RoamAbout™

Wireless Networking

Access Point 3000
Hardware Installation Guide

P/N 9033978-01

enterasys™

Networks that Know

Electrical Hazard: Only qualified personnel should perform installation procedures.

Riesgo Eléctrico: 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: 9033978-01 April 2005

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

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

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

Dokumentation http://www.enterasys.com/support/manuals

Radio Certification and Regulatory Information
Zertifizierung für Funkgeräte und gesetzliche Vorschriften

Caution: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Precaución: Cualquier cambio o modificación a este dispositivo sin la aprobación del organismo autorizado, puede anular el derecho del usuario a operar el equipo.

Achtung: Änderungen oder Modifikationen, die an diesem Gerät ohne Zustimmung der verantwortlichen Partei vorgenommen werden, können die Berechtigung des Benutzers zum Betrieb des Geräts ungültig machen.

This document provides the regulatory information and technical specifications for the RoamAbout 802.11a/b/g RBT3K-AG.

To ensure that you have the latest version of this document, check the Website: www.enterasys.com/products/wireless.

Dieses Dokument enthält die gesetzlichen Vorschriften und technischen Daten für RoamAbout 802.11a/b/g RBT3K-AG.

Die aktuelle Version dieses Dokuments finden Sie auf der Website: www.enterasys.com/products/wireless.

Europe - European Union Notice

All products with the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).

- EN 55022:1998 (CISPR 22)
- EN 55024:1998 (IEC61000-4-2,3,4,5,6,8,11)
- EN 61000-3-2:2000 (IEC610000-3-2)
- EN 61000-3-3:1995 (IEC610000-3-3)
- EN 60950 Januar 2000 (IEC60950)

Products labeled with the CExxxx or the CE alert marking contain a radio transmitter that complies with the R&TTE-Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards).

- EN 300 328-1 Dezember 2001 V1.3.1
- EN 300 328-2 Dezember 2001 V1.2.1
- EN 301 893 August 2003 V1.2.3
- EN 301 489-1 August 2002 V1.2.1
- EN 301 489-17 August 2000 V1.2.1
- EN 60950 (IEC60950) Januar 2000

To determine the type of transmitter, check the identification label on your Wireless LAN Product.

Europa – Hinweis der Europäischen Union

Alle Artikel mit dem CE-Zeichen erfüllen die Anforderungen der EMV-Richtlinie (89/336/EEC) und der Niederspannungsrichtlinie (73/23/EEC) der EU-Kommission. Die Übereinstimmung mit diesen Richtlinien schließt die Konformität mit den folgenden europäischen Normen ein (die entsprechenden internationalen Normen sind in Klammern angegeben).

- EN 55022:1998 (CISPR 22) – Funkstörungen
- EN 55024:1998 (IEC61000-4-2,3,4,5,6,8,11)
- EN 61000-3-2:2000 (IEC610000-3-2)
- EN 61000-3-3:1995 (IEC610000-3-3)
- EN 60950 Januar 2000 (IEC60950)

Ein Artikel, der mit CExxxx oder dem CE-Warnhinweis gekennzeichnet ist, enthält einen Funksender, der den Anforderungen der R&TTE-Richtlinie (1999/5/EC) der EU-Kommission entspricht. Die Übereinstimmung mit dieser Richtlinie schließt die Konformität mit den folgenden europäischen Normen ein (die entsprechenden internationalen Normen sind in Klammern angegeben).

- EN 300 328-1 December 2001 V1.3.1
- EN 300 328-2 December 2001 V1.2.1
- EN 301 893 August 2003 V1.2.3
- EN 301 489-1 August 2002 V1.2.1
- EN 301 489-17 August 2000 V1.2.1
- EN 60950 (IEC60950) January 2000

Den Typ des Senders entnehmen Sie dem Kennzeichnungsetikett Ihres drahtlosen LAN-Geräts.

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 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.

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 or more 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 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 minimum distance 20cm between the radiator and your body.

If the RBT3K-AG or RBT3K-AG-G device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Enterasys Networks declares that the RBT3K-1G, RBT3K-AG, and RBT3K-AG-G (RoamAbout Access Point 3000) are limited in the 2.4 GHz band on channel 1-11 by specified firmware controlled in USA.

Canada - Industry Canada (IC)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI Notice

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Channel Information

802.11a	• Europe: 19 non-overlapping channel (5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz) • Japan: 4 non-overlapping channels (5.15 ~ 5.25 GHz) • US/Canada:12 non-overlapping channels (5.15 ~ 5.35 GHz, 5.725 ~ 5.825 GHz)
802.11b/g	• Major European countries: 13 (1 ~ 13) • Japan: 14 (1~13 or 14) • US/Canada: 11 (1 ~ 11)

Country Specific Power Limits and Restrictions

~~A~~	~~B~~	~~DK~~	~~FIN~~	**Member states in EU with restrictive use for this product are crossed out!** ***Les états membres de l'Union Européenne avec une utilisation restrictive de ce produit sont rayés !*** **Mitgliedsstaaten der EU mit eingeschränkten Nutzungsrechten für dieses Produkt sind herausgestrichen** ***Gli Stati membri nella Comunità Europea (EU) con restrizioni sull'uso di questi prodotti sono contrassegnati di seguito!***
~~F~~	~~D~~	~~IRL~~	~~I~~	
~~CHE~~	~~NOR~~	~~NL~~	~~P~~	
~~S~~	~~UK~~	~~L~~	~~SR~~	
~~ISL~~	~~E~~			

N826

CE0560 Notice

CE 0560 !

Important Notice:
Low power radio LAN product operating in 2.4 / 5GHz band for Home and Office environments.
Please refer to flyer/manual for details on restrictions.

Notice Importante :
Produit réseau local radio basse puissance opérant dans la bande de fréquence 2.4 / 5 GHz pour les environnements bureautiques et résidentielles. Merci de vous référer au manuel pour les détails des restrictions

Wichtige Mitteilung
Low Power FunkLAN Produkt für den Home- und Office-Bereich, das im 2.4 / 5GHz Band arbeitet. Weitere Informationen bezüglich Einschränkungen finden Sie im Datenblatt/Handbuch

Nota Importante:
Apparati Radio LAN a bassa potenza, operanti a 2.4 / 5 GHz, per ambienti domestico ed ufficio.
Fare riferimento alla Guida d'Utente per avere informazioni dettagliate sulle restrizioni

Enterasys herby declares this Radio LAN device is in compliance with the essential requirements and other provisions of the R&TTE-Directive 1999/5/EC. A copy of this signed declaration can be obtained by contact Enterasys Networks, 50 Minuteman Road, Andover, MA 01810, USA. Attn: Wireless Group.

Enterasys erklärt hiermit, dass dieses LAN-Funkgerät die wesentlichen Anforderungen und sonstigen relevanten Vorschriften der R&TTE-Richtlinie 1999/5/EC erfüllt. Eine Kopie dieser unterzeichneten Erklärung erhalten Sie von Enterasys Networks, 50 Minuteman Road, Andover, MA 01810, USA. Attn: Wireless Group.

Approved Countries

The following table lists the approved countries, Access Point 3000 part numbers, and if applicable, the approval numbers and references.

Approved Country	Part Number	Approval Number	Approval Reference
Australia	RBT3K-AG		
Canada	RBT3K-AG	IC: 3857A-RBT3KAG	
Europe	RBT3K-AG		
Hong Kong	RBT3K-AG		
Japan	RBT3K-AG	201NY03215095	
Mexico	RBT3K-AG		
USA	RBT3K-AG	HEDWA610260	

Approved Countries Configuration

The following table provides the configuration for approved countries.

Country	Part Number	IEEE 802.11a Only	IEEE 802.11 b/g Only	Comments
Austria (A)	RBT3K-AG	**5150 – 5350-MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** Not permitted (Military band)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Belgium (B)	RBT3K-AG	Not approved	Not approved	
Denmark (DK)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 -2483.5 MHz** < 100 mW EIRP	
Estonia (ES)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	

Country	Part Number	IEEE 802.11a Only	IEEE 802.11 b/g Only	Comments
Finland (FIN)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
France (F)	RBT3K-AG	**5150 – 5350-MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** Under examination (Not permitted)	1>**2400 -2483.5 MHz** < 100 mW eirp (Indoors only) 2>**2400 – 2483.5 MHz** < 100 mW (Indoors only) 3>**2400 – 2483.5 MHz** < 100 mW (Indoors only)	1> Metropolitan France 2> Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte 3> Réunion and Guyana
Germany (D)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Greece (EL)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Hungary (HU)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Iceland (ISL)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Ireland (IRL)	RBT3K-AG	**5150 – 5350-MHz** < 200 mW EIRP (Indoors only)	1>**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	1> provision of services to the public is permitted. Public service provider is required to hold an appropriate Telecommunications License (ref. ODTR 98/44R).

