a method to communicate with those people.

NOTES

NOTE*: Antennas should only be installed by a qualified antenna installer. The antenna installation professional should be licensed or certified in accordance with local regulations.*

If you are planning to use an outdoor antenna refer to the RoamAbout Outdoor Antenna Site Preparation and Installation Guide *for regulatory information, FCC requirements, and detailed procedures to install outdoor antennas.*

1. Select the AP from the **Managed List** field in the AP Manager main window.
2. Click on the **Integrity** drop-down menu and select **Link Test**.
3. Under **Remote Station Info** in the Link Test window, click the down arrow to list the available APs in the LAN-to-LAN configuration.
4. Choose the AP to test the signal quality then click **Start Sampling** to start the test.
5. 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.
6. 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 allows you to investigate the operation of your RoamAbout PC Card and the installed driver.

Run the card test only in situations where there is 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 advance to the Card Diagnostics window, perform the following steps:

1. Click on the **Advanced** drop-down menu and select **Card Diagnostics**.
2. Click on the **Test Card Now** button to perform the card diagnostics. The results of the card diagnostics are listed under the self test fields.

⚠ ***CAUTION***: *Running the Card Test may disrupt normal operation of the RoamAbout PC Card. This may result in a loss of your current connection to your network. When you click the Test Card Now button, the RoamAbout Client Utility displays a warning that allows you to either abort or proceed with the Card Test.*

Click on the **Generate Report** button to create a log file of the wireless network card components and system settings of your computer. If you need to contact RoamAbout technical support, the card test results may help the support representative determine the cause of a malfunctioning device.

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, 98, 2000, Me, or XP system:

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

Monitoring the AP Using RMON

The AP 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 AP 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 AP 2000 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.

Monitoring RADIUS Client Operations

Using the console port, you can monitor the RADIUS client statistics for the primary and secondary RADIUS servers.

Using the RoamAbout R2 Console Port

To view the RADIUS client statistics, choose RADIUS Client Statistics from the **Security and Policy Configuration** menu. Refer to **Table 6-1** for a description of the statistics.

Using the Access Point 2000 Console Port

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.
2. Choose **Authentication Options**.
3. Choose **Monitor RADIUS Client Operation**. The menu options are:

   List RADIUS Client Statistics: Displays the AP RADIUS counter information.

   List RADIUS Client Parameters: Displays the AP RADIUS configuration.

   List RADIUS Client Statistics and Parameters: Displays the AP RADIUS parameters and counter information.

   Clear RADIUS Client Statistics: Resets all the counters to 0.
4. Choose **List RADIUS Client Statistics** to display the RADIUS Client Statistics for the Primary Server and/or the Secondary Server. Field descriptions are listed in **Table 6-1**.

Table 6-1: RADIUS Client Statistics Menu - Field Descriptions

Field	Description
Invalid Server Addresses	Number of RADIUS Access-Response packets received from unknown addresses.
Round Trip Time	Time interval (in hundredths of seconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
Access Requests	Number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Access Retransmissions	Number of Access-Request packets retransmitted to the RADIUS authentication server.
Access Accepts	Number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	Number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	Number of RADIUS Access-Challenged packets (valid or invalid) received from the server.
Malformed Access Responses	Number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Malformed packets do not include bad authenticators, signature attributes, or unknown types.
Bad Authenticators	Number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from the server.
Pending Requests	Number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable increments when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, time-out, or retransmission.
Timeouts	Number of authentication time-outs to this server. After a time-out the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a time-out. A send to a different server is counted as a Request, as well as a time-out.
Unknown Types	Number of RADIUS packets of unknown type which were received from the server on the authentication port.
Packets Dropped	Number of RADIUS packets received from the server on the authentication port and dropped for some other reason.

Checking RoamAbout Product Version Numbers

Using AP Manager

To check the RoamAbout AP 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.

Using the Access Point 2000 Console Port

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

Using the RoamAbout R2 Console Port

To check the RoamAbout R2 firmware version using the console port, choose **Current Configuration** from the Main Menu.

Using the Client Utility

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.

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

Upgrading the RoamAbout AP Firmware

The AP 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 AP, copy the image file from the web site to the same directory as the AP Manager or BootP/TFTP server.

