Wi-Fi EVERYWHERE

Vivato VA2200 Wi-Fi AP/Bridge User Guide

Manual Part Number: 720-01375-02
Printed in U.S.A.
Print Date: July 26, 2004

Copyright © 2004, Vivato, Inc.

All rights reserved. No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from Vivato, Inc.

“Vivato” is a U.S. registered trademark of Vivato, Inc.

Who Should Read This Document?

The Vivato Wi-F AP/Bridge and Wi-Fi Base Station system introduces a new category of Wi-Fi products. Anyone installing this product, configuring this product for operation, or performing network management operations involving this product, should read this document before working with the Wi-Fi AP/Bridge.

Printing This Document

To print this document from the User Guide.PDF file, open the file in Adobe® Acrobat® or Acrobat Reader® and select File>Page Setup. Configure your printer to print 8.5”x11”, portrait orientation, 2-sided. Unless you need the entire manual printed, Vivato suggests that you print only the required portion(s).

VIVATO, INC. END USER LIMITED WARRANTY AND LICENSE TERMS

LIMITED WARRANTY

Vivato, Inc. ("Vivato") warrants that the hardware of the Vivato products ("Product") will be free from defects in material and workmanship under normal use for a period of one (1) year (i) if purchased directly from Vivato, from the date of shipment by Vivato to End User, or (ii) if purchased from a Vivato authorized reseller ("Reseller"), from the date of shipment by Reseller to End User. Vivato warrants that the media upon which software (“Software”) is provided will be free from defects in material and workmanship under normal use for a period of ninety (90) days (i) if purchased directly from Vivato, from the date of shipment by Vivato to End User, or (ii) if purchased from a Reseller, from the date of shipment by Reseller to End User. Except for the forgoing, the Software is provided "AS IS" with all faults and without warranty of any kind. This limited warranty extends only to the End User who is the original purchaser of the Product and licensee of the Software and may not be transferred to any other party. The date of original shipment of Product and Software shall be determined by the information on file at Vivato regarding End User in accordance with Vivato's then current procedures.

REMEDY

End User's sole and exclusive remedy, and Vivato's entire liability under this Limited Warranty in the event that Product or Software does not perform as warranted above, will be, at Vivato's or its service center's option, to repair or replace such Product or Software or to refund the purchase price paid for such Product or Software. Vivato's obligations hereunder are conditioned upon the return, freight pre-paid of the alleged affected Product or Software in accordance with Vivato's or its service centers then current Return Material Authorizations ("RMA") procedure. All warranty claims shall be directed to Vivato’s technical assistance center as designated by Vivato’s web site (www.vivato.net). Vivato or its authorized repair center shall have the right to inspect the Product or Software claimed as not performing as warranted. This warranty is conditioned upon receipt by Vivato of notice of any alleged covered manufacturing defect in material or workmanship within thirty (30) days after discovery, subject to the warranty period. In no event shall Vivato be responsible for any costs associated with the removal (or re-installation) of Product or Software from (or into) items into which such Product or Software have been integrated by Buyer (or other third parties), or costs associated with other products into which the Product or Software may have been integrated or used.

After receiving an RMA for Product or Software, End User shall ship such Product, Software or component thereof, clearly identifying it with its RMA, to Vivato’s designated repair facility in its original shipping cartons or equivalent, freight prepaid. Damage to Product or Software that occurs during return shipment will not be covered by this warranty. Upon receipt of the Product or Software returned in accordance with Vivato's then current RMA procedure, Vivato, at its option, shall (i) repair or replace such Product, Software or component thereof with equivalent or better, new or refurbished Product, Software or parts, and shall return the repaired or replaced Product or Software to End User freight prepaid by Vivato, or (ii) refund the purchase price of such Product or Software. The remainder of the original warranty coverage shall apply to such repaired or replacement Product or Software.