Country	Part Number	IEEE 802.11a Only	IEEE 802.11 b/g Only	Comments
Italy (I)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** 1 W EIRP (Indoors only)	1>**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	1> If used outside of own premises, general authorization is required.
Latvia (LA)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only	1>**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	1> If used outside of own premises, general authorization is required.
Lithuania (LT)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Luxembourg (L)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) 1>**5470 – 5725 MHz** < 1 W EIRP (Indoors only)	1>**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	1> System provider for third party traffic may require a Telecommunications Act License.
Norway (NOR)	RBT3K-AG	**5150 – 5350-MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only) Not permitted at Ny-Ålesund.	* Norwegian Post and Telecommunications Authority: List of radio communications equipment that does not have to be notified according to Art. 6.4 in the R&TTE Directive (1999/5/EC) > RLAN (2.4 – 2.483.5 GHz, 5.15 – 5.35 GHz & 5.47 – 5.725 GHz)
Netherlands (NL)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors)	
Poland (PO)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	

Country	Part Number	IEEE 802.11a Only	IEEE 802.11 b/g Only	Comments
Portugal (P)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) 5470 – 5725 MHz < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Slovenia (SA)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) 5470 – 5725 MHz < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Slovakia (SK)	RBT3K-AG	**5150 – 5350-MHz** < 120 mW EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Spain (E)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors)	
Sweden (S)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
Switzerland (CHE)/ Liechtenstein (LI)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** Not implemented (Exclusive Military band)	**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	
United Kingdom (UK)	RBT3K-AG	**5150 – 5350 MHz** < 200 mW EIRP (Indoors only) **5470 – 5725 MHz** < 1 W EIRP (Indoors only)	1>**2400 – 2483.5 MHz** < 100 mW EIRP (Indoors only)	1> System provider for third party traffic may require a Wireless Telegraphy and/or Telecommunications Act License.

The user is responsible for compliance with the conditions of assignment and for the consequences of any violation, corrective action, or offense.

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

Appendix B: Default Settings

Appendix C: Cables and Pin-outs

Appendix D: Troubleshooting

Figures

Tables

About This Guide

Purpose of This Manual

This manual describes how to install the RoamAbout Access Point 3000. It also includes basic configuration information, problem solving, and connector pin assignment information.

Intended Audience

This manual is intended for use by personnel who will install and set up the RoamAbout Access Point 3000.

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.

Associated Documents

You can download the documentation from the Enterasys Networks Web site.

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

Check the Web site regularly for product upgrades:

http://www.enterasys.com/products/wireless

Document Conventions

The following icons are used in this document:

Electrical Hazard: Warns against an action that could result in personal injury or death.

Riesgo Electrico: Advierte contra una acción que pudiera resultar en lesión corporal o la muerte debido a un riesgo eléctrico.

Elektrischer Gefahrenhinweis: Warnung vor sämtlichen Handlungen, die zu Verletzung von Personen oder Todesfällen – hervorgerufen durch elektrische Spannung – führen können!

Caution: Contains information essential to avoid damage to the equipment.

Precaución: Contiene información esencial para prevenir dañar el equipo.

Achtung: Verweißt auf wichtige Informationen zum Schutz gegen Beschädigungen.

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:	www.enterasys.com/support
Phone:	(603) 332-9400 1-800-872-8440 (toll-free in the U.S. and Canada) For the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support/gtac-all.html
Email:	**support@enterasys.com** To expedite your message, please type **[wireless]** in the subject line.
To send comments concerning this document to the Technical Publications Department: **techpubs@enterasys.com** To expedite your message, please include the document Part Number in the email message.	

Before calling Enterasys Networks, please 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
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (for example, layout and 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

1

Introduction

Overview

The Enterasys Networks Wireless Access Point 3000 is an IEEE 802.11a/b/g (RBT3K-AG & RBT3K-AG-G), or an IEEE 802.11b/g only (RBT3K-1G), access point that provides transparent, wireless high-speed data communications between the wired LAN and fixed, portable 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, 802.11b, and 802.11g technology, this access point can easily replace a 10 Mbps Ethernet connection or seamless integration into a 10/100 Mbps Ethernet LAN.

In addition, the access point offers full network management capabilities through an easy to configure Web interface, and a command line interface for initial configuration and troubleshooting.

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) modulation technology to achieve a communication rate of up to 11 Mbps.

The access point also 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).

Kit Checklist

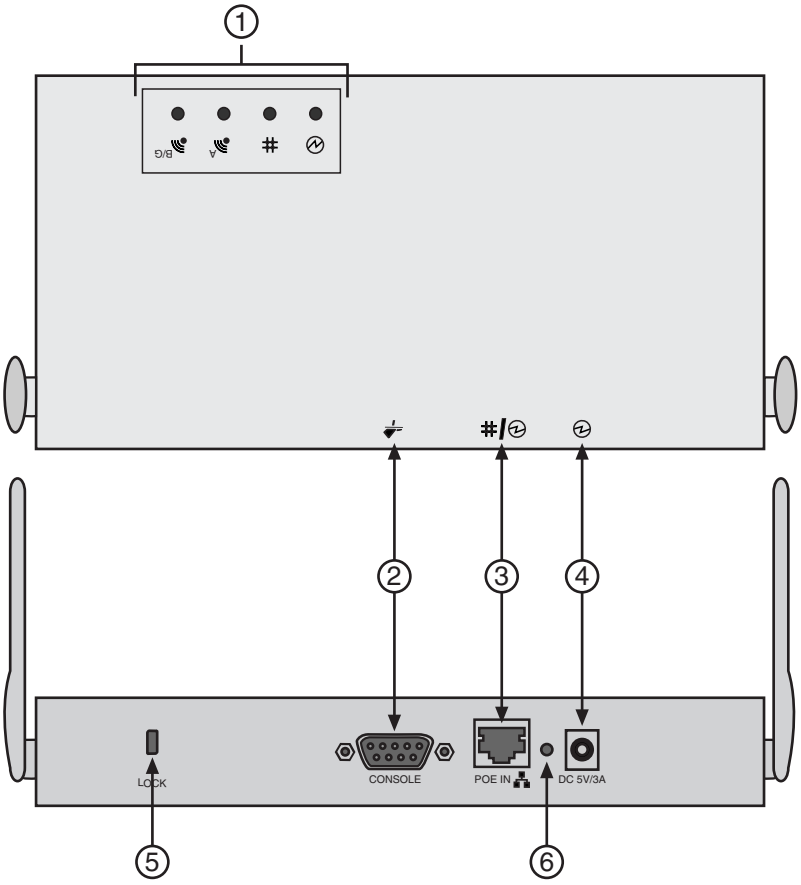
Physically inspect all cartons for shipping damage. Report any damage to your shipping carrier. Also verify that you have received the correct basic components and options listed. Report any discrepancies to your Enterasys Sales Representative.

- RoamAbout Access Point 3000
- *RoamAbout Access Point 3000 Hardware Installation Guide*
- One RS-232 console cable
- One 5.1 Vdc power adapter and power cord
- Plastic cover
- Four rubber feet
- Security clip (used with ceiling mount)
- Mounting bracket and two ceiling mount clips

Hardware Description

Figure 1-1 displays the top view and back panel of the Access Point 3000.

Figure 1-1 Access Point 3000



1 Status indicators for Access Point and the 802.11a and 802.11b/g interfaces
2 Console Port Connector
3 RJ-45 Port PoE Connector
4 Power Supply Connector
5 Security Slot
6 Reset Button

Component Description

Antennas

The access point includes two antennas for wireless communications. The signal transmitted from both antennas is identical, but only the best signal received on one of the antennas is used. The antennas transmit the outgoing signal along a horizontal plane perpendicular to the antenna (in the shape of a toroidal sphere, or a donut). The antennas should be adjusted to different angles to provide better coverage.

LED Indicators

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

Figure 1-2 LED Indicators

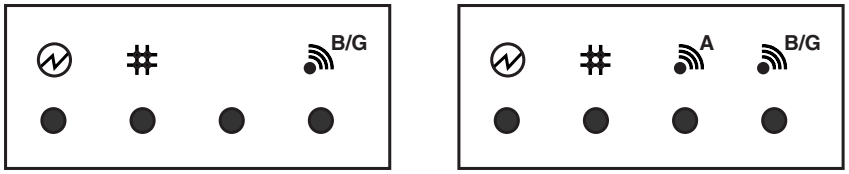


Table 1-1 LED Indicator Descriptions

LED	Status	Description
Power	On	Indicates that the power is on.
	Flashing	Indicates: • running a self-test • loading software program
	Flashing (Prolonged)	Indicates system errors
Ethernet Link	On	Indicates a valid 10/100 Mbps Ethernet cable link.
	Flashing	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.
802.11a Radio Interface 1	On	Indicates a valid 802.11a wireless link.
	Very Slow Flashing	Searching for network association.
	Slow Flashing	Associated with network but no activity.
	Fast Flashing	Indicates that the access point is transmitting or receiving data through wireless links. Flashing rate is proportional to network activity.