- For the Access Point Classic, select the latest V*.BIN file for firmware upgrades.
- For the Access Point 2000, select the N*.BIN file for firmware upgrades, or R*.BIN file for BootROM upgrades.
- For the RoamAbout R2, select the latest G*.Z file for firmware upgrades, or B*.BIN file for BootROM upgrades.

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

The AP Manager includes a BootP/TFTP loader, called NetRider Loader, that upgrades the AP. 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 AP; you might load an incorrect image. You can only upgrade one AP at a time. When you start the upgrade, the AP immediately stops its operation.

Using the AP Manager

To upgrade the AP 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 AP is unavailable. You can determine when the upgrade is complete by looking at the AP LEDs or by trying to view parameters using the AP Manager.

Using the Access Point 2000 Console Port

Perform the following to upgrade the Access Point using the console port. Do not choose the Save command when using the Upgrade Flash command.

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.

4. Choose **BootP Server** if a BootP server has been configured with the correct file. Choose **TFTP Server** if you wish to upgrade the AP with a specific image. If choosing **TFTP Server**, you will be prompted for the server IP address and image file name.

5. Follow the online instructions to complete the upgrade.

Using the RoamAbout R2 Console Port

To upgrade the RoamAbout R2 using the console port:

1. Make sure that you have properly configured a BootP/TFTP server.

2. Choose **Reset/Upgrade** from the Main Menu.

3. Choose **Upgrade Flash**.

4. Enter the following:

   Image Path: If using NetRider Loader, only enter the filename. Otherwise, enter the path to the image file relative to the TFTP server’s local root directory. For example: *c:\rmabt\image\filename.z*

   TFTP Server IP Address: IP address of the TFTP server where the image file is stored.

   Download Type: Select **Application** if upgrading the AP firmware, or **Boot ROM** if upgrading the BootROM.

5. Choose **Apply**. You are asked to confirm the upgrade.

Using the AP Hardware Reset Button

The AP hardware Reset button (labeled as S1 on the unit) forces the AP to download a firmware image and reset to factory default values. Use the Reset button when you are unable to reload or upgrade the AP using the AP Manager or console port (i.e, should the AP firmware suffer data corruption).

To use the Reset button, perform the following:

1. Remove the power from the AP.

2. If this is an Access Point or Access Point 2000, restore the AC power then press the Reset button on the Access Point. If an image is not available, the AP waits approximately three minutes then resets to factory default values.

3. If this is a RoamAbout R2, restore the power then insert a toothpick or equivalent into the reset hole on the R2. If an image is not available, the R2 waits approximately three minutes then resets to the current configuration values.

Replacing the PC Card in an AP

You may need to replace a defective PC Card or upgrade the PC Card in an AP. If upgrading the AP from a 2 Mbit/s PC Card to an 11 Mbit/s PC Card, make sure that the AP firmware version is V5.0 or greater, as described in the **"Checking RoamAbout Product Version Numbers" section on page 6-13**.

NOTE*: Refer to the Regulatory information, FCC requirements, and installation information shipped with the PC Card before you install it***.**

You should disable encryption before replacing a PC Card with one that does not support encryption.

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

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

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

Chapter 7

Problem Solving

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

If the problem appears to be with an AP or a specific client, check the LEDs first. The AP LEDs are described in the next section. The client LEDs are described on **page 7-19**.

In This Chapter

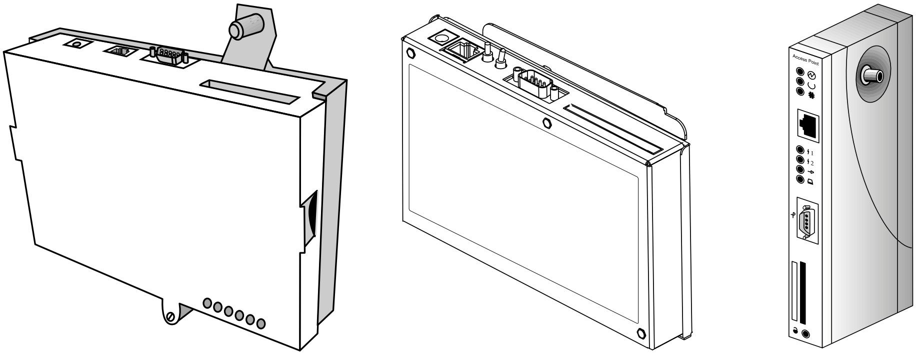
Information in this chapter is presented as follows:

Using the AP LEDs to Determine the Problem

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

Figure 7-1 shows the RoamAbout APs.

