RoamAbout®

Wireless Networking

RBT-4102-LIC Access Point Installation Guide

P/N 9034249

enterasys™

Networks that Know

Electrical Hazard: Only qualified personnel should perform installation procedures.

Riesgo Electrico: Solamente personal calificado debe realizar procedimientos de instalacion.

Elektrischer Gefahrenhinweis: Installationen sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.

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.
50 Minuteman Road
Andover, MA 01810

Part Number: 9034249 January 2006

Documentation URL: http://www.enterasys.com/support/manuals

RBT-4102-LIC Compliances

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 70 centimeters (27.5 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Wireless 5 GHz Band Statements:

As the Access Point can operate in the 5150-5250 MHz frequency band it is limited by the FCC to indoor use only so as to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

High power radars are allocated as primary users (meaning they have priority) of the 5250-5350 MHz and 5650-5850 MHz bands. These radars could cause interference and /or damage to the access point when used in Canada.

Wireless 4.9 GHz Band Statement:

Installation and operartion requires an approved license from the FCC.

Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing the access point:

Warning: Installation and removal of the unit must be carried out by qualified personnel only.

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A.	The cord set must be UL-approved and CSA certified.
	• The minimum specifications for the flexible cord are: • No. 18 AWG – not longer than 2 meters, or 16 AWG. • Type SV or SJ • 3-conductor
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.

Enterasys Networks, Inc.
Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc. on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program/firmware installed on the Enterasys product (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, and supersedes all prior discussions, representations, understandings or agreements, whether oral or in writing, between the parties with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. **LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. **RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

   (i) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

   (ii) Incorporate the Program, in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

   (iii) Publish, disclose, copy, reproduce or transmit the Program, in whole or in part.

   (iv) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.

   (v) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. **APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on Contracts for the International Sale of Goods, the United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. **EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the Program is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. **DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON- INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. **AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. **OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. **ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. **ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock or assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. **WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. **SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. **TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

About This Guide

This guide shows you how to install the Enterasys Networks RoamAbout RBT-4102-LIC Access Point.

Intended Audience

Read this guide if you are a network administrator, or other person installing the RoamAbout RBT-4102-LIC Access Points in a network.

Associated Documents

Consult the RoamAbout Wireless Networking Access Point RBT-4102 Configuration Guide to configure and manage the RBT-4102-LIC Access Point.

You can download documentation from the Enterasys Networks documentation web site: http://www.enterasys.com/support/manuals/n-s.html#R.

Conventions Used in This Document

The following safety, advisory notices, and typographical conventions appear in this manual.

bold type	Actual user input values or names of screens and commands.
blue type	Indicates a hypertext link. When reading this document online, click the text in blue to go to the referenced figure, table, or section.
italic type	User input value required.
`courier`	Used for command-level input or output.
	**Note:** Calls the reader's attention to any item of information that may be of special importance.
	**Caution:** This situation or condition can lead to data loss or damage to the product or other property.
	**Warning!** This situation or condition can cause injury.
	**Warning!** High voltage. This situation or condition can cause injury due to electric shock.

Getting Help

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

World Wide Web	http://www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S.) For the Enterasys Networks Support toll-free number in your country: http://www.enterasys.com/support/gtac-all.html
Internet mail	support@enterasys.com To expedite your message, please type **[RoamAbout]** in the subject line.
To send comments concerning this document to the Technical Publications Department: techpubs@enterasys.com Please include the document Part Number in your email message.	

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

Network Configuration

Overview

Wireless networks support a standalone configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs. The RoamAbout RBT-4102-LIC, also provides bridging services that can be configured independently on either the 5 GHz or 2.4 GHz radio interfaces.

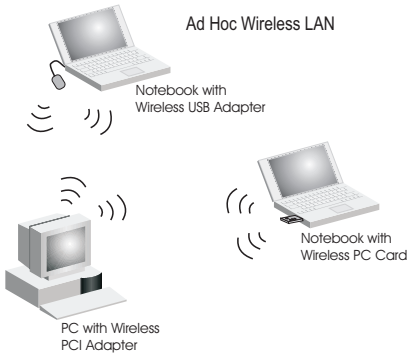
Access points can be deployed to support wireless clients and connect wired LANs in the following configurations:

- Ad hoc for departmental, SOHO or enterprise LANs
- Infrastructure for wireless LANs
- Infrastructure wireless LAN for roaming wireless PCs
- Infrastructure wireless bridge to connect wired LANs
- The 802.11b and 802.11g frequency band which operates at 2.4 GHz can easily encounter interference from other 2.4 GHz devices, such as other 802.11b or g wireless devices, cordless phones and microwave ovens. If you experience poor wireless LAN performance, try the following measures:
- Limit any possible sources of radio interference within the service area
- Increase the distance between neighboring access points
- Decrease the signal strength of neighboring access points.
- Increase the channel separation of neighboring access points (for example, up to 3 channels of separation for 802.11b, or up to 4 channels for 802.11a, or up to 5 channels for 802.11g)

Network Topologies

Ad Hoc Wireless LAN (no Access Point)

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel. An ad hoc wireless LAN can be used for a branch office or SOHO operation.

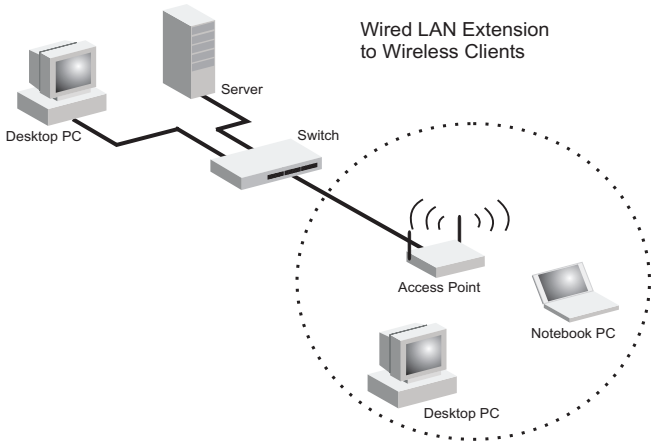


Infrastructure Wireless LAN

The access point also provides access to a wired LAN for wireless workstations. An integrated wired/wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can talk to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via the access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.

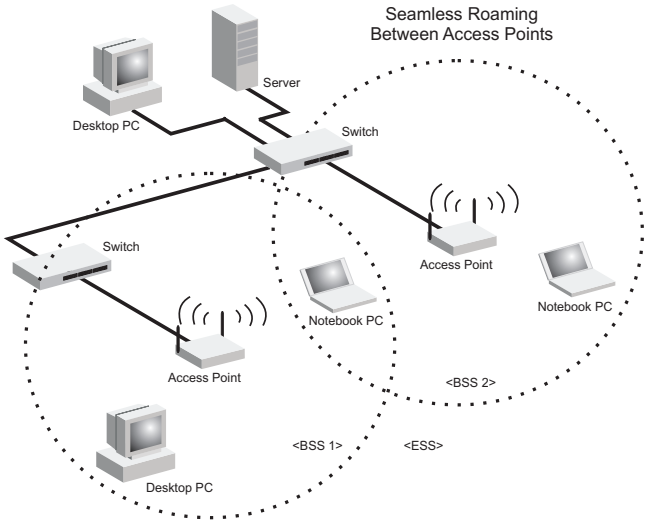


Infrastructure Wireless LAN for Roaming Wireless PCs

The Basic Service Set (BSS) defines the communications domain for each access point and its associated wireless clients. The BSS ID is a 48-bit binary number based on the access point's wireless MAC address, and is set automatically and transparently as clients associate with the access point. The BSS ID is used in frames sent between the access point and its clients to identify traffic in the service area.

The BSS ID is only set by the access point, never by its clients. The clients only need to set the Service Set Identifier (SSID) that identifies the service set provided by one or more access points. The SSID can be manually configured by the clients, can be detected in an access point's beacon, or can be obtained by querying for the identity of the nearest access point. For clients that do not need to roam, set the SSID for the wireless card to that used by the access point to which you want to connect.