LIMITATIONS OF WARRANTY

This warranty does not apply to Product or Software which fails to perform as warranted due to: (a) improper handling, installation, removal, repair, maintenance, abuse or improper use; (b) damage caused by vandalism, severe weather, lightning, chemical hazards, fire, contact with high-voltage power lines or other electrical stress; (c) repairs, modifications, or any alterations performed or attempted by End User or

any third party, unless authorized by Vivato as stated below; (d) use in conjunction with equipment which is not compatible with Product or Software; (e) documentation errors; (f) software errors; or (g) Product or Software provided to End User for evaluation, testing, demonstration or other purposes for which Vivato does not receive payment of purchase price or license fee.

Vivato does not warrant or accept any responsibility for Product or Software, which has been repaired or altered by anyone other than Vivato, or a Vivato authorized service center. In the event of any such unauthorized repairs or alterations, this warranty shall become void. No agent, distributor, Reseller or representative is authorized to make any warranties or to assume any liabilities on behalf of Vivato.

Vivato shall make the final determination as to the existence and cause of any alleged defect of Product or Software. Non-payment of invoices for Product or Software, within the stated terms, shall cause this warranty to be suspended until late invoices are fully paid.

If the Product or Software is found to have been damaged due to misuse, abnormal operating conditions, or unauthorized repair, the repairs and/or replacement of such Product or Software will be done at End User's expense under Vivato's then current time and material repair terms. In such event, an estimate of the cost of repairs and/or replacement will be submitted to End User for approval before the work is started. If the returned Product or Software is found by Vivato to be in compliance with this Limited Warranty, Vivato may charge a fee for the evaluation, which may include reasonable travel and expenses, if applicable.

Minor or non-substantive defects or deviations, or errors or omissions of Product or Software shall not constitute a warranty defect. End User understands and acknowledges that the form, function and operation of the Product and Software will change from time to time.

EXCEPT AS SPECIFIED HEREIN, VIVATO MAKES NO OTHER WARRANTIES WITH RESPECT TO PRODUCT AND SOFTWARE AND DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, TO THE EXTENT ALLOWED BY APPLICABLE LAW, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, SATISFACTORY QUALITY, WARRANTIES OF NON-INFRINGEMENT OR WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. ALL SUCH WARRANTIES ARE HEREBY EXPRESSLY DISCLAIMED. VIVATO DOES NOT WARRANT THAT THE PRODUCT OR SOFTWARE IS ERROR-FREE OR THAT OPERATION OF THE PRODUCT OR SOFTWARE WILL BE SECURE OR UNINTERRUPTED AND VIVATO HEREBY DISCLAIMS ANY AND ALL LIABILITY ON ACCOUNT THEREOF. This disclaimer and exclusion shall apply even if the express warranty set forth herein fails in its essential purpose.

LIMITATION OF LIABILITY

NOTWITHSTANDING ANYTHING ELSE, VIVATO SHALL NOT BE LIABLE TO END USER OR ANY THIRD PARTY UNDER ANY PROVISION HEREIN OR UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY, FOR ANY INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, INDIRECT OR SPECIAL DAMAGES, OR COST, OR FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCT, SOFTWARE, OR SERVICES, WHETHER OR NOT VIVATO OR ANYONE ELSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL VIVATO BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE AGGREGATE AMOUNT PAID BY END USER TO VIVATO FOR THE PRODUCT AND SOFTWARE, DURING THE SIX MONTHS PREVIOUS TO THE TIME THE CLAIM ARISES. THE RIGHT TO RECOVER DAMAGES WITHIN THE LIMITATIONS SPECIFIED IN THIS SECTION IS END USER'S EXCLUSIVE ALTERNATIVE REMEDY IN THE EVENT ANY OTHER CONTRACTUAL REMEDY FAILS

IN ITS ESSENTIAL PURPOSE.

END USER LICENSE

PLEASE READ THIS BEFORE INSTALLING, USING OR DOWNLOADING VIVATO SUPPLIED PRODUCT OR SOFTWARE.