Figure 7-1: RoamAbout APs



R2 Wireless Access Platform

Access Point 2000

Access Point Classic

RoamAbout R2 LEDs

Table 7-1 describes the function of each LED. Error conditions cause the LEDs to turn on, off, or blink in a pattern. **Table 7-2** describes the LED patterns.

Table 7-1: RoamAbout R2 LED Descriptions

Name	Description
System Status	Lights when the RoamAbout R2 passes self-test. If the RoamAbout R2 fails the test, the LED blinks at a steady rate.
Power	Lights when the power is on.
Wired Forwarding ¦1	Lights when the RoamAbout R2 is forwarding packets to the wired Ethernet port.
Wireless Forwarding (Slot 1) ¦2	Lights when the RoamAbout R2 is forwarding packets to the wireless port (slot 1).
Wireless LAN Activity on the RoamAbout R2 (Slot 1, Slot 2)	Blinks, indicating activity, 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 RoamAbout R2 using the wireless port.
L	Lights indicating a link (connection) to the wired Ethernet port.
A	Flashes when there is activity to or from the wired Ethernet port.
Mezzanine Wireless Forwarding (Slot 2) ¦3	Lights when the RoamAbout R2 is forwarding packets to the wireless port (slot2). This LED is only available if you purchased the RoamAbout R2 Mezzanine slot upgrade option.

Table 7-2: RoamAbout R2 LED Patterns

Wired LAN	Wireless LAN	Wireless Forwarding	Wired Forwarding	System OK	Meaning of LED Pattern
¦3	📶	¦2	¦1	⏻	
○	○	○	○	○	No power. Check the power connections.
○	○	○	○	◍	Diagnostics failed. If the pattern continues to display, contact technical support.
⊕	⊕	○	●	●	Normal operating mode.
⊕	⊕	○	○	●	RoamAbout R2 is waiting for the Spanning Tree. No action is required.
⊕	⊕	⊕	●	●	RoamAbout R2 is occasionally saturated. No action is required.
⊕	◍	○	◍	◍	Cannot communicate with the wireless network. Verify that the PC Card is properly inserted.
○	⊕	◍	◍	◍	Cannot communicate with the wired network. Verify that the Ethernet cable is properly connected.

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

AP 2000 LEDs

Table 7-3 describes the function of each LED. Error conditions cause the LEDs to turn on, off, or blink in a pattern. Table 7-4 describes the patterns, the most likely causes, and possible corrective actions. Table 7-5 describes the LED patterns during an AP firmware upgrade. If you suspect an AP failure, run the self-test by removing then reapplying AC power.

Table 7-3: RoamAbout AP 2000 LED Summary Table

Name	Description
Power/ System Status	Lights when the AP has power and has passed the self-test. If the AP fails the test, the LED blinks at a steady rate.
Bridge State ¦1	Lights when the AP is forwarding packets.
AP Saturated ¦2	Lights when the AP is saturated. Saturation occurs when the AP 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 AP 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 AP from establishing a connection to the network.
Wired LAN Activity ＃	Lights when data is received on the Ethernet port. Data transmitted by the AP is not shown. Data traffic forwarded to the Ethernet port from the wireless port is not shown.