Table 1-1 LED Indicator Descriptions (continued)

LED	Status	Description
B/G 802.11g or 802.11b Radio Interface 2	On	Indicates a valid 802.11g or 802.11b wireless link.
	Very Slow Flashing	Searching for network association.
	Slow Flashing	Associated with network but no activity.
	Fast Flashing	Indicates that the access point is transmitting or receiving data through wireless links. Flashing rate is proportional to network activity.

Security Slot

The access point includes a security slot on the rear panel. You can prevent unauthorized removal of the access point by wrapping a 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 in Appendix C. 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 uses an MDI (for example, internal straight-through) pin configuration. You can use a straight-through twisted-pair cable to connect the port to most network interconnection devices, such as a switch or router that provide MDI-X ports. However, when connecting the access point to a workstation or other device that do not have MDI-X ports, you must use a crossover twisted-pair cable.

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" on page 1-5 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 to restore the factory default configuration. If you hold down the button for less than five seconds, the access point will perform a hardware reset. If you hold down the button for five seconds or more, **ALL** configuration changes you 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 supply 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.

Features and Benefits

The features and benefits of the Access Point 3000 include the following:

- Local network connection via 10/100 Mbps Ethernet ports or 54 Mbps wireless interface (supporting up to 250 mobile users)
- IEEE 802.11a, 802.11b, and 802.11g compliant
- Advanced security through 64/128/152-bit Wired Equivalent Protection (WEP) encryption, IEEE 802.1x port authentication, Wi-Fi Protected Access (WPA), AES (802.11i ready), SSID broadcast disable, remote authentication via RADIUS server, and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network
- Provides seamless roaming within the IEEE 802.11a, 802.11b, and 802.11g WLAN environment
- Automatically selects the available channel at power-up.

Applications

The Wireless products offer a high speed, reliable, cost-effective solution for 10/100 Mbps wireless Ethernet client access to the network in applications such as:

- Remote access to corporate network information
- E-mail, file transfer, and terminal emulation
- Difficult-to-wire environments
- Historical or old buildings, asbestos installations, and open areas where wiring is difficult to employ.
- Frequently changing environments
- Retailers, manufacturers, and banks that frequently rearrange the workplace or change location
- Temporary LANs for special projects or peak times
- Trade shows, exhibitions and construction sites which need temporary setup for a short time period. Retailers, airline and shipping companies that need additional workstations for a peak period. Auditors who require workgroups at customer sites.
- Access to databases for mobile workers, for example: doctors, nurses, retailers, or white-collar workers who need access to databases while being mobile in a hospital, retail store, or an office campus.

2

Hardware Installation

Preparing to Install

Choose a proper place for the access point. 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 *RoamAbout Access Point 3000 Configuration Guide*). Normally, the higher you place the access point, the better the performance.

Electrical Hazard: Only qualified personnel should perform installation procedures.

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

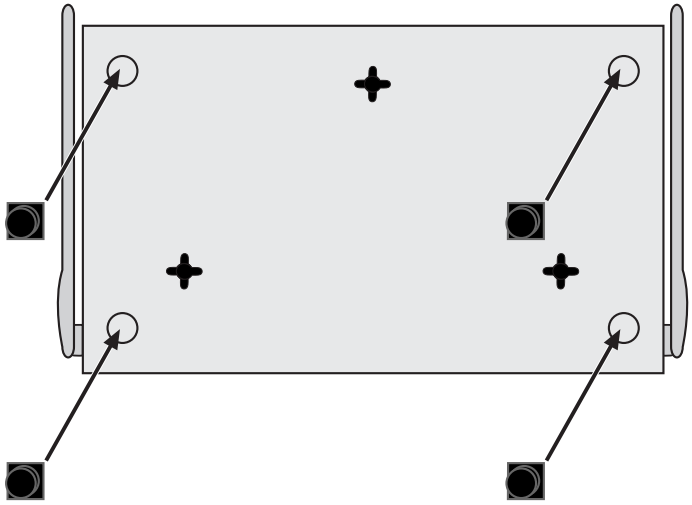
Elektrischer Gefahrenhinweis: Installationen sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.

Mounting the Access Point

The access point can be mounted on any horizontal surface, wall or ceiling.

Mounting on a Horizontal Surface

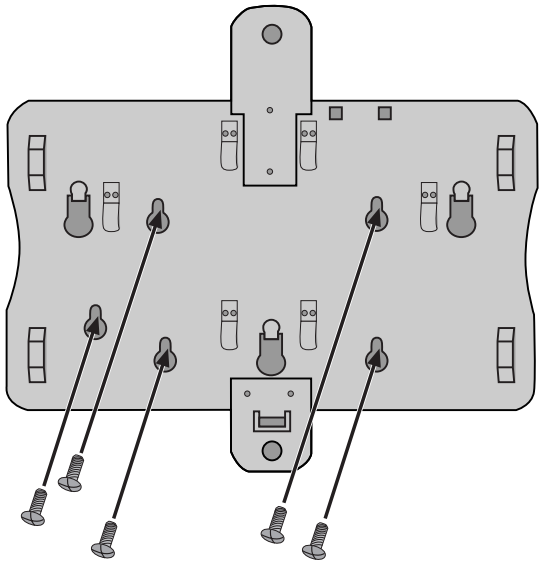
To keep the access point from sliding on the surface, attach the four rubber feet provided in the kit to the embossed circles on the bottom of the access point, as shown below.



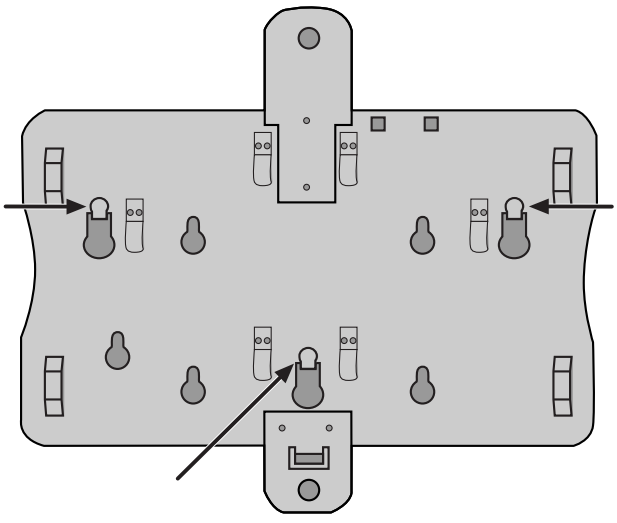
Mounting on a Wall

To mount the Access Point 3000 on a wall, perform the following steps:

1. Locate at least two mounting holes/slots on the mounting bracket that line up with a wall stud.
2. Use two screws to secure the flat side of the mounting bracket to the wall stud. Use plastic anchors, or self-anchoring screws (not included) to secure the mounting bracket to the wallboard, as shown below.

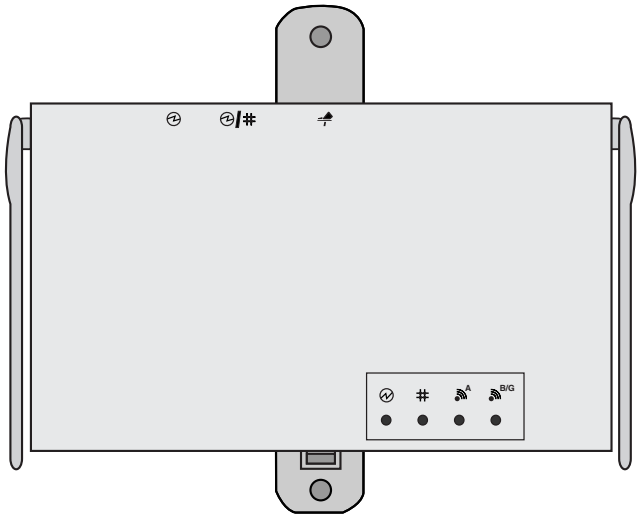


3. Slide the access point over the mounting bracket to locate the three raised tabs, as shown in the following figure.



4. Slide the access point over the raised tabs and lock them into place, as shown in the following figure.

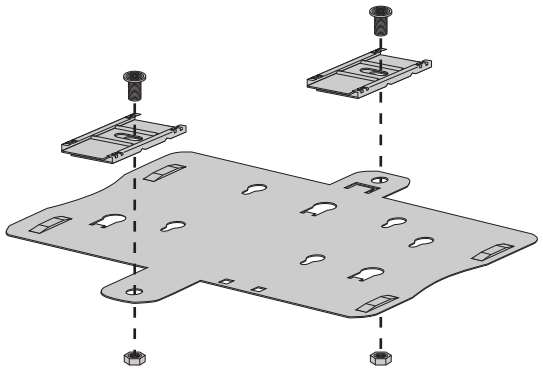
Note: The access point will not slide if it was successfully locked into place.