A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All wireless network cards and adapters and wireless access points within a specific ESS must be configured with the same SSID.



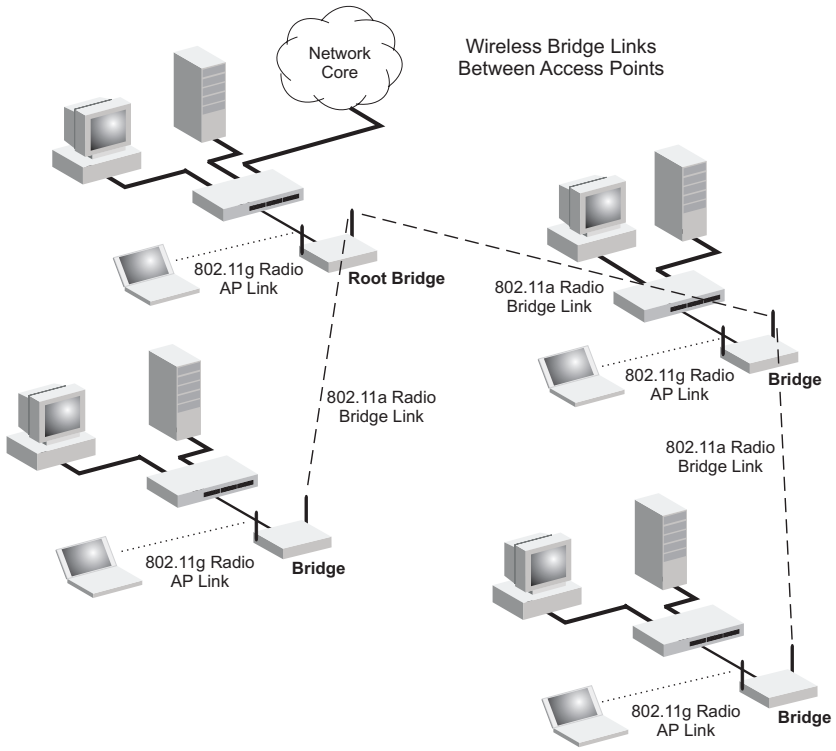
Infrastructure Wireless Bridge

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for bridge connections between BSS areas (access points). The access point uses WDS to forward traffic on links between units.

The access point supports WDS bridge links on either the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) bands and can be used with various external antennas to offer flexible deployment options.

Up to six WDS bridge links can be specified for each unit in the wireless bridge network. One unit only must be configured as the “root bridge” in the wireless network. The root bridge should be the unit connected to the main core of the wired LAN. Other bridges must configure one “parent” link to the root bridge or to a bridge connected to the root bridge. The other five available WDS links can be specified as “child” links to other bridges. This forms a tiered-star topology for the wireless bridge network.

When using WDS on a radio band, only wireless bridge units can associate to each other. Wireless clients can only associate with the access point using a radio band set to access point.



2

Access Point Overview

Features

The RoamAbout RBT-4102-LIC is an IEEE 802.11a/b/g access point that provides transparent, wireless high-speed data communications between the wired LAN and fixed or mobile devices equipped with an 802.11a, 802.11b, or 802.11g wireless adapter.

This solution offers fast, reliable wireless connectivity with considerable cost savings over wired LANs (which include long-term maintenance overhead for cabling). Using 802.11a and 802.11g technology, these access points can easily replace a 10 Mbps Ethernet connection or seamlessly integrate into a 10/100 Mbps Ethernet LAN.

The RBT-4102-LIC supports up to eight Virtual Access Points per physical radio interface, that is eight on the 802.11a radio, and eight on the 802.11g radio. This allows traffic to be separated for different user groups using an access point that services one area. For each VAP, different security settings, VLAN assignments, and other parameters can be applied.

Each radio interface on the RBT-4102-LIC can operate in one of three modes:

- **Access Point** – Providing connectivity to wireless clients in the service area.
- **Bridge (Point-to-Point)** – Providing links to other access points in "Bridge" or "Root Bridge" mode connecting wired LAN segments.
- **Root Bridge (Point-to-Multipoint)** – Providing links to other access points in "Bridge" mode connecting wired LAN segments. Only one unit in the wireless bridge network can be set to "Root Bridge" mode.

In addition, the access point offers full network management capabilities through an easy to configure web interface, a command line interface for initial configuration and troubleshooting, and support for Simple Network Management tools.

Radio Characteristics – The IEEE 802.11a/g standard uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates at the 5 GHz Unlicensed National Information Infrastructure (UNII) band for connections to 802.11a clients, and at 2.4 GHz for connections to 802.11g clients.

IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard. IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) modulation technology to achieve a communication rate of up to 11 Mbps.

The access point supports a 54 Mbps half-duplex connection to Ethernet networks for each active channel (up to 108 Mbps in turbo mode on the 802.11a interface).

Package Checklist

The RoamAbout package includes:

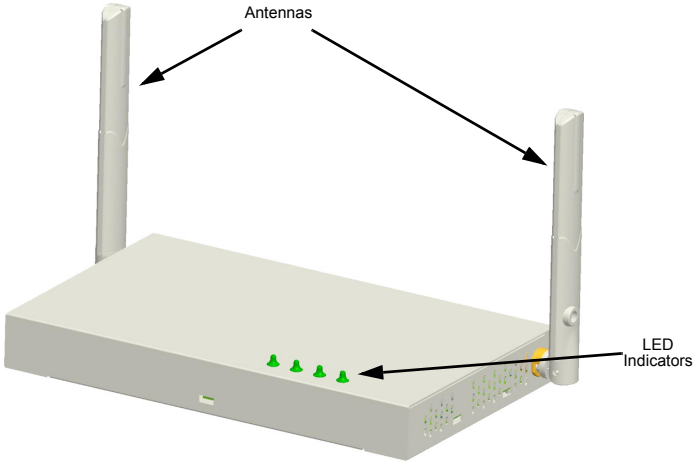
- One RoamAbout RBT-4102-LIC
- One RS-232 console cable
- One AC power adapter and power cord
- Four rubber feet
- Three wall-mounting screws
- Bezel
- Mounting bracket
- This Installation Guide
- Documentation CD (includes the Installation Guide and Management Guide)

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

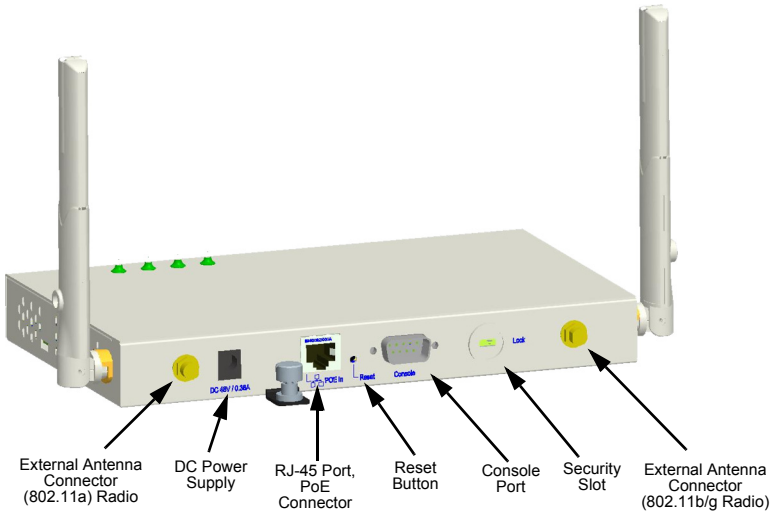
Caution: The Bezel should not be used in a plenum area.