Table 7-4: RoamAbout AP 2000 LED Patterns

Wired LAN ＃	Wireless LAN 📶	AP Saturated ¦2	Bridge State ¦1	Power/ System Status ⏻	Meaning of LED Pattern
○	○	○	○	○	No power. Check the power connections.
○	◍	◍	○	◍	Diagnostics failed. The AP automatically resets after one minute. If the pattern continues to display, contact technical support.
⊕	⊕	○	●	●	Normal operating mode.
⊕	⊕	○	○	●	AP is waiting for the Spanning Tree. No action is required. **or** Spanning Tree detected a bridge loop and disconnected the port. Remove the loop.
⊕	⊕	⊕	●	●	AP is occasionally saturated. No action is required.
⊕	◍	○	◍	◍	Cannot communicate with the wireless network. Verify that the PC Card is properly inserted.
○	⊕	◍	◍	◍	Cannot communicate with the wired network. Verify that the Ethernet cable is properly connected.
⊕	◍	◍	◍	◍	Cannot communicate with the wireless or wired network.

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

Table 7-5: Network Loading LED Patterns

Wired LAN	Wireless LAN	AP Saturated	Bridge State	Power/ System OK	Meaning of LED Pattern
#	📶	¦2	¦1	⏻ ◡	
∷	●	○	⊕	●	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

AP (Classic) LEDs

Table 7-6 describes the LED functions. **Table 7-7** describes the patterns, likely causes, and possible corrective actions. **Table 7-8** describes the patterns during a firmware upgrade.

Table 7-6: AP (Classic) LEDS

Name	Description
Power OK ⊘	Lights (green) when the AP has power.
Module OK ○	Lights (green) when the AP passes its power-up self-test. The LED is off if the AP 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 AP 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 AP from establishing a connection to the network.
Bridge State ¦1	Lights (green) when the AP is forwarding packets.
AP Saturated ¦2	Lights (yellow) when the AP is saturated. Saturation occurs when the AP 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 ➡	The LED lights (green) when packets are: • Received on the wireless port and forwarded to the Ethernet port. • Addressed to or generated by the AP 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 AP from establishing a connection to the network.
Card Present ⏏	Lights (green) when the PC Card is correctly installed at power-up.

Table 7-7: AP (Classic) LED Patterns

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
⏻	◡	#	¦1	¦2	→	⏏	
●	○	○	◍	◍	◍	⁘	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.
●	●	⊕	●	⊕	⊕	●	AP 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 7-8: Network Loading/Upline Dumping LED Patterns

Power OK	Module OK	Wired LAN	Bridge State	Saturated	Wireless LAN	Card Present	Meaning of LED Pattern
⏻	◡	#	¦1	¦2	➜	⏏	
●	●	○	⊕	○	●	⁘	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
●	○	○	◍	○	●	⁘	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

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

Showing Counters

You can display the values of all the counters maintained by the AP. This information can help you 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.

Using the AP Manager

Perform the following to show a subset of the counters using the AP Manager. For a description of the counters, click the **Help** button.

1. Select the AP from the Managed List field.

2. Click the **Counters** button.

Using the Access Point 2000 Console Port

To show all the counters using the console port:

1. Choose **Module-Specific Options** from the RoamAbout AP Installation Menu.

2. Choose **Show Counters**. The first screen displays counters with information specific to the Ethernet interface. The second screen displays the same counters with information specific to the wireless interface. The subsequent screens display a subset of the counters with information specific to wireless ports 1 through 6. The counters are described in **Table 7-9**. The final screen shows the RoamAbout PC Card counters, which are described in **Table 7-10 on page 7-14**.

Using the RoamAbout R2 Console Port

To show counters using the console port, choose **Counters** from the Main Menu. You can display the counters for the wired or wireless interface. The same set of counters is used for both ports. The counters and their descriptions are listed in **Table 7-11 on page 7-17**.