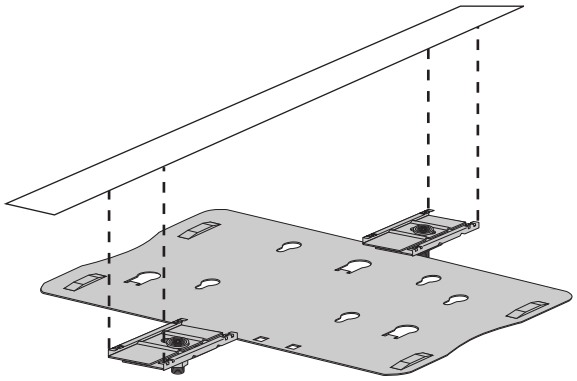
Mounting on the Ceiling

To mount the Access Point 3000 on the ceiling, perform the following steps:

1. If you received washers with your kit, discard them.
2. Attach the mounting clips to the mounting bracket as shown below. Ensure that the screws line up with the holes on the tab of each side of the mounting bracket. **Ensure that the nuts are secure, but do not** tighten them.



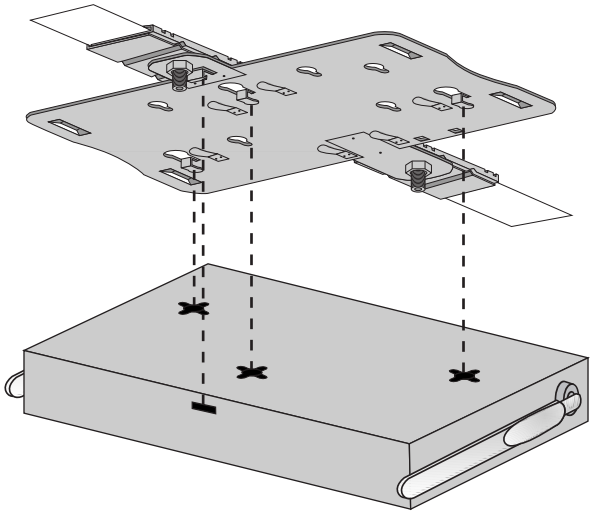
3. Slide the mounting clips over the ceiling support, as shown below.



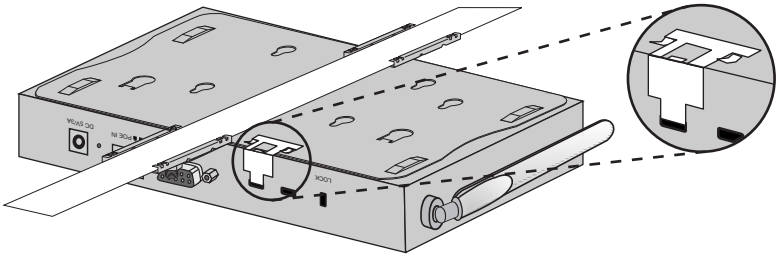
4. Tighten the bolts securely in place.

5. Slide the access point over the mounting bracket to locate the three raised tabs. and lock them in place, as shown below.

Note: The access point will not slide if it was successfully locked into place.



6. Attach the locking clip to the mounting bracket and to the access point, as shown below.



Removing the Access Point from the Mounting Bracket

To remove the access point from the mounting bracket:

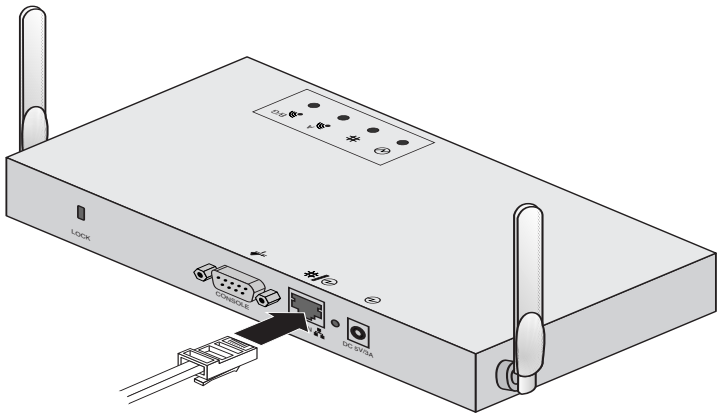
1. Remove the locking clip, applicable.
2. Press down on the access point to compress the locking tabs.
3. Slide the access point off the mounting bracket.

Connecting the Cables

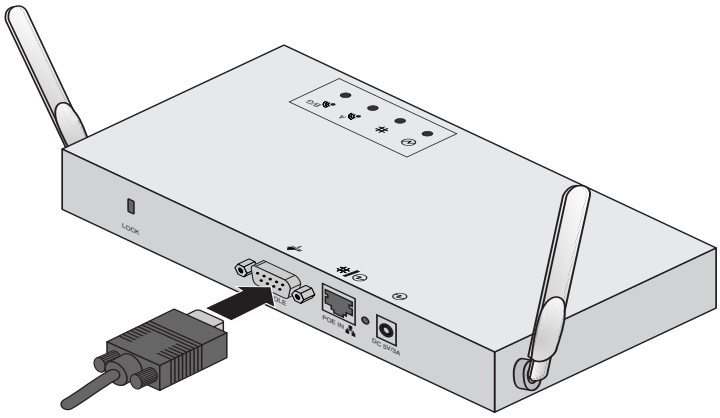
Note: Refer to Appendix C for cabling and pin-out information.

Perform the following steps to connect the cables and power on the access point:

1. 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, 4, or 5 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 uses an MDI pin configuration, you must use a straight-through cable for network connections to hubs or switches that only have MDI-X ports, and crossover cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDI/MDI-X operation, you can use either straight-through or crossover cable.

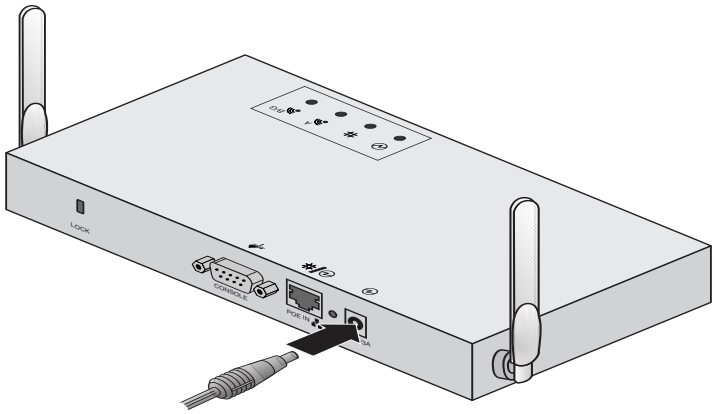


2. Connect the Power Cord. Connect the power adapter to the access point, and the power cord to an AC power outlet. Otherwise, the access point can derive its operating power directly from the RJ-45 port when connected to a device that provides IEEE 802.3af compliant Power over Ethernet (PoE).

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

   Precaución: SÓLO se debe utilizar el adaptador de corriente que fue incluido con este punto de acceso. De lo contrario, el producto podría dañarse.

   Achtung: Verwenden Sie AUSSCHLIESSLICH das im Lieferumfang enthaltene Netzteil für diesen Access Point. Anderenfalls besteht die Gefahr, dass das Produkt beschädigt wird.



3. Observe the Self Test. When you power on the access point, verify that the PWR indicator stops flashing and remains on, and that the other indicators start functioning as described under "LED Indicators" on page 1-3. If the PWR LED does not stop flashing, the self test has not completed correctly.

4. Position the Antennas. The antennas emit signals along a plane perpendicular to the antenna (with the propagation pattern shaped as a toroidal sphere), and provide more effective coverage when positioned along different axes. For example, you might position the antennas 45 to 90 degrees from each other.

   The access point also compares the strength of an incoming signal on both antennas, and uses the antenna receiving the stronger signal to communicate with a wireless client.

5. Place the plastic cover over the access point (if you are not using the console cable), and then snap it in place.

6. Lock the access point in place (optional). 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

7. Proceed to Chapter 3 to configure the Access Point 3000.

3

Initial Configuration

Overview

The Enterasys Networks RoamAbout Access Point 3000 includes a Web-based interface, and a direct connection to the console port for CLI management. You can also manage the Access Point 3000 using an SNMP manager, such as Enterasys Networks NetSight Atlas.

You can perform the initial configuration steps through the CLI or the Web interface.

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.

If you utilize a DHCP server to provision new elements in your IP network, use your DHCP server or other utilities to determine the IP address assigned to this access point. Then, use the DHCP assigned IP address to connect to the access point.

Using the CLI

The Access Point 3000 includes 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 null-modem cable that complies with the wiring assignments shown in Appendix C.

Required Connections

To connect to the console port, complete 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. See 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 will be displayed.

   For a description of how to use the CLI and a list of all the CLI commands refer to the *RoamAbout Access Point 3000 Configuration Guide*.

Initial Configuration Using the CLI

To use the CLI to minimally configure the access point, perform the following steps:

1. Make a serial connection to the access point's console port as described in the *RoamAbout Access Point 3000 Hardware Installation Guide*.
2. Use terminal emulation software to connect to the access point's CLI.
3. Enter **admin** for the user name, and **password** for the password to log in.