Hardware Description

Top Panel



Rear Panel



Component Description

Antennas

The access point includes integrated diversity antennas for wireless communications. A diversity antenna system uses two identical antennas to receive and transmit signals, helping to avoid multipath fading effects. When receiving, the access point checks both antennas and selects the one with the strongest signal. When transmitting, it will continue to use the antenna previously selected for receiving. The access point never transmits from both antennas at the same time.

The antennas transmit the outgoing signal as a toroidal sphere (doughnut shaped), with the coverage extending most in a direction perpendicular to the antenna. The antenna should be adjusted to an angle that provides the appropiate coverage for the service area. For further information, see “Position the Antennas” on page 3-4.

External Antenna Connectors

The access point supports external antenna connections for both the 2.4 GHz and 5 GHz radios. These antennas offer a variety of options for extending the radio range and shaping the coverge area. For a list of external antennas, their model type and gain refer to “External Antennas” on page C-6.

For information on the external antennas available, refer to the following document on the Enterasys Web site:

http://www.enterasys.com/support/manuals/n-s.html#R

LED Indicators

The access point includes four status LED indicators, as shown in Figure 2-1, and described in Table 2-1.

Figure 2-1 LED Indicators

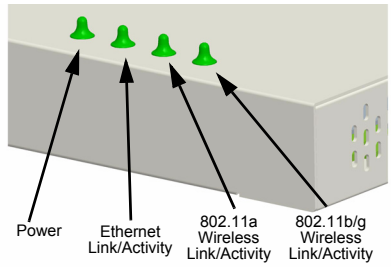


Table 2-1 LED Status Descriptions

LED	Status	Description
Power	On Green	Indicates that the system is working normally.
	Flashing Green	Indicates: • running a self-test. • loading software program.
	On Amber	Indicates a CPU or system failure.
	Flashing Amber (Prolonged)	Indicates system errors.
Link	On Green	Indicates a valid 10/100 Mbps Ethernet cable link.
	Flashing Green	Indicates that the access point is transmitting or receiving data on a 10/100 Mbps Ethernet LAN. Flashing rate is proportional to your network activity.

Table 2-1 LED Status Descriptions (continued)

LED	Status	Description
802.11a	On Green	Indicates the 802.11a radio is enabled.
	Flashing Green	Indicates that the access point is transmitting or receiving data through wireless links. Flashing rate is proportional to network activity.
	Off	Indicates the 802.11a radio is disabled.
802.11b/g	On Green	Indicates the 802.11b/g radio is enabled.
	Flashing Green	Indicates that the access point is transmitting or receiving data through wireless links. Flashing rate is proportional to network activity.
	Off	Indicates the 802.11b/g radio is disabled.

Security Slot

The access point includes a Kensington security slot on the rear panel. You can prevent unauthorized removal of the access point by wrapping the Kensington security cable (not provided) around an unmovable object, inserting the lock into the slot, and turning the key.

Console Port

This port is used to connect a console device to the access point through a serial cable. This connection is described under "Console Port Pin Assignments" on page B-4. The console device can be a PC or workstation running a VT-100 terminal emulator, or a VT-100 terminal.

Ethernet Port

The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3 or 802.3u specifications.

This port supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

The access point appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to remote workstations on the wireless infrastructure.

Note: The RJ-45 port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. Refer to the description for the "Power Connector" for information on supplying power to the access point's network port from a network device, such as a switch, that provides Power over Ethernet (PoE).

Reset Button

This button is used to reset the access point or restore the factory default configuration. If you hold down the button for less than 5 seconds, the access point will perform a hardware reset. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the access point.

Power Connector

The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The power adapter automatically adjusts to any voltage between 100~240 volts at 50 or 60 Hz. No voltage range settings are required.

The access point may also receive Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard.

Notes:

- The access point supports both endspan and midspan PoE.
- If the access point is connected to a PoE source device and also connected to a local power source through the AC power adapter, AC power will be disabled.

3

Installing and Connecting Your Access Point

Installation Requirements and Recommendations

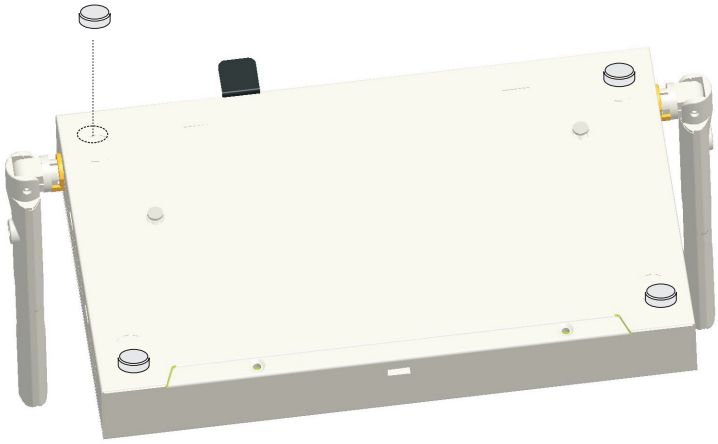
Select a Site – Choose a proper place for the access point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. Try to place the access point in a position that can best cover its Basic Service Set (refer to "Infrastructure Wireless LAN" on page 1-2). For optimum performance, consider these points:

- Mount the access point as high as possible above any obstructions in the coverage area.
- Avoid mounting next to or near building support columns or other obstructions that may cause reduced signal or null zones in parts of the coverage area.
- Mount away from any signal absorbing or reflecting structures (such as those containing metal).

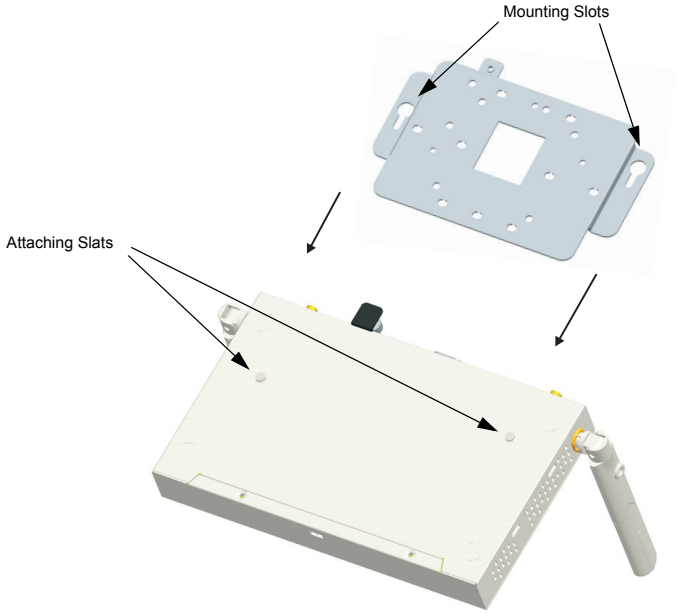
Installing the Access Point

1. **Mount the Access Point** – The access point can be mounted on any horizontal surface or a wall.

   - **Mounting on a Horizontal Surface** – To keep the access point from sliding on the surface, attach the four rubber feet provided in the accessory kit to the marked circles on the bottom of the access point.