Table 7-9: RoamAbout AP (Classic and 2000) Counters

Counter	Description
Individually addressed bytes sent	Total number of bytes transmitted by the interface as part of unicast messages. Normal behavior for this counter shows a relatively high value that is increasing rapidly.
Multicast bytes sent	Total number of bytes transmitted by the interface as part of multicast messages. This value is expected to be a large number.
Individually addressed bytes received	Total number of bytes received by the interface as part of unicast messages. It is normal behavior for this counter to increase rapidly.
Multicast bytes received	Total number of bytes received by the interface as part of multicast messages. It is normal behavior for this counter to have a high value.
Individually addressed frames sent	Number of messages sent by the interface that are destined for another device. In most LAN applications, it is normal behavior for this counter to have a high value and continuously increase (you can see it run). For example, this counter should increase rapidly when running the Link Test.
Multicast frames sent	Total number of messages sent by the interface 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 Individually Addressed Frames Sent counter.
Individually addressed frames received	Number of messages sent by other devices to this interface. In most LAN applications, it is normal behavior for this counter to have a high value and continuously increase (you can see it run). For example, this counter should increase rapidly when running the Link Test.
Multicast frames received	Number of broadcast or multicast messages received by the interface. 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 Individually Addressed Frames Received counter.
Tagged frames rec'd/ sent/discard	The VLAN counters are shown on one line: **Received**: Number of tagged frames received on the interface minus the number of tagged frames discarded. **Sent**: Number of tagged frames sent by the interface. **Discarded**: Number of tagged frames discarded by the interface. If there are no discarded frames, the number of frames received on the wired interface will be the same as the number of frames sent by the wireless interface, and vice versa.
Frames deferred	Number of frames for which the first transmission attempt on the selected interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

Table 7-9: RoamAbout AP (Classic and 2000) Counters (Cont'd)

Counter	Description
Single collision	Number of successfully transmitted frames on the selected interface for which transmission is inhibited by exactly one collision. Frames counted in this counter are not counted by the MultipleCollisionFrames counter.
Multiple collisions	Number of successfully transmitted frames on the selected interface for which transmission is inhibited by more than one collision. Frames counted in this counter are not counted by the SingleCollisionFrames counter.
Excessive collisions	Number of frames for which transmission on the selected interface fails due to excessive collisions.
Carrier check failed	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on the selected interface. The count is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
Transmit Frame too long	Total number of times the interface failed to transmit frames due to a frame being larger than the maximum frame size of 1518 bytes.
Remote failure to defer	Number of frames for which the first transmission attempt on the selected interface is delayed because the medium is busy. The count does not include frames involved in collisions.
Block check error	Number of frames received on the selected interface that are not an integral number of octets in length and do not pass the FCS check. The count is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user).
Frame error	Number of times messages were received while a transmission elsewhere in the network was in progress. This counter is expected to be zero. Non-zero-values indicate a heavily loaded system.
Receive Frame too long	Total number of times the interface received a frame that was larger than the maximum frame size of 1518 bytes.
Data Overrun	The total number of frames which contain data overrun errors.
System buffer unavailable	Total number of times the interface failed to have a system receive buffer available to store an incoming frame. These failures can occur during a broadcast storm or bursts of frames destined for the interface.
Collision detect check fail	This counter is not used on the wired interface. For the wireless interface, the number of times a received message was discarded because it could not be decrypted by the 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.

Table 7-10: RoamAbout AP Classic and 2000) PC Card Counters

Counter	Description
Individually addressed frames sent (TxUnicastFrames)	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 continuously increase (you can see it run). For example, this counter should increase rapidly when running the Link Test.
Multicast frames sent (TxMulticastFrames)	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)	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 in this counter should be greater than the sum of TxUnicastFrames and TxMulticastFrames.
Individually addressed bytes sent (TxUnicastOctets)	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)	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)	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.
Single retry frames sent (TxSingleRetryFrames)	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)	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 could result in lower throughput for the PC Card if 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.

Table 7-10: RoamAbout AP Classic and 2000) PC Card Counters (Cont'd)

Counter	Description
Transmit retry limit exceeded frames (TxRetryLimitExceeded)	Number of messages that could not be delivered after the maximum number of retransmissions. You can use this counter 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)	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)	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 continuously increase (you can see it run). For example, this counter should increase rapidly when running the Link Test.
Multicast frames received (RxMulticastFrames)	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)	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)	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)	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)	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)	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.

Table 7-10: RoamAbout AP Classic and 2000) PC Card Counters (Cont'd)

Counter	Description
Wrong station address on transmit (TxDiscardsWrongSA)	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 the driver and protocol stack.
Receive WEP errors (RxDiscardsWEP Undecryptable)	Number of times a received message was discarded because it could not be decrypted by the 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 AP or other client.
Receive message in message fragments (RxMessageInMsg Fragments)	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 msg fragments (RxMessage InBadMsgFragments)	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.
Receive WEP ICV errors	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.
Receive WEP excluded	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 AP is configured to accept encrypted data only (DENY NON-ENCRYPTED DATA is enabled).