   The access point 3000 CLI prompt appears.

```
Username: admin
Password:********
RoamAbout 3000#
```

4. Set the Country Code. This restricts operation of the access point to the radio channels permitted for wireless networks in the specified country.

   a. Type **country ?** to display the list of countries.

```
RoamAbout 3000#country ?
WORD  Country code: AL-ALBANIA, DZ-ALGERIA, AR-ARGENTINA, AM-ARMENIA, AU-
AUSTRALIA, AT-AUSTRIA, AZ-AZERBAIJAN, BH-BAHRAIN, BY-BELARUS, BE-BELGIUM,
BZ-BELIZE, BO-BOLVIA, BR-BRAZIL, BN-BRUNEI_DARUSSALAM, BG-BULGARIA, CA-
CANADA, CL-CHILE, CN-CHINA, CO-COLOMBIA, CR-COSTA_RICA, HR-CROATIA, CY-
CYPRUS, CZ-CZECH_REPUBLIC, DK-DENMARK, DO-DOMINICAN_REPUBLIC, EC-ECUADOR,
EG-EGYPT, EE-ESTONIA, FI-FINLAND, FR-FRANCE, GE-GEORGIA, DE-GERMANY, GR-
GREECE, GT-GUATEMALA, HK-HONG_KONG, HU-HUNGARY, IS-ICELAND, IN-INDIA, ID-
INDONESIA, IR-IRAN,IE-IRELAND, IL-ISRAEL, IT-ITALY, JP-JAPAN, JO-JORDAN,
KZ-KAZAKHSTAN,KR-KOREA_REPUBLIC, KW-KUWAIT, LV-LATVIA, LB-LEBANON, LI-
LIECHTENSTEIN, LT-LITHUANIA, LU-LUXEMBOURG, MO-MACAU, MK-MACEDONIA, MY-
MALAYSIA, MX-MEXICO, MC-MONACO, MA-MOROCCO, NL-NETHERLANDS, NZ- KP-NORTH
KOREA, NO-NORWAY, OM-OMAN, PK-PAKISTAN, PA-PANAMA, PE-PERU, PH-
PHILIPPINES, PL-POLAND, PT-PORTUGAL, PR-PUERTO_RICO, QA-QATAR, RO-ROMANIA,
RU-RUSSIA, SA-SAUDI_ARABIA, SG-SINGAPORE, SK-SLOVAK_REPUBLIC, SI-
SLOVENIA, ZA-SOUTH_AFRICA, ES-SPAIN, SE-SWEDEN, CH-SWITZERLAND, SY-SYRIA,
TW-TAIWAN, TH-THAILAND, TR-TURKEY, UA-UKRAINE, AE-UNITED_ARAB_EMIRATES,
GB-UNITED_KINGDOM,US-UNITED_STATES,UY-URUGUAY,VE-VENEZUELA,VN-VIETNAM
RoamAbout 3000#country US
```

b. Determine the code for your country, and then type **country** followed by your country code (for example, **country US** for United States).

c. Reboot the RoamAbout Access Point 3000.

```
RoamAbout 3000#country US
Please reset the AP to make the country code change effective
RoamAbout 3000#reset board
Reboot system now? <y/n>: y
Username: admin
Password:********
RoamAbout 3000#
```

5. If your access point uses a DHCP assigned IP address go on 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 3000#configure
Enter configuration commands, one per line. End with CTRL/Z
RoamAbout 3000(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
RoamAbout 3000(if-ethernet)#
```

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

```
RoamAbout 3000(if-ethernet)#no ip dhcp
DHCP client state has changed. Please reset AP for change to take effect.
RoamAbout 3000(if-ethernet)#exit
RoamAbout 3000#reset board
Reboot system now? <y/n>: y
Username: admin
Password:********
RoamAbout 3000#configure
Enter configuration commands, one per line. End with CTRL/Z
RoamAbout 3000(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
RoamAbout 3000(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 3000(if-ethernet)#ip address ip-address netmask gateway
RoamAbout 3000(if-ethernet)#end
RoamAbout 3000(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.

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

```
RoamAbout 3000(config)#username JadaPerl
RoamAbout 3000(config)#password G7nq1Z
Confirm new password: G7nq1Z
RoamAbout 3000(config)#
```

7. Enable Management VLAN.

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.

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

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

```
RoamAbout 3000(config)#management-vlanid 10
RoamAbout 3000(config)#management-vlan enable
Reboot system now? <y/n>:y
Username: admin
Password:********
```

8. Refer to the *RoamAbout Access Point 3000 Configuration Guide* for advanced configuration information.

Using Web Management

To use the Web interface to minimally configure the access point, perform the following 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** (for more information about the username and password, refer to Refer to the *RoamAbout Access Point 3000 Configuration Guide* for advanced configuration information.

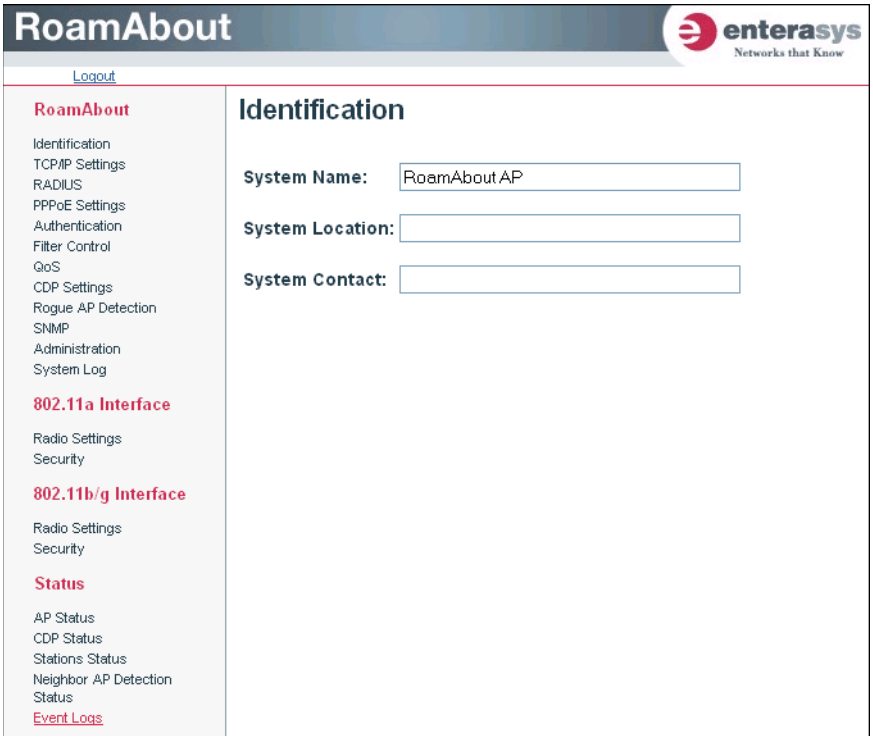
The Country Code page appears.

3. To set the Country, perform the following steps:
   a. Click the arrow in the **Country** pull-down menu to select the appropriate country, then click **Apply** at the bottom of the page.

      The access point prompts you to reset.

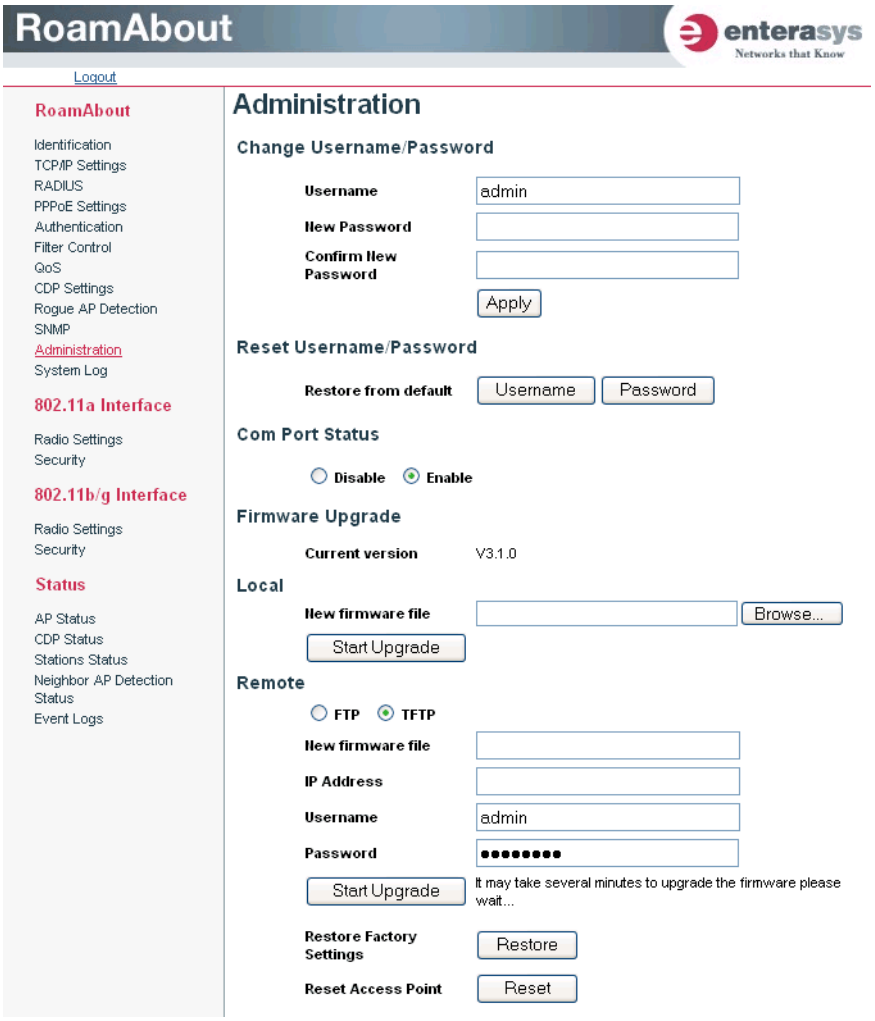
   b. Click **OK**.