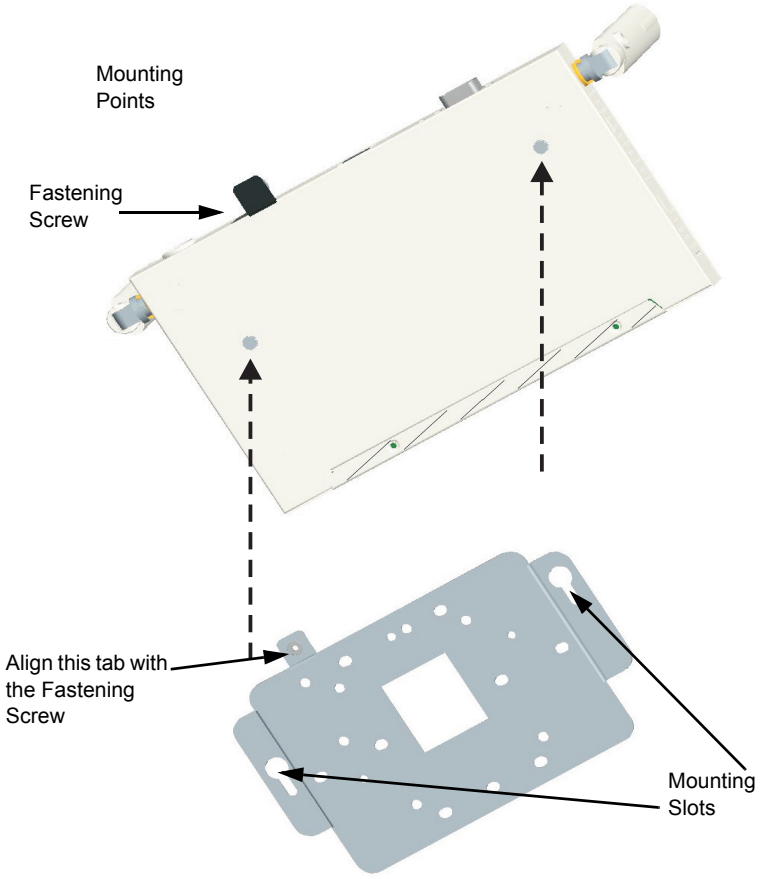
   - **Mounting on a Wall** – To mount on a wall or ceiling you must first attach the mounting bracket to the base of the access point. Align the two mounting slots on the bracket with the raised attaching slats and screw the unit into place firmly.



Bottom of Access Point

The access point should be mounted only to a wall or wood surface that is at least 1/2-inch thick plywood or its equivalent. To mount the access point on a wall, always use its wall-mounting bracket. The access point must be mounted with the RJ-45 cable connector oriented upwards to ensure proper operation.

2. Using the mounting bracket, mark the position of the four screw holes on the wall. For concrete or brick walls, you will need to drill holes and insert wall plugs for the screws.
3. Position the mounting bracket over the wall screw holes, then insert the included screws and tighten them down to secure the bracket firmly to the wall.
4. Attach the access point to the mounting bracket. Line up the two mounting points on the bracket with the two mounting slots on the bottom of the access point (see the following figure). Place the mounting points of the bracket into the mounting slots of the bracket, slide it into position so that the bracket fastening screw on the access point lines up with the tab on the bracket. Then screw down the fastening screw to secure the access point to the bracket.



Bracket

5. **Lock the Access Point in Place** – To prevent unauthorized removal of the access point, you can use a Kensington Slim MicroSaver security cable (not included) to attach the access point to a fixed object.
6. **Connect the Power Cord** – Connect the power adapter to the access point, and the power cord to an AC power outlet. Otherwise, the access point can derive its operating power directly from the RJ-45 port when connected to a device that provides IEEE 802.3af compliant Power over Ethernet (PoE).

Warning: Use ONLY the power adapter supplied with this access point. Otherwise, the product may be damaged.

Note: If the access point is connected to both a PoE source device and an AC power source, AC will be disabled.

7. **Observe the Self Test** – When you power on the access point, verify that the Power indicator stops flashing and remains on, and that the other indicators start functioning as described in "LED Indicators" on page 2-4.

   If the PWR LED does not stop flashing, the self test has not completed correctly. Refer to Appendix A, Diagnosing Access Point Indicators.

8. **Connect the Ethernet Cable** – The access point can be wired to a 10/100 Mbps Ethernet through a network device such as a hub or a switch. Connect your network to the RJ-45 port on the back panel with category 3, or 4 UTP Ethernet cable. When the access point and the connected device are powered on, the Ethernet Link LED should light indicating a valid network connection.

   Note: The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

9. **Position the Antennas** – Each antenna emits a radiation pattern that is toroidal (doughnut shaped), with the coverage extending most in the direction perpendicular to the antenna. Therefore, the antennas should be oriented so that the radio coverage pattern fills the intended horizontal space. Also, the diversity antennas should both be positioned along the same axes, providing the same coverage area. For example, if the access point is mounted on a horizontal surface, both antennas should be positioned pointing vertically up to provide optimum coverage.

10. **Connect the Console Port** – Connect the console cable (included with RBT-4102-LIC) to the RS-232 console port for accessing the command-line interface. You can manage the access point using the console port, the web interface, or SNMP management software, such as Enterasys NetSight or HP's OpenView.

4

Initial Configuration

Overview

You can manage the RoamAbout RBT-4102-LIC Wireless Access Point using:

- The Command Line Interface (CLI) accessed through a direct connection to the console port

  Refer to *RoamAbout RBT-4102 Wireless Access Point Configuration Guide* to view a list of all the CLI commands, and how to use them.

- The web interface accessed through a web browser (Internet Explorer V5.0 or above, or Netscape Navigator V6.2 or above).

Note: You must click on the **Apply** button at the bottom of each Web interface page for the configuration changes on that page to take effect.

- An SNMP manager, such as Enterasys Networks NetSight management applications.

Using the CLI

Required Connections

The access point provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuration. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the access point. You can use the console cable provided with this package, or use a cable that complies with the wiring assignments.

To connect to the console port, perform the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the access point.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or 2).
   - Set the data rate to 9600 baud.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.

- Set the emulation mode to VT100.
- When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, press the **Enter** key to initiate the console connection. The console login screen is displayed.

Logging In

To use the CLI to minimally configure the access point, follow these steps:

1. Enter **admin** for the user name, and **password** for the password to log in.

   The Access Point 4102 CLI prompt appears.

```
Username: admin
Password:********
RoamAbout 4102#
```

Note: The access point requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server by default. If a DHCP server does not respond, then the access point uses the default address, 192.168.1.1, which may not be compatible with your network. To assign an IP address, you must use the CLI. Go to Step 2.

2. If your access point uses a DHCP assigned IP address, go to Step 3 to change the default username and password.

   Otherwise, disable DHCP for this access point as follows:

   a. Type **configure** to enter configuration mode.

   b. Type **interface ethernet** to access the Ethernet interface configuration mode.

```
RoamAbout 4102#configure
Enter configuration commands, one per line. End with CTRL/Z
RoamAbout 4102(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
RoamAbout 4102(if-ethernet)#
```

c. Disable DHCP. Type **no ip dhcp**.

```
RoamAbout 4102(if-ethernet)#no ip dhcp
DHCP client state has changed. Please reset AP for change to take effect.
RoamAbout 4102(if-ethernet)#exit
RoamAbout 4102#reset board
Reboot system now? <y/n>: y
Username: admin
Password:********
RoamAbout 4102#configure
Enter configuration commands, one per line. End with CTRL/Z
RoamAbout 4102(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
RoamAbout 4102(if-ethernet)#
```

d. Set the IP Address. Type **ip address** ***ip-address netmask gateway,*** where ***ip-address*** is the access point's IP address, ***netmask*** is the network mask for the network, and ***gateway*** is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network.

```
RoamAbout 4102(if-ethernet)#ip address ip-address netmask gateway
RoamAbout 4102(if-ethernet)#end
RoamAbout 4102(config)#
```

After configuring the access point's IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be accessed using Telnet from any computer attached to the network.

3. Change the default username and password: type **username** and specify a unique user name; type **password** and specify a unique password.

```
RoamAbout 4102(config)#username KateJB
RoamAbout 4102(config)#password ******
Confirm new password: ******
RoamAbout 4102(config)#
```

4. Enable Management VLAN.

   a. Type **management-vlanid** and specify a management vlanid.

   b. Type **management-vlan enable**, and reset the access point.