Table 7-11: RoamAbout R2 Counters

Counter	Wired Description
DropEvents	Total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
Octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Pkts	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcasts	Total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Multicasts	Total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	Total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Pkts	Total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	Total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is entirely normal for this counter to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	Total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
Pkt 64 Octets	Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Pkts 65 to 127 Octets	Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Table 7-11: RoamAbout R2 Counters (Cont'd)

Counter	Wired Description
Pkts 128 to 255 Octets	Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts 256 to 511 Octets	Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts 512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts 1024 to 1518 Octets	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Displaying Error Logs

The AP can display error logs used by support personnel to analyze system faults.

The AP Manager displays the number of times the AP has been reset and the last four error messages for both the Access Point 2000 and the R2. To see the reset count from the AP Manager, select the AP in the **Managed List** field then click the **Reset** button. To display the error messages in the AP Manager, click the **Troubleshooting** button.

The Access Point 2000 console port displays additional error information. To display the last eight error messages, choose **Dump Error Log** from the RoamAbout AP Installation Menu. The error log displays various information, including the current reset count. You can also display additional error information by choosing **Module-Specific Options** from the RoamAbout AP Installation Menu then selecting **Dump Error Log**.

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 7-12** 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

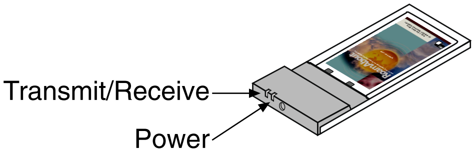


Table 7-12: RoamAbout PC Card LED Description

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 indicate 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 AP does not have Secure Access enabled. • The client may not be within range of an AP or ad-hoc network.
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 7-23**. Typically, this only happens on a Windows NT system. • Verify the versions of the PC Card driver as described in the **“Checking RoamAbout Product Version Numbers” section on page 6-13**. • Consult the RoamAbout web site to see if newer versions are available and if so, upgrade the 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, the problem could be one of the following:

- The PC Card 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 *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide*. Then reinstall the driver.

Client Cannot Connect to the Network

This situation may occur in one of the following situations:

- Wireless network name is incorrect. The wireless network name is case sensitive.
- If using **ANY** as the wireless network name or the field is blank, verify that the RoamAbout AP has disabled Secure Access.
- If the wireless network is using MAC Address authentication, the client’s MAC address must be configured on the RADIUS server.
- If the wireless network is using 802.1X Rapid Rekeying, the client must also be configured for Rapid Rekeying. The procedure to configure a Windows XP client for Rapid Rekeying is in **“Set Up Rapid Rekeying on the Clients” on page 5-38**.
- 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 network protocols.
- The driver is not loaded. Install the driver as described in the *RoamAbout 802.11 PC Card Drivers and Utilities Setup and Installation Guide*.
- There is a device conflict as described in **“Device Conflict on a Windows System” on page 7-23**.
- 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 on Windows 95, 98, and Me operating systems:

1. From the Windows desktop, click **Start** then select **Settings→Control Panel**.
2. Double-click on **Network**. Verify that the list of network components includes Client for Microsoft Networks and, optionally, Client for NetWare Networks.
3. 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.
4. 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 is not opened, click **Start**, select **Settings→Control Panel**, then double click **Network**.
2. Click the **Identification** tab. 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.
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**. 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, refer to the online help for information.
6. Enter the I/O Port and IRQ values that you wrote down.

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.

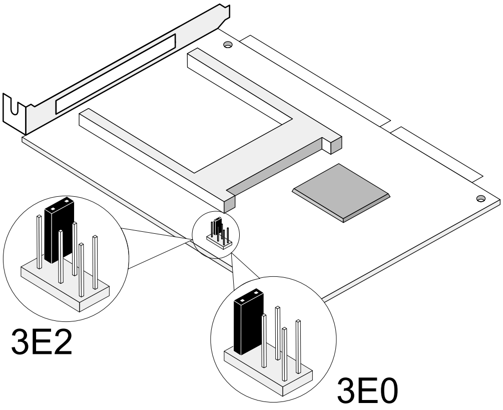
Changing the ISA Adapter Address

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 SNMP Trap Addresses (Access Point Only)

To have the AP 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 AP SNMP agent.