THIS END USER LICENSE ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU AS "END USER" (AS EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND VIVATO, INC. ("VIVATO") REGARDING VIVATO PRODUCT ("PRODUCT") AND SOFTWARE ("SOFTWARE"). SOFTWARE INCLUDES ALL SOFTWARE, ASSOCIATED MEDIA, ANY PRINTED MATERIALS, AND ANY "ONLINE" OR ELECTRONIC DOCUMENTS. BY INSTALLING, USING OR DOWNLOADING VIVATO SUPPLIED PRODUCT OR SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN VIVATO IS UNWILLING TO LICENSE THIS PRODUCT AND SOFTWARE TO YOU. IN SUCH EVENT: (A) DO NOT INSTALL, USE OR DOWNLOAD THE VIVATO SUPPLIED PRODUCT OR SOFTWARE, AND (B) YOU MAY RETURN THE VIVATO SUPPLIED PRODUCT OR SOFTWARE FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM VIVATO OR AN AUTHORIZED VIVATO RESELLER, AND THIS RIGHT APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Product or Software except to the extent a particular Product or Software: (a) is the subject of a separate written agreement signed by both an authorized representative of Vivato and End User ("Written Agreement"), (b) includes separate "click-on" license agreement as a part of the installation and/or download process ("Click-On Agreement"), or (c) separate terms are provided by Vivato for particular Product or Software ("Separate Terms"). To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the Written Agreement, (2) the Click-On Agreement, (3) the Separate Terms, and (4) this End User License.

1. **License**. End User is granted a limited, nonexclusive and nontransferable license to use the Product (including the object code version of the Software) solely for its own internal business operations in accordance with the accompanying documentation. Except as expressly permitted by such license, End User shall not use, reproduce, make, have made, import, offer for sale, sell, modify, adapt, rent, lease, loan, create derivative works of, display, perform, distribute, sublicense or otherwise exploit the Product or Software in any way for any purpose.

2. **No Copying, Modification or Reverse Engineering**. End User agrees that it shall not copy, modify, enhance, reverse engineer, disassemble, decompile, or make derivative works of the Product or Software, or otherwise attempt to derive the source code, algorithms or other aspects of the Product or Software, in whole or part.

3. **Proprietary Rights**. End User acknowledges that all patents, copyrights, trade secrets, trade names, trademarks, and all other intellectual property rights in or related to the Product and Software are the exclusive property of Vivato and its licensors (if any). No right, title or interest, expressed or implied, in or to the Product or Software, including without limitation patent, copyright, trade secret or other intellectual property rights therein, other than the limited license granted above, is transferred from Vivato to End User. Title to and ownership of the Software shall

remain with Vivato and its licensors (if any). End User shall not alter or erase any copyright, confidential or proprietary notices appearing on the Product, Software or related documentation.

4. **Termination**. This EULA is effective until terminated. End User's license under this EULA shall immediately terminate should End User fail to comply with the terms of this EULA. Without prejudice to any other rights, Vivato may terminate this EULA if End User fails to comply with its terms and conditions. Upon termination, the End User must promptly cease use of the Software and destroy it and its component parts.

5. **Confidentiality**. End User acknowledges that the Product and Software contains confidential and proprietary information belonging to Vivato and its licensors (if any). End User shall exercise at least the same degree of care, but in no event less than a reasonable degree of care, to safeguard the confidentiality of Vivato and its licensors' confidential and proprietary information as End User would exercise with respect to End User's own confidential information and trade secrets. End User shall not disclose or transfer any such Confidential Information to a third party other than as may be specifically authorized by Vivato in writing. End User shall take reasonable steps to protect Confidential Information, including, without limitation, by restricting disclosure of such Confidential Information only to those persons with a "need to know" and who are subject to confidentiality undertakings. The term Confidential Information shall not include information that is or becomes publicly available without breach of this Section or was known to End User at the time of disclosure without an obligation of confidentiality, as demonstrated by files in existence at the time of disclosure.