      The Identification page appears.



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

The Administration page appears.



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

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

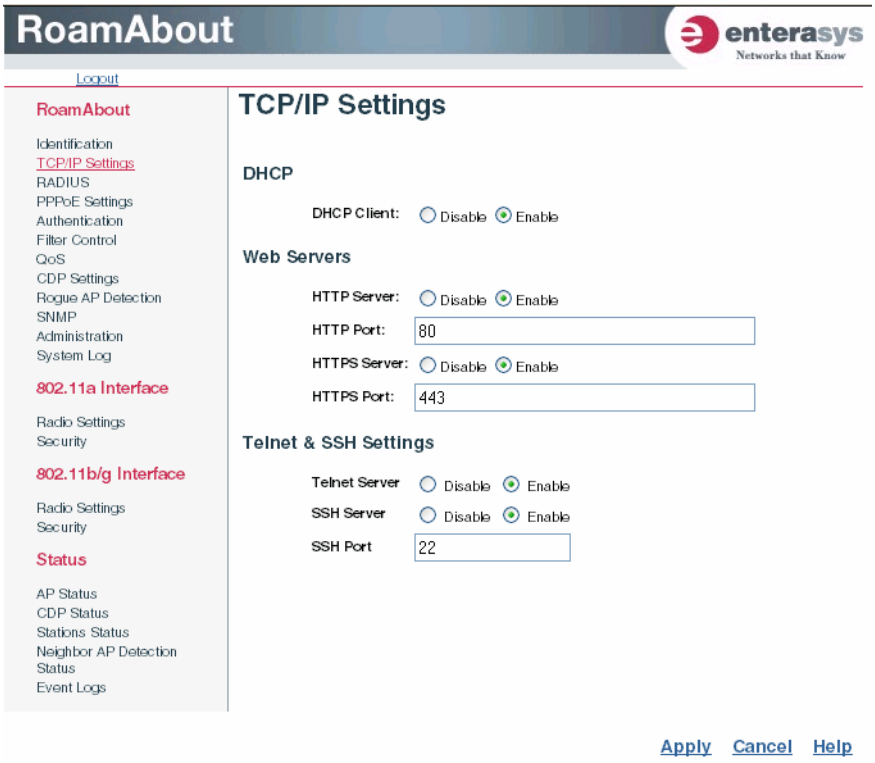
b. Click **OK**.

   The access point reboots and the Login window appears.

5. Enter the username **admin** and the password **password**, and click **LOGIN**.
6. To set a static IP address, perform the following steps:

   a. Click **TCP/IP Settings** from the menu on the left 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 **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**.

7. To set the username and password, perform the following steps:

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

      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.

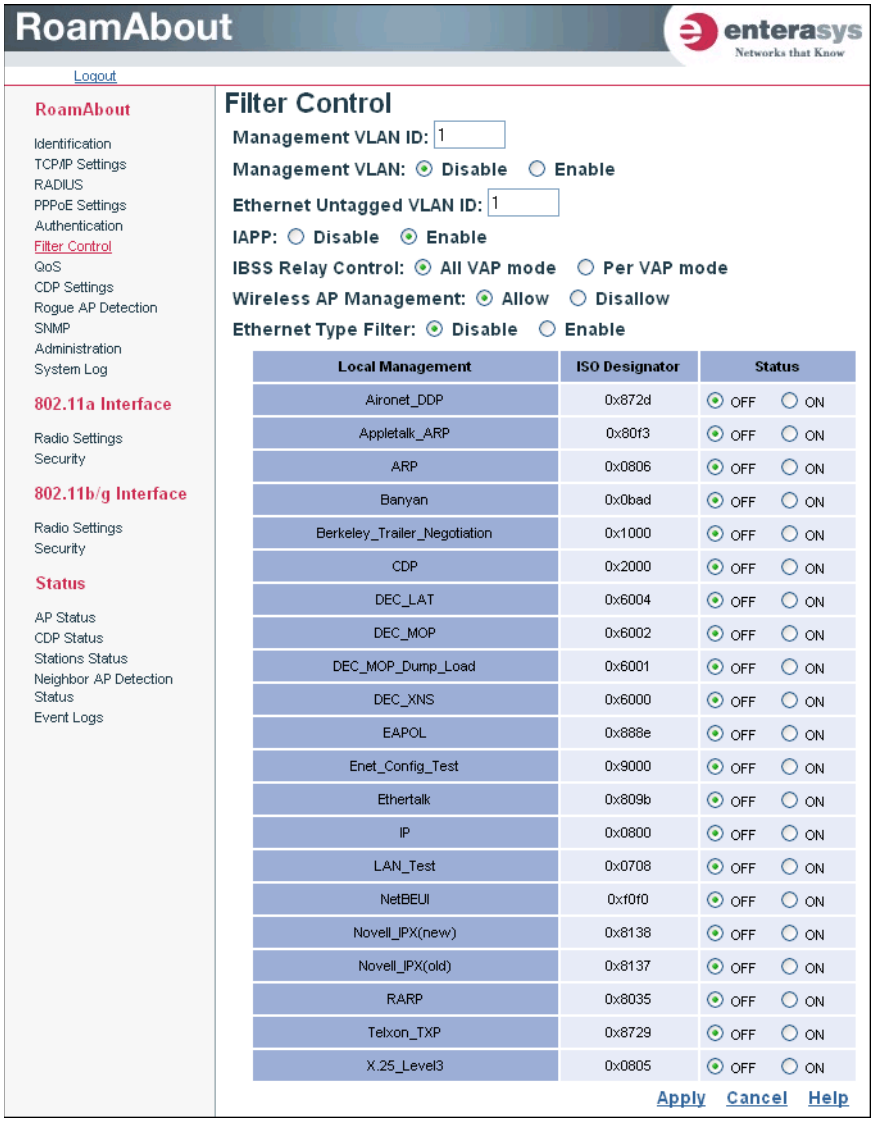
f. Click **OK**.

The Administration page appears.

8. Set management VLAN:

a. Click **Filter Control** from the menu on the left of the page.

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**.

9. Refer to the *RoamAbout Access Point 3000 Configuration Guide* for advanced configuration information.

A

Specifications

General Specifications

Maximum Channels

802.11a:

US & Canada: 13 (normal mode), 5 (turbo mode)

Japan: 4 (normal mode), 1 (turbo mode)

ETSI: 11 channels (normal mode), 4 (turbo mode)

802.11b/g:

FCC/IC: 1 to 11

ETSI: 1 to 13

France: 10 to 13

MKK: 1 to 14

Maximum Clients

250 if you are NOT using encryption or authentication.

120 if you ARE using encryption or authentication.

Operating Range

See "Maximum Distance Tables" on page D-3.

Data Rate

802.11a:

Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel

Turbo Mode: 12, 18, 24, 36, 48, 72, 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 to 5.25 GHz (lower band) US/Canada, Japan
- 5.25 to 5.35 GHz (middle band) US/Canada
- 5.725 to 5.825 GHz (upper band) US/Canada
- 5.50 to 5.70 GHz Europe

802.11b/g:

- 2.4 to 2.4835 GHz (US, Canada, ETSI)
- 2.4 to 2.497 GHz (Japan)

Power Supply

Input: 100 to 240 AC, 50 to 60 Hz

Output: 5.1 Vdc, 3A

Power consumption: 13.2 watts

802.3af compliant: Input voltage: 48 volts, 0.27A, 12.96 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, PoE 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

0.80 kg (1.76 lb)

LED Indicators

PWR (Power), Ethernet Link (Ethernet Link/Activity), 802.11a and 802.11g (Wireless Link/Activity)

Network Management

Web-browser, RS232 console, Telnet, SNMP

Temperature

Operating: 0°C to 55°C (32°F to 131 °F)

Storage: 0°C to 70 °C (32 °F to 158 °F)

Humidity

15% to 95% (non-condensing)

EMC Compliance (Class B)

FCC Class B (US)

ICES-003 (Canada)

VCCI (Japan)

RCR STD-33A

EN55024, EN5022

Radio Signal Certification

For the latest radio certification and regulatory information, go to http://www.enterasys.com/products/wireless/. The information is listed under County Approvals.