Note: Before enabling the VLAN feature on the access point, you must set up the network switch port to support tagged VLAN packets from the access point. The switch port must also be configured to accept the access point's management VLAN ID and native VLAN IDs. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

```
RoamAbout 4102(config)#management-vlanid 10
RoamAbout 4102(config)#management-vlan enable
Reboot system now? <y/n>:y
Username: admin
Password:********
```

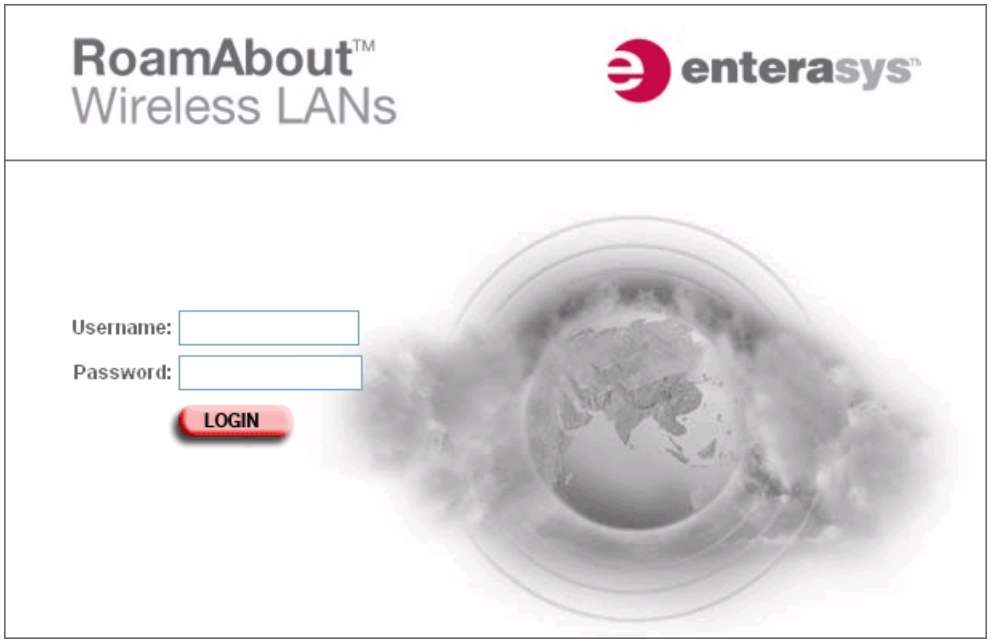
5. Refer to the *RoamAbout RBT-4102 Wireless Access Point Configuration Guide* for advanced configuration.

Using Web Management

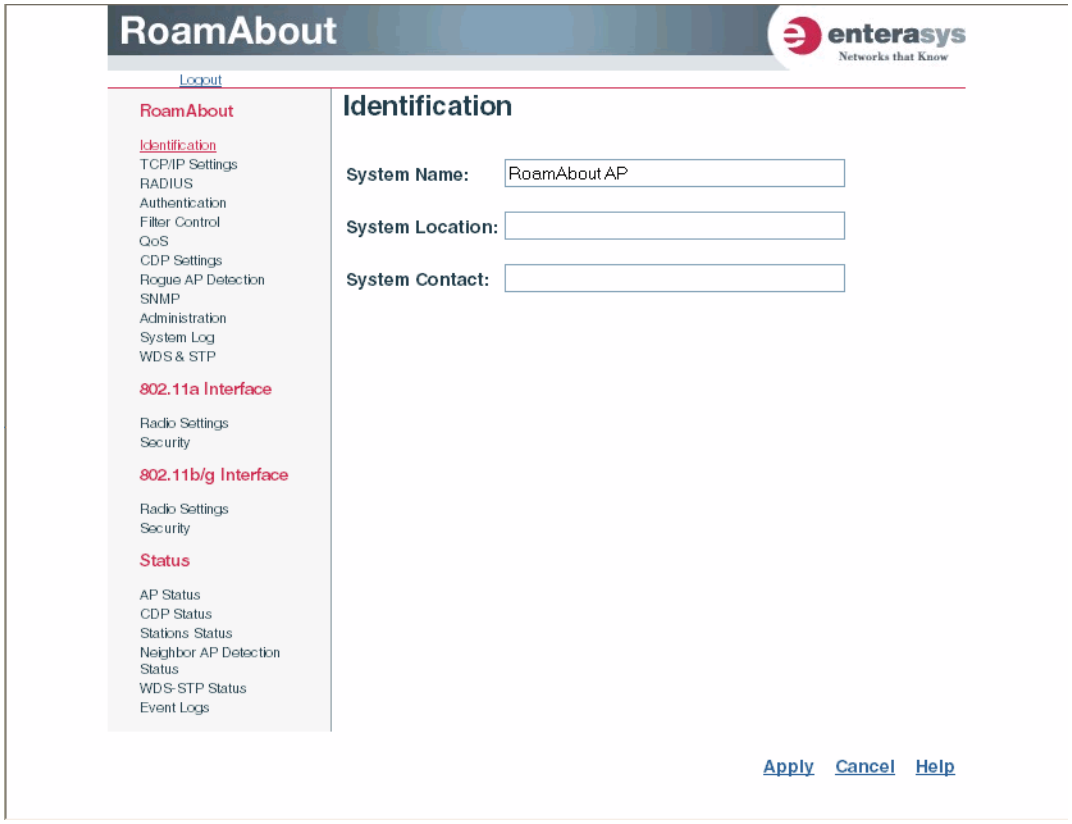
To use the Web interface to minimally configure the access point, follow these steps:

1. Open a Web browser and enter the access point's IP address in the address field:
   - If your access point uses a DHCP assigned IP address, make sure the access point is connected to your network, and enter the DHCP assigned IP address in your browser's address field. Use your DHCP server or other utility to determine the access point's IP address.
   - If your access point uses a static IP address, connect a system to the access point's Ethernet port and enter the default IP address: **http://192.168.1.1/** in your browser's address field.

   The access point's Login window appears.
2. Enter the username **admin** and the password **password** and click **LOGIN**.