***NOTE**: This feature is not available on the RoamAbout R2.*

The AP sends an SNMP trap when any of the following events occur:

- AP is powered on (coldstart trap).
- Ethernet network connection is established (network link up trap).
- User tried to communicate with the AP 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 AP Installation Menu.
2. Enter the IP address of the system that you want to receive the SNMP traps.

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

Setting Upline Dump (Access Point Only)

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

NOTE

***NOTE**: This feature is not available on the RoamAbout R2.*

The Upline Dump setting is available by clicking the **Network Parameters** button in the AP Manager, or selecting the **Module-Specific Options** in the console port RoamAbout AP 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.

NOTES

***NOTE**: 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 xxxxxxx is the last 6 digits of the AP's wired MAC address.

Appendix A

PC Card Information

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

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)	13 (low power cards) 14 (high power cards)
	Other countries that adhere to 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

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)	13 (low power cards) 14 (high power cards)
	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 AP. This frequency is controlled by the LAN administrator who sets the RoamAbout AP 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	[1]**2422**	[1]**2422**	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	[2]**2437**	[2]**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**

[1] The Access Point 2000 uses this channel as the default.
[2] The RoamAbout R2 uses this channel as the default.

Appendix B

Connecting a Device to the Console Port

This Appendix describes how to connect a device to the console port. Refer to the *Hardware Installation Guide* for more information.

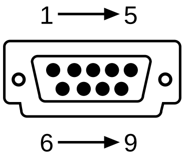
You can manage the AP using its console port or using the RoamAbout AP Manager program. You do not need to use the console port if you use the AP Manager.

You can connect 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. To connect a device to the AP console port, do the following:

1. Choose a device (terminal or personal computer) to connect to the AP.
2. Connect a null modem cable or equivalent to the device and the AP using the following pin assignment:

For the Access Point 2000:

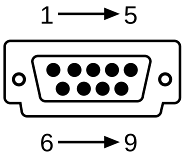
Pin	Assignment
1	Data Carrier Detect (DCD)
2	Receive Data (RXD)
3	Transmit Data (TXD)
4	Data Terminal Ready (DTR)
5	Ground
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	No connect



For the RoamAbout R2 Wireless Access Platform:

Pin	Assignment
[1, 4, 6]*	(1) Data Carrier Detect (DCD) (4) Data Terminal Ready (DTR) (6) Data Set Ready (DSR)
2	Receive Data (RXD)
3	Transmit Data (TXD)
5	Ground
7, 8*	(7) Request to Send (RTS) (8) Clear to Send (CTS)
9	No connect

*** [1,4,6] and [7,8] are tied together.**



3. If using a terminal, configure the transmit and receive baud rates to 9600 baud only.

4. If using a personal computer, configure a terminal emulation application to use 9600 baud transmit and receive rates. The following is an example of configuring the Microsoft Windows HyperTerminal application:

a) Open the HyperTerminal application, which is usually located in **Programs→Accessories→HyperTerminal**.

b) Create a new connection. Depending on the system configuration, HyperTerminal could automatically prompt you for a new connection name. Choose a name that identifies the connection type, such as AP Console Port.

c) Ignore or cancel any prompts for modem or phone information.

d) In a **Connect Using** or similar field, select the port that is connected to the AP, such as COM1.

e) In the Port Settings window, enter:

— **Bits per second**: 9600

— **Data bits**: 8

— **Parity**: None

— **Stop Bits**: 1

— **Flow Control**: Hardware (for the Access Point 2000)
None (for the RoamAbout R2)

To connect to the console port at a later date, open HyperTerminal and select **File→Open** to open the AP Console Port connection.

5. Press <**Enter**> until the RoamAbout Main Menu is displayed. The Installation Menu allows you to display and modify various AP and wireless networking parameters.

   If this is a RoamAbout R2, you are prompted for a username and password. The default username is **admin** and the default password is **password**.