RBT3K-AG & RBT3K-AG-G 2.4 GHz & 5 GHz	**RBT3K-1G 2.4 GHz Only**
FCC part 15.247 (2.4 GHz)	FCC part 15.247 (2.4 GHz)
FCC part 15 15.407(b)	
RSS-210 (Canada)	RSS-210 (Canada)
EN 300.328-1 V1.3.1	EN 300.328-1 V1.3.1
EN 300.328-2 V1.2.1	EN 300.328-2 V1.2.1
EN 301 489-01: V.1.3.1	
EN 301 489-17: V.1.2.1	
EN 301 893: V.1.2.1	
MPT RCR std.33 (D33 1~13 Channel, T66 Channel 14)	MPT RCR std.33 (D33 1~13 Channel, T66 Channel 14)

Safety

CSA/NTRL (CSA 22.2 No. 950 & UL 1950)

EN60950 (TÜV/GS), IEC60950 (CB)

LVD/EN 60950

Plenum Rated UL2043

Standards

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

Sensitivity

802.11a

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)	-84	-84	-84	-84
16 QAM (24 Mbps)	-81	-81	-81	-81
16 QAM (36 Mbps)	-77	-77	-78	-78
64 QAM (48 Mbps)	-73	-73	-73	-73
64 QAM (54 Mbps)	-69	-70	-70	-67

802.11g

IEEE 802.11g	
Data Rate	**Sensitivity (dBm)**
6 Mbps	-88
9 Mbps	-87
12 Mbps	-86
17 Mbps	-85
24 Mbps	-81
36 Mbps	-77
48 Mbps	-72
54 Mbps	-70

802.11b

IEEE 802.11b	
Data Rate	**Sensitivity (dBm)**
1 Mbps	-93
2 Mbps	-90
5.5 Mbps	-90
11 Mbps	-87

Transmit Power

802.11a

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

802.11g

IEEE 802.11g	Maximum Output Power (GHz - dBm)		
Data Rate	2.412	2.417 to 2.467	2.472
6 Mbps	20	20	18
9 Mbps	20	20	18
12 Mbps	20	20	18
18 Mbps	20	20	18
24 Mbps	20	20	18
36 Mbps	20	19	17
48 Mbps	17	16	15
54 Mbps	15	14	13

802.11b

IEEE 802.11b	Maximum Output Power (GHz - dBm)		
Data Rate	2.412	2.417 to 2.467	2.472
1 Mbps	15	16	15
2 Mbps	15	16	15
5.5 Mbps	15	16	15
11 Mbps	15	16	15

B

Default Settings

This Appendix lists the access point system defaults.

To reset the access point defaults, refer to the CLI command "`reset configuration`" from the Exec level prompt. Refer to the *RoamAbout Access Point 3000 Configuration Guide*.

Feature	Parameter	Default
Identification	System Name	RoamAbout AP
Administration	User Name	admin
	Password	password
TCP/IP	DHCP	Enabled
	HTTP Server	Enabled
	HTTP Port	80
	HTTPS Server	Enabled
	HTTPS Port	443
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	Primary DNS Address	0.0.0.0
	Secondary DNS Address	0.0.0.0
RADIUS (Primary and Secondary)	IP Address	0.0.0.0
	Port	1812
	Key	
	Timeout	5 seconds
	Retransmit attempts	3
PPPoE	Settings	Disabled
	IP Allocation Mode	Automatically allocated
	Local IP Address	0.0.0.0
	Remote IP Address	0.0.0.0

Feature	Parameter	Default
MAC Authentication	MAC Authentication	Local MAC
	Local MAC System Default	Allow
	Local MAC Permission	Allow
802.1x Authentication	Status	Disabled
	Broadcast Key Refresh	0 minutes (disabled)
	Session Key Refresh	0 minutes (disabled)
	RADIUS Session Timeout	60 minutes
802.1x Supplicant	Status	Disabled
VLAN	Management VLAN ID	1
	VLAN	Disabled
Filter Control	IAPP	Enabled
	IBSS Relay	Allow
	Wireless AP Management	Allow
	Ethernet Type Filter	Disabled
QoS	Status	Off
SNMP	Status	Enabled
	Community (Read Only)	public
	Community (Read/Write)	private
	Trap Destination	Enable
	Trap Destination IP Address	0.0.0.0
	Trap Destination Community Name	public
System Log	Syslog Setup	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	Server Name / IP	0.0.0.0
	Logging Level	Error
	SNTP Server	Disabled
	SNTP Primary Server	137.92.140.80
	SNTP Secondary Server	192.43.244.18
	Time Zone	GMT-05
	Daylight Savings	Disabled

Feature	Parameter	Default
Wireless Interface 802.11a	Radio Settings	Enabled
	Native VLAN ID	1
	Description	RoamAbout AP3000 - 802.11a
	Network Name (SSID)	RoamAbout Default Network Name
	Secure Access	Disable
	Turbo Mode	Disabled
	Radio Channel	N/A
	Auto Channel Select	Enabled
	Transmit Power	100%
	Maximum Tx Data Rate	54 Mbps
	Beacon Interval	100 ms
	Multicast Data Rate	6 Mbps
	Data Beacon Rate (DTIM)	2 Beacons
	Fragment Length	2346 bytes
	RTS Threshold	2347 bytes
	Maximum Associations	100
Wireless Security 802.11a	Authentication Type Setup	Open System
	Data Encryption Setup	Disabled
	WPA Clients	Supported
	WPA Key Management	WPA authentication over 802.1x
	Multicast Cipher Mode	WEP
	WPA Pre-Shared Key Type	Hexadecimal
	Shared Key Setup	64 bit
	Shared Key Type	Hexadecimal
	WEP Transmit Key Number	1
	Key	none

Feature	Parameter	Default
Wireless Interface 802.11b/g	Radio Settings	Enabled
	Description	RoamAbout AP3000 - 802.11 b/g
	Network Name (SSID)	RoamAbout Default Network Name
	Native VLAN ID	1
	Secure Access	Disabled
	Radio Channel	6
	Auto Channel Select	Disabled
	Fragment length	2346 Bytes
	Working Mode	b & g mixed
	Transmit Power	100%
	Maximum Tx Data Rate	54 Mbps
	Multicast Data Rate	1 Mbps
	Beacon Interval	100 ms
	Data Beacon Rate (DTIM	2 Beacons
	RTS Threshold	2347 bytes
	Maximum Associations	100
Wireless Security 802.11b/g	Authentication Type Setup	Open System
	Data Encryption Setup	Disabled
	WPA Clients	Supported
	WPA Key Management	WPA authentication over 802.1x
	Multicast Cipher Mode	WEP
	WEP Pre-Shared Key Type	Hexadecimal
	Shared Key Setup	64 bit
	Key Type	Hexadecimal
	Transmit Key Number	1
	Keys	none

C

Cables and Pin-outs

Twisted-Pair Cable Assignments

Caution: 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.

Precaución: NO utilice un conector de teléfono en el puerto RJ-45. Utilice solamente cable de par trenzado con conectores RJ-45 para cumplir con los estándares de la FCC.

Achtung: Verbinden Sie keine Telefonkabel mit dem RJ-45-Anschluss. Verwenden Sie ausschließlich verdrillte Kabel mit RJ-45-Anschlüssen, die den FCC-Standards entsprechen.

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.

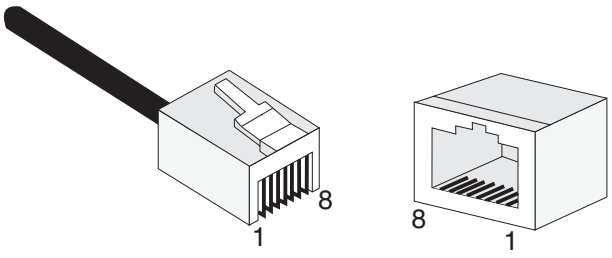
Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (Refer to “Straight-Through Wiring” on page C-2 and “Crossover Wiring” on page C-3 for an explanation.)

Precaución: Cada par debe estar adjunto a los contactos del conector RJ-45 en una orientación específica. Refiérase a “Straight-Through Wiring” y “Crossover Wiring” para una explicación al respecto.

Achtung: Jedes Kabelpaar muss in einer bestimmten Ausrichtung mit den RJ-45-Anschlüssen verbunden werden. Weitere Informationen hierzu finden Sie unter „Straight-Through Wiring“ (Standard-Verkabelung) und „Crossover Wiring“ (Crossover-Verkabelung).

Figure C-1 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.

Figure C-1 RJ-45 Connector Pin-Out



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, or 100-ohm Category 5 or better cable for 100 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 is wired with MDI pinouts. This means that you must use crossover cables for connections to PCs or servers, and straight-through cable for connections to switches or hubs. However, when connecting to devices that support automatic MDI/MDI-X pinout configuration, you can use either straight-through or crossover cable.