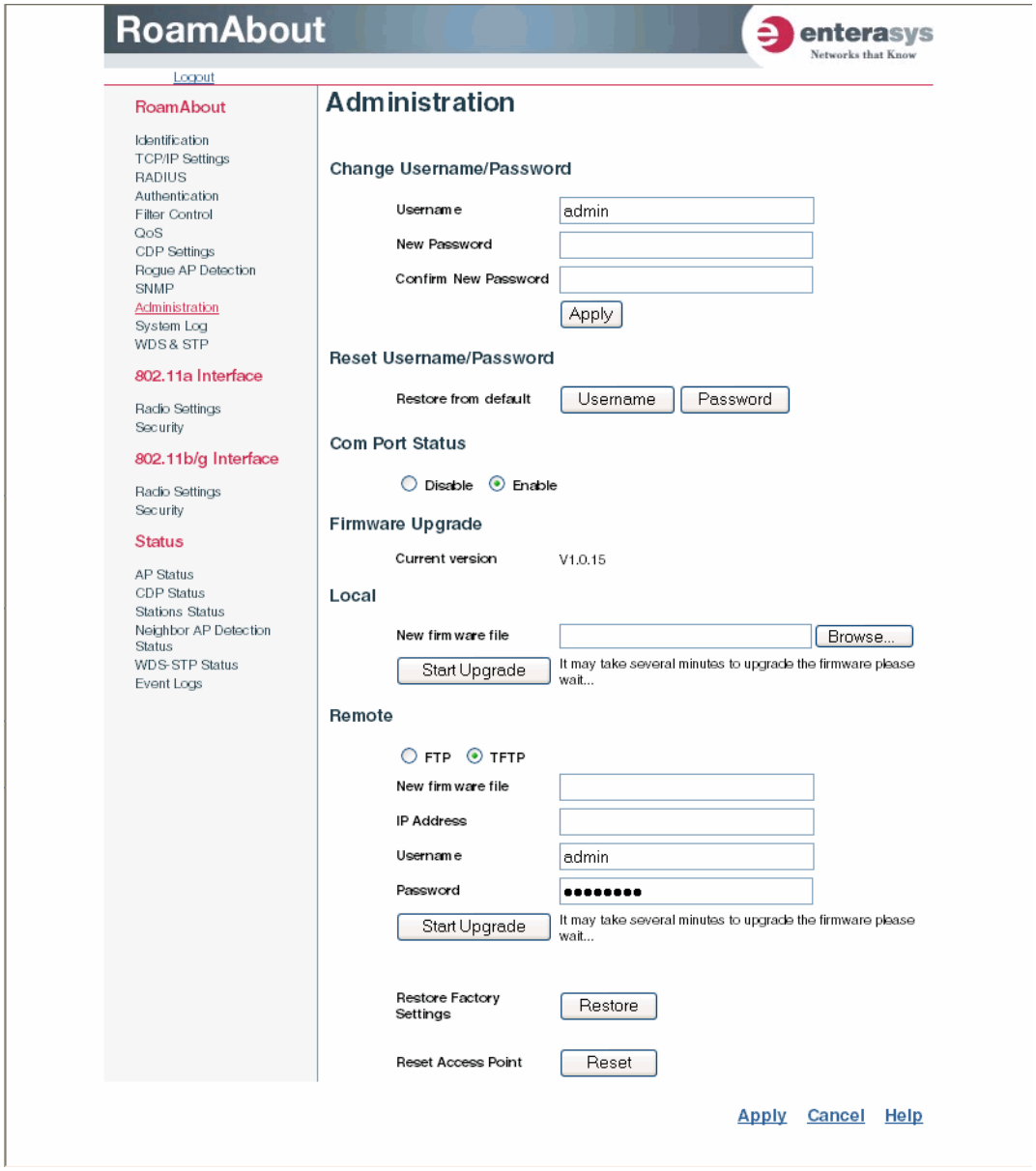


The Identification page appears.



c. Click **Administration** from the menu on the left-hand side of the page.

The Administration page appears.



d. Click **Reset**, at the bottom of the page.

   The access point prompts you to confirm that you want to reboot the system.

e. Click **OK**.

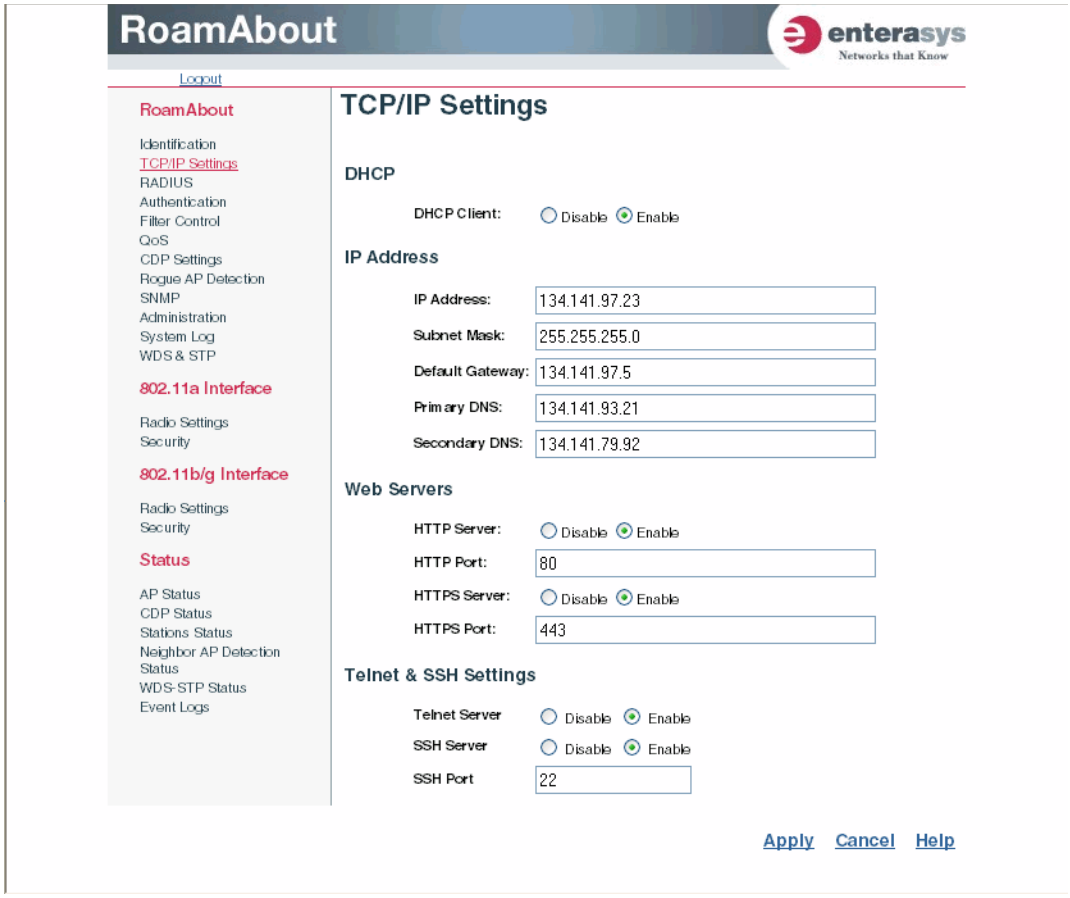
   The access point reboots and the Login window appears.

f. Enter the username **admin** and the password **password** and click **LOGIN**.

3. To set a static IP address:

   a. Click **TCP/IP Settings** from the menu on the left hand side of the page.

      The TCP/IP Settings page appears.



   b. Click the **DHCP Client: Disable** radio button.

      An IP Address section appears on the page.

   c. Specify the **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary** and **Secondary DNS**.

   d. Click **Apply** at the bottom of the page.

   e. Type the IP address that you specified for the access point in your browser's address field. For example, enter http://10.2.101.22/.

      The Login window appears.

   f. Enter the username **admin** and the password **password** and click **LOGIN**.

   g. Click **Administration** from the menu on the left of the page.

      The Administration page appears.

   h. Click **Reset**, at the bottom of the page.

      The access point prompts you to confirm that you want to reboot the system.

i. Click **OK**.

The access point reboots and the Login window appears.

j. Enter the username **admin** and the password **password** and click **LOGIN**.

4. Set username and password.
   a. Click **Administration** from the menu.

   The Administration page appears.

   b. Specify a new **username** in the Username field.
   c. Specify a new **password** in the Password field.
   d. Specify the new **password again** in the Confirm Password field.
   e. Click **Apply** at the bottom of the page.