   NOTE*: If your screen remains blank after 3 seconds, press the Ctrl and L keys together. If the screen still remains blank, shut down the terminal emulation program and restart it.*

Use the console as follows:

- Use your arrow keys to navigate through the screens.
- Press your **Enter** (or **Return**) key to activate a data entry field.
- Press the space bar to toggle a multiple choice field.
- Select **Apply** if you want to check your configuration changes before saving them.
- Select **Save** before you Reset, Reload or Exit out of the console to save your configuration changes in each screen.
- If you do not want to change the existing value, press <Enter> to go back to the previous menu.

Appendix C

ASCII to HEX Conversion

This Appendix provides the ASCII to HEX conversion for use with third party products that do not allow ASCII entry of encryption keys.

ASCII Value	HEX Value
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
A	41
a	61
B	42
b	62
C	43
c	63
D	44
d	64

ASCII Value	HEX Value
E	45
e	65
F	46
f	66
G	47
g	67
H	48
h	68
I	49
i	69
J	4A
j	6A
K	4B
k	6B
L	4C
l	6C
M	4D
m	6D
N	4E
n	6E
O	4F
o	6F
P	50
p	70

ASCII Value	HEX Value
Q	51
q	71
R	52
r	72
S	53
s	73
T	54
t	74
U	55
u	75
V	56
v	76
W	57
w	77
X	58
x	78
Y	59
y	79
Z	5A
z	7A

Glossary

802.1X

IEEE 802.1X uses security protocols, such as RADIUS, to provide centralized user identification, authentication and dynamic key management.

Access Platform

See R2 Wireless Access Platform.

Access Point

A wired to wireless bridge that connects a wireless LAN to a wired Ethernet LAN.

Ad-Hoc network

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

Ad-hoc networks are also referred to as peer-to-peer networks.

AP

A generic term that refers to the RoamAbout Access Point, RoamAbout Access Point 2000, or the RoamAbout R2 Wireless Access Platform.

Beacon

A message that is transmitted at regular intervals by the RoamAbout AP 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 AP 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 AP and its wireless clients within a wireless infrastructure network containing multiple APs.

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 AP.

Endpoint Bridge Mode

An AP mode that allows two APs to communicate, effectively connecting two wired LANs through a wireless link.

Ethernet Adapter

The Ethernet Adapter is used on wired devices (for example, desktop computers and printers) to make them wireless devices.

ETSI

European Telecommunications Standards Institute (ETSI) regulations.

FCC

Federal Communications Commission (FCC) and Canada (Industry Canada (IC)).

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. 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.

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.

MAC Address

This is the hardware address of the device. The MAC address consists of 12 hexadecimal digits, and is printed on the device.

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.

Multipoint Bridge Mode

An AP mode that allows up to seven APs to communicate, effectively connecting wired LANs through a wireless link.

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 AP.

PC Card

A network card that installs in an AP or wireless client to provide wireless connectivity in a LAN environment.

PCI Adapter

An option for the RoamAbout PC Card for computers that do not have a PCMCIA slot. The PCI adapter installs into a computer and provides a PCMCIA slot for the PC Card.

PCMCIA

The Personal Computer Memory Card International Association (PCMCIA) is the standards body for the type of PC Card used with the RoamAbout products.

R2 Wireless Access Platform

An expandable wireless access platform designed to support existing, and future, radio technologies and networking requirements.

RADIUS

RADIUS (Remote Authentication Dial-In User Service). RADIUS is an IETF standard protocol for Authentication, Authorization and Accounting.

Range Extender Antenna

An indoor antenna that extends the coverage area of a RoamAbout wireless device.

Rapid Rekeying

Also known as Key Tumbling, provides frequent, automatic, redistribution of IEEE 802.11 WEP Encryption keys for enhanced security.

RoamAbout AP Manager

Software used to manage and configure one or more APs. The software is installed on a Windows computer that connects to the AP 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 APs. As the client moves away from its AP and the signal level decreases, the RoamAbout PC Card automatically connects to another AP 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 APs 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

(Access Point 2000 only.) When enabled, the multipoint AP relays messages from one AP to another. When disabled, each of the APs in the LAN-to-LAN multipoint configuration can only communicate with the multipoint AP and its wired LAN.

Index