10/100BASE-TX MDI and MDI-X Port Pinouts

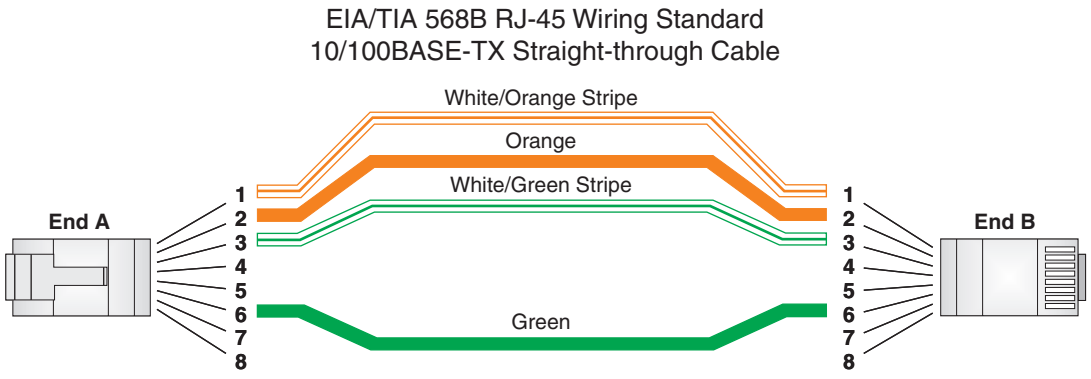
Pin	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)
4,5,7,8	Not used	Not used

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

Straight-Through Wiring

Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use "straight-through" cable for network connections to hubs or switches that only have MDI-X ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either "straight-through" or "crossover" cable.

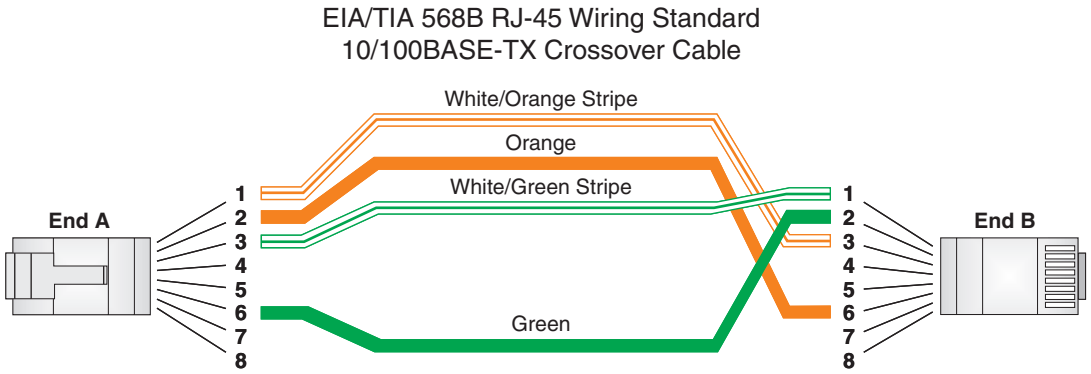
Figure C-2 10/100 BASE-TX Straight-through Cable



Crossover Wiring

Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use "crossover" cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either "straight-through" or "crossover" cable.

Figure C-3 10/100 BASE-TX Crossover Cable



Console Port Pin Assignments

The DB-9 DCE serial port on the front panel of the Access Point 3000, shown in Figure C-4, is used to connect to the access point for out-of-band console configuration. The on-board menu-driven configuration program can be accessed from a terminal, or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in Table C-1 through Table C-3.

Figure C-4 Console Port Pin Assignment

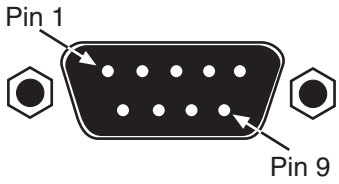


Table C-1 Wiring Map for Serial Cable

Signal (serial port)	Pin	Signal (management console port)
Unused	1	Unused
TXD (transmit data)	2	RXD (receive data)
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
GND (ground)	5	GND (ground)
Unused	6	Unused
CTS (clear to send)	7	RTS (request to send)

Table C-1 Wiring Map for Serial Cable (continued)

Signal (serial port)	Pin	Signal (management console port)
RTS (request to send)	8	CTS (clear to send)
Unused	9	Unused

Note: The left hand column pin assignments are for the female DB-9 connector on the access point. Pin 2 (TXD or “transmit data”) must emerge on the management console’s end of the connection as RXD (“receive data”). Pin 7 (CTS or “clear to send”) must emerge on the management console’s end of the connection as RTS (“request to send”).

Table C-2 Serial Cable Signal Directions for DB-9 Ports

DB-9 to DB-9 AP		Terminal or PC
1	Reserved →	1
2	←	2
3	Reserved	3
4	—	4
5	Reserved ←	5
6	→ Reserved	6
7		7
8		8
9		9

Table C-3 Serial Cable Signal Directions for DB-25 Ports

DB-9 to DB-25 AP		Terminal or PC
1	Reserved →	8
2	←	3
3	Reserved	2
4	—	20
5	Reserved ←	7
6	→ Reserved	6
7		4
8		5
9		22

D

Troubleshooting

Troubleshooting Steps

Check the following items before contacting technical support.

1. If wireless clients cannot access the network, check the following:
    a. Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
    b. If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
    c. If authentication is being performed through a RADIUS server, ensure that the clients are properly configured on the RADIUS server.
    d. If authentication is being performed through IEEE 802.1x, be sure the wireless users have installed and properly configured 802.1x client software.
    e. If MAC address filtering is enabled, be sure the client's address is included in the local filtering database or on the RADIUS server database.
    f. If the wireless clients are roaming between access points, make sure that all the access points and wireless devices in the Extended Service Set (ESS) are configured to the same SSID, and authentication method.
2. If the access point cannot be configured using Telnet, a Web browser, or SNMP software:
    a. Be sure to have configured the access point with a valid IP address, subnet mask and default gateway.
    b. If VLANs are enabled on the access point, the management station should be configured to send tagged frames with a VLAN ID that matches the access point's native VLAN. However, to manage the access point from a wireless client, the AP Management Filter should be disabled. Refer to the *RoamAbout Access Point 3000 Configuration Guide* for more information.
    c. Check that you have a valid network connection to the access point and that the Ethernet port or the wireless interface that you are using has not been disabled.
    d. If you are connecting to the access point through the wired Ethernet interface, check the network cabling between the management station and the access point. If you are connecting to the access point from a wireless client, ensure that you have a valid connection to the access point.
    e. If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (for example, four sessions). Try connecting again at a later time.

3. If you cannot access the on-board configuration program via a serial port connection:
   a. Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.
   b. Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix C.
4. If you forgot or lost the password:

   You can reset the access point back to its default configuration by pressing the reset button on the back panel for 5 seconds or more. **You will lose all of your configuration settings**. Then, use the default user name "admin" with the password "password" to access the management interface.
5. If all other recovery measures fail, and the access point is still not functioning properly, take any of these steps:
   a. Reset the access point using the console interface, Web interface, or through a power reset.
   b. Reset the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. **You will lose all of your configuration settings**. Then, use the default user name "admin" with the password "password" to access the management interface.

Maximum Distance Tables

Table D-4 through Table D-6 list the wireless distances.

Note: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those posted in the following tables.

Table D-4 802.11a Wireless Distance

	Speed and Distance Ranges									
Environment	108 Mbps	72 Mbps	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	9 Mbps	6 Mbps
Outdoors[1]	30 m 99 ft.	40 m 131 ft	85 m 279 ft	250 m 820 ft	310 m 1016 ft	400 m 1311 ft	445 m 1459 ft	455 m 1492 ft	465 m 1525 ft	510 m 1672 ft
Indoors[2]	15 m 49.5 ft	20 m 66 ft	25 m 82 ft	35 m 115 ft	40 m 131 ft	45 m 148 ft	50 m 164 ft	55 m 180 ft	66 m 216 ft	70 m 230 ft

Table D-5 802.11b Wireless Distance Table

	Speed and Distance Ranges			
Environment	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Outdoors[1]	300 m 984 ft	465 m 1525 ft	500 m 1639 ft	515 m 1689 ft
Indoors[2]	60 m 197 ft	70 m 2 30 ft	83 m 272 ft	85 m 279 ft

Table D-6 802.11g Wireless Distance Table

	Speed and Distance Ranges											
Environment	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	11 Mbps	9 Mbps	6 Mbps	5 Mbps	2 Mbps	1 Mbps
Outdoors[1]	82 m 269 ft	100 m 328 ft	300 m 984 ft	330 m 1082 ft	350 m 1148 ft	450 m 1475 ft	470 m 1541 ft	485 m 1590 ft	495 m 1623 ft	510 m 1672 ft	520 m 1705 ft	525 m 1722 ft
Indoors[2]	20 m 66 ft	25 m 82 ft	35 m 115 ft	43 m 141 ft	50 m 164 ft	57 m 187 ft	66 m 216 ft	71 m 233 ft	80 m 262 ft	85 m 279 ft	90 m 295 ft	93 m 305 ft

1. Outdoor Environment: A line-of-sight environment with no interference or obstruction between the access point and clients.
2. Indoor Environment: A typical office or home environment with floor to ceiling obstructions between the access point and clients.