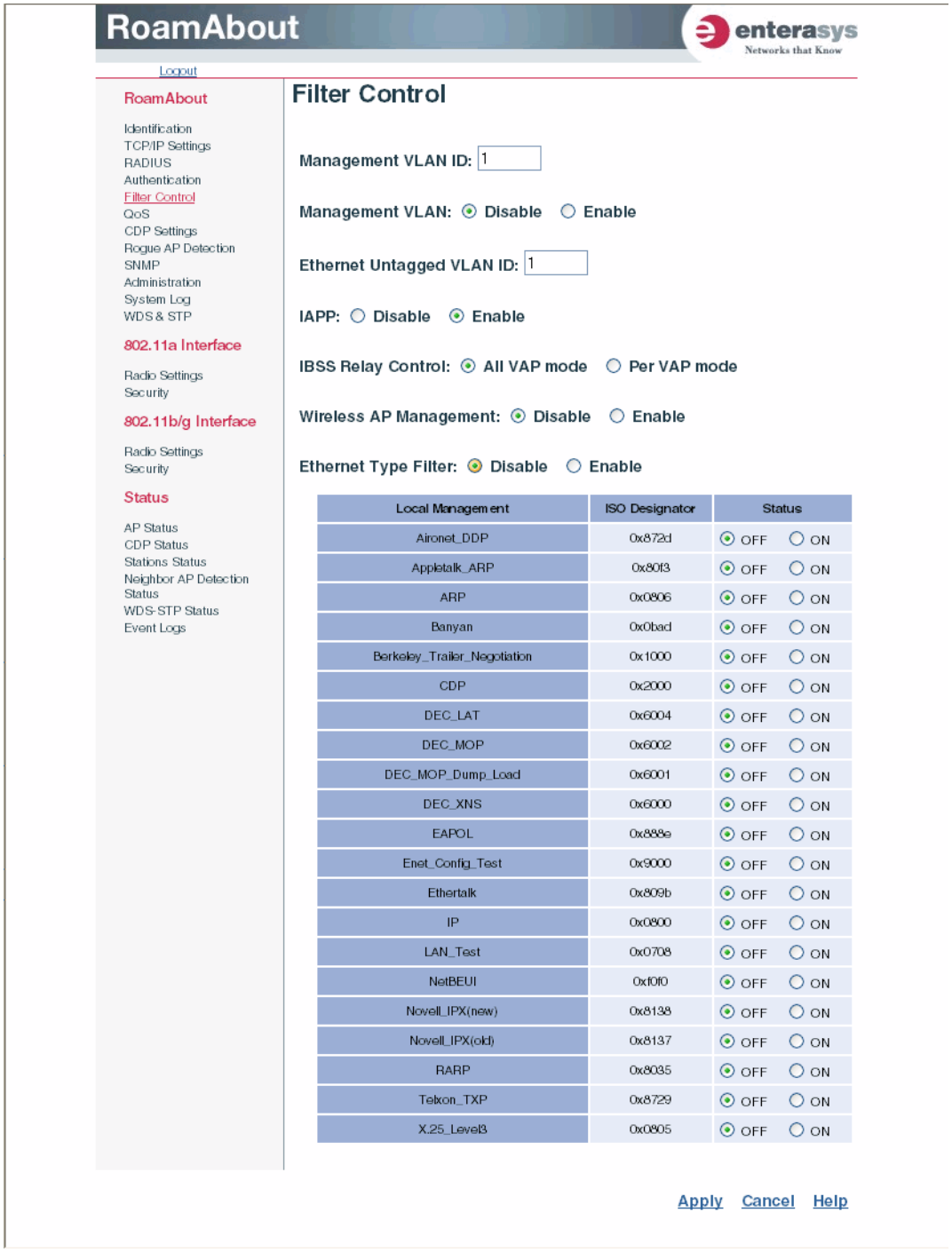
   The access point displays a Settings Saved message.

   f. Click **OK**.

   The Administration page appears.

5. Set management VLAN:
   a. Click **Filter Contro**l from the menu.

   The Filter Control page appears.



b. Click the **Management VLAN ID:** field and enter the VLAN ID from which you will manage the AP.

c. Click the **Management VLAN: Enable** radio button.

d. Click **Apply** at the bottom of the page.

   The access point displays a dialog box indicating that the VLAN status has changed and will take effect after the next reboot. The dialog box prompts you to choose whether to reboot now or later.

e. Click **OK** to reboot now.

   The access point reboots and the Login window appears.

f. Enter the **username** and the **password** that you specified for this access point and click **LOGIN**.

6. Refer to the *RoamAbout RBT-4102 Wireless Access Point Configuration Guide* for advanced configuration.

A

Diagnosing Access Point Indicators

Troubleshooting Chart	
Symptom	**Action**
Power LED is Off	• AC power adapter may be disconnected. Check connections between the access point, the power adapter, and the wall outlet. • PoE power to the access point may be disabled at the connected switch port. Check the switch configuration to be sure that PoE power is enabled for the switch and specified port. Also check that the switch has not exceeded its power budget and turned off the port power.
Power LED is Amber	The access point has detected a system error. Reboot the access point to try and clear the condition. If the condition does not clear, contact your local dealer for assistance.
Ethernet/Link LED is Off	• Verify that the access point and attached device are powered on. • Be sure the cable is plugged into both the access point and corresponding device. • Verify that the proper cable type is used and its length does not exceed specified limits. • Check the cable connections for possible defects. Replace the defective cable if necessary.

Note: For troubleshooting wireless connectivity problems, refer to the *RoamAbout Wireless Access Point RBT-4102 Configuration Guide*.

B

Cables and Pin-outs

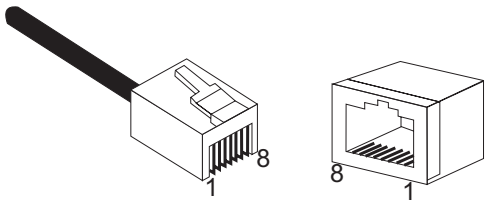
Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Notes:

- Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (Refer to "Straight-Through Wiring" on page B-3 and "Crossover Wiring" on page B-4 for an explanation.)
- DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through or crossover cables for all network connections to PCs, switches, or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable.

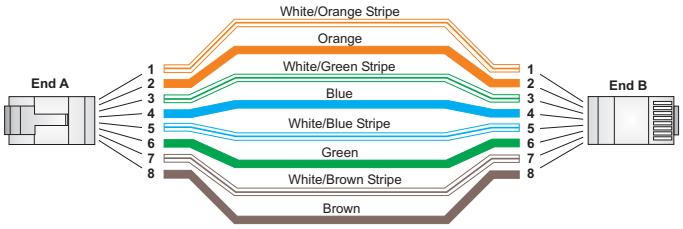
Pin	MDI Signal Name	MDI-X Signal Name
1	Receive Data plus (RD+) and GND (Positive V_{port})	Transmit Data plus (TD+) and -48V feeding power (Negative V_{port})
2	Receive Data minus (RD-) and GND (Positive V_{port})	Transmit Data minus (TD-) and -48V feeding power (Negative V_{port})
3	Transmit Data minus (TD+) and -48V feeding power (Negative V_{port})	Receive Data plus (RD+) and GND (Positive V_{port})
4	GND (Positive V_{port})	-48V feeding power (Negative V_{port})
5	GND (Positive V_{port})	-48V feeding power (Negative V_{port})
6	Transmit Data minus (TD-) and -48V feeding power (Negative V_{port})	Receive Data minus (RD-) and GND (Positive V_{port})
7	-48V feeding power (Negative V_{port})	GND (Positive V_{port})
8	-48V feeding power (Negative V_{port})	GND (Positive V_{port})

Note: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

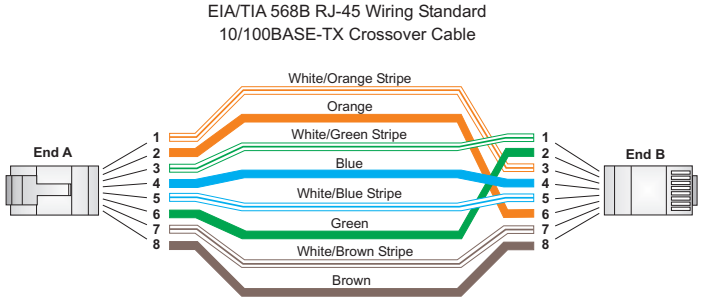
If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Straight-through Cable



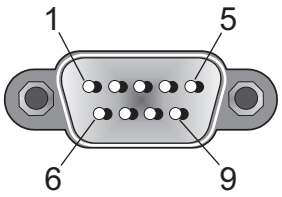
Crossover Wiring

If the twisted-pair cable is to join two ports and either both ports are labeled with an “X” (MDI-X) or neither port is labeled with an “X” (MDI), a crossover must be implemented in the wiring.



Console Port Pin Assignments

The DB-9 console port on the front panel of the access point is used to connect to the access point for out-of-band console configuration. The command-line configuration program can be accessed from a terminal, or a PC running a terminal emulation program. The pin assignments and cable wiring used to connect to the console port are provided in the following table.



10/100BASE-TX MDI and MDI-X Port Pinouts		
Switch’s 9-Pin Serial Port	**Null Modem**	**PC’s 9-Pin DTE Port**
2 RXD	<---------RXD ----------	3 TxD
3 TXD	----------TXD ---------->	2 RxD
5 SGND	----------SGND ----------	5 SGND

Note: The left hand column pin assignments are for the male DB-9 connector on the access point. Pin 3 (TXD or “transmit data”) must emerge on the management console’s end of the connection as RXD (“receive data”).

C

Specifications

Maximum Channels

802.11a:

RBT-4102-LIC
US & Canada: 13 (normal mode), 5 (turbo mode), 3 (in 4.9 GHz licensed mode)

802.11b/g:

RBT-4102-LIC
FCC/IC: 1-11

Data Rate

802.11a:
Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel
Turbo Mode: 12, 18, 24, 36, 48, 54, 96, 108 Mbps per channel
802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11b: 1, 2, 5.5, 11 Mbps per channel

Modulation Type

802.11a: BPSK, QPSK, 16-QAM, 64-QAM
802.11g: CCK, BPSK, QPSK, OFDM
802.11b: CCK, BPSK, QPSK

Network Configuration

Infrastructure

Operating Frequency

802.11a:
5.15 ~ 5.25 GHz (lower band) US
5.25 ~ 5.35 GHz (middle band) US
5.725 ~ 5.825 GHz (upper band) US
4.955 ~ 4.975 GHz (FCC licensed mode) US

802.11b/g:
2.4 ~ 2.4835 GHz (US)

AC Power Adapter

Input: 100-240 AC, 50-60 Hz
Output: 48 VDC, 0.38 A

Unit Power Supply

DC Input: 48 VDC, 0.38 A maximum
Input voltage: 48 volts, 0.27 A, 12.95 watts
Power consumption: 9.6 W maximum

PoE (DC)

Input voltage: 48 volts, 0.27A, 12.95 watts

Note: Power can also be provided to the access point through the Ethernet port based on IEEE 802.3af Power over Ethernet (PoE) specifications. When both PoE is provided and the adapter is plugged in, AC power will be turned off.

Physical Size

21.83 x 13.73 x 3.27 cm (8.60 x 5.40 x 1.29 in)

Weight

0.687 kg (1.514 lbs)

LED Indicators

Power, Ethernet Link/Activity, 11a and 11g Wireless Link/Activity

Network Management

Web-browser, RS232 console, Telnet, SSH, SNMP

Temperature

Operating: -5 to 50 °C (23 to 122 °F)
Storage: 0 to 70 °C (32 to 158 °F)

Humidity

15% to 95% (non-condensing)

Compliances

RBT-4102-LIC
FCC Class B (US)

Radio Signal Certification

RBT-4102-LIC
FCC Part 15C 15.247, 15.207 (2.4 GHz)
FCC Part 15E 15.407 (5 GHz)
FCC Part 90

Safety

UL/CUL (CSA 22.2 No. 60950-1 & UL60950-1)
EN60950-1 (TÜV/GS), EN60601, IEC60950-1 (CB)

Standards

IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX,
IEEE 802.11a, b, g

Sensitivity

IEEE 802.11a	Sensitivity (GHz - dBm)			
Modulation/Rates	**5.15-5.250**	**5.25-5.350**	**5.50-5.700**	**5.725-5.825**
BPSK (6 Mbps)	-88	-88	-88	-88
BPSK (9 Mbps)	-87	-87	-87	-87
QPSK (12 Mbps)	-86	-86	-86	-86
QPSK (18 Mbps)	-83	-83	-83	-83
16 QAM (24 Mbps)	-80	-80	-80	-80
16 QAM (36 Mbps)	-76	-76	-76	-76
64 QAM (48 Mbps)	-73	-73	-73	-73
64 QAM(54 Mbps)	-70	-70	-70	-70

IEEE 802.11g	
Data Rate	**Sensitivity (dBm)**
6 Mbps	-88
9 Mbps	-86
12 Mbps	-85
17 Mbps	-84
24 Mbps	-80
36 Mbps	-76
48 Mbps	-73
54 Mbps	-70

IEEE 802.11b	
Data Rate	**Sensitivity (dBm)**
1 Mbps	-90
2 Mbps	-89
5.5 Mbps	-87
11 Mbps	-85

Transmit Power

IEEE 802.11a	Maximum Output Power (GHz - dBm)			
Data Rate	**5.15-5.250**	**5.25-5.350**	**5.50-5.700**	**5.725-5.825**
6 Mbps	20	20	20	19
9 Mbps	20	20	20	19
12 Mbps	20	20	20	19
8 Mbps	20	20	20	19
24 Mbps	20	20	20	19
36 Mbps	20	20	19	19
48 Mbps	19	19	18	18
54 Mbps	18	18	17	16

IEEE 802.11g	Maximum Output Power (GHz - dBm)		
Data Rate	**2.412**	**2.417~2.467**	**2.472**
6 Mbps	20	20	20
9 Mbps	20	20	20
12 Mbps	20	20	20
18 Mbps	20	20	20
24 Mbps	20	20	20
36 Mbps	20	20	20
48 Mbps	20	20	20
54 Mbps	19	19	19

IEEE 802.11b	Maximum Output Power (GHz - dBm)		
Data Rate	**2.412**	**2.417~2.467**	**2.472**
1 Mbps	20	20	20
2 Mbps	20	20	20
5.5 Mbps	20	20	20
11 Mbps	20	20	20

Operating Range

Note: The operating range distances listed in the following tables are for typical environments only. Operating ranges can vary considerably depending on factors such as local interference and barrier composition. It is recommended to do a site survey to determine the maximum ranges for specific access point locations in your environment.

802.11a Wireless Distance Table							
Speed and Distance Ranges[1]							
54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	9 Mbps	6 Mbps
27 m 89 ft	40 m 132 ft	46 m 152 ft	55 m 182 ft	60 m 198 ft	66 m 218 ft	76 m 251 ft	80 m 264 ft

[1] A typical environment (office or home) with floor to ceiling obstructions between the access point and clients.

802.11g Wireless Distance Table											
Speed and Distance Ranges[1]											
54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	11 Mbps	9 Mbps	6 Mbps	5 Mbps	2 Mbps	1 Mbps
43 m 141 ft	50 m 164 ft	57 m 187 ft	63 m 207 ft	67 m 220 ft	71 m 233 ft	75 m 246 ft	77 m 253 ft	81 m 266 ft	85 m 279 ft	85 m 279 ft	85 m 279ft

[1] A typical environment (office or home) with floor to ceiling obstructions between the access point and clients.

802.11b Wireless Distance Table			
Speed and Distance Ranges[1]			
11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
70 m 230 ft	75 m 246 ft	85 m 279 ft	85 m 279 ft

[1] A typical environment (office or home) with floor to ceiling obstructions between the access point and clients.

External Antennas

The RBT-4102-LIC has been certified by the FCC, for use in the United States, to operate with these antennas:

Note: High gain point to point antenna, model RBTES-AH-P23M (Gain 23 dBi), is certified under specific point-to-point condition and the use of point-to-multipoint systems, omnidirectional applications, and multiple co-related intentional radiators transmitting the same information is prohibited.

FCC External Antenna Configurations		
Antenna Model	**Antenna Type**	**Antenna Gain**
RBT4K-AG-IA	2.4–2.5 GHz Omnidirectional Indoor Range Extender	1 dBi with 8 ft. cable
	5.15-5.35 GHz Omnidirectional Indoor Range Extender	
	5.725–5.825 GHz Omnidirectional Indoor Range Extender	
RBTES-AH-M10M	5.725–5.825 GHz Omnidirectional, outdoor	10 dBi
RBTES-AH-P23M	5.725-5.825 GHz Directional, outdoor	23 dBi
RBTES-AW-S1590M	4.9- 5.35 GHz Adjustable Sector, outdoor	15 dBi/90°
	5.4-5.7 GHz Adjustable Sector, outdoor	16 dBi/60°

Index

W