6. **U.S. Government End Users**. If the Software as incorporated in the Product is acquired by or on behalf of a unit or agency of the United States government, this provision applies. The Software is (a) existing computer software, and was developed at private expense, (b) is a trade secret of Vivato for all purposes of the Freedom of Information Act, (c) is "commercial computer software" subject to limited utilization as expressly stated in this EULA, (d) in all respects is proprietary data belonging to Vivato, and (e) is unpublished and all rights are reserved under the copyright law of the United States. For civilian agencies and entities acquiring Software under a GSA Schedule, Software is licensed only with "Restricted Rights" and use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software – Restricted Rights clause at 52.227-19 of the Federal Acquisition Regulations and its successors. For units of the Department of Defense ("DoD"), this Software is licensed only with "Restricted Rights" and use, duplication, or disclosure is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013 of the DoD Supplement to the Federal Acquisition Regulations and its successors.

7. **Warranty**. The Product and Software is being provided to End User under the terms of the End User Limited Warranty, which is attached hereto and incorporated by reference herein. **EXCEPT AS SPECIFIED IN THE LIMITED WARRANTY, VIVATO MAKES NO OTHER WARRANTIES WITH RESPECT TO PRODUCT OR SOFTWARE AND DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, TO THE EXTENT ALLOWED BY APPLICABLE LAW, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, SATISFACTORY QUALITY, WARRANTIES OF NON-INFRINGEMENT OR WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. ALL SUCH WARRANTIES ARE HEREBY EXPRESSLY DISCLAIMED. VIVATO DOES NOT WARRANT THAT THE PRODUCT OR SOFTWARE IS ERROR-FREE OR THAT OPERATION OF THE PRODUCT OR SOFTWARE WILL BE SECURE OR UNINTERRUPTED AND VIVATO HEREBY DISCLAIMS ANY AND ALL LIABILITY ON**

ACCOUNT THEREOF. **This disclaimer and exclusion shall apply even if the express warranty set forth herein fails in its essential purpose.**

8. **Limitation of Liability**. **NOTWITHSTANDING ANYTHING ELSE, VIVATO SHALL NOT BE LIABLE TO END USER OR ANY THIRD PARTY UNDER ANY PROVISION HEREIN OR UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY (A) FOR ANY AMOUNTS IN EXCESS OF THE AGGREGATE AMOUNTS PAID BY END USER TO VIVATO FOR THE PRODUCT AND SOFTWARE, OR (B) FOR ANY INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, INDIRECT OR SPECIAL DAMAGES, OR COST OR (C) FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, whether or not VIVATO or anyone else has been advised of the possibility of such damages.** T**he right to recover damages within the limitations specified in this Section is End User's exclusive alternative remedy in the event any other contractual remedy fails in its essential purpose.**

9. **Applicable Law; Jurisdiction. The validity, interpretation, performance of this End User Limited Warranty and License Terms shall be governed by the laws of the State of California, USA, without giving effect to its conflict of laws provisions.** Buyer irrevocably agrees and consents that the state courts of San Francisco County, California, USA or the United States District Court for the Northern District of California shall have exclusive personal jurisdiction over Buyer and proper venue with regard to any claims arising in connection with the purchase, sale, license or performance of any Product or Software, and any objection to the jurisdiction or venue of any such court is hereby waived. The parties agree that rights and obligations hereunder shall not be governed by the United Nations Convention on the International Sale of Goods.

Safety Information

You must heed any and all safety precautions and warnings in this document or indicated on the Vivato Wi-Fi AP/Bridge whenever you are operating or servicing this product. Failure to comply with all precautions and warnings found in this document violates the design, manufacture, and intended use requirements of the product. Vivato, Inc. assumes no liability for the operator's failure to obey these warnings and cautions.

The person installing the Vivato Wi-Fi AP/Bridge must be qualified by Vivato, Inc. or by a Vivato authorized reseller.

This product must only be serviced by qualified Vivato personnel or its certified agent.

Power Supply: A separate direct current (DC) power supply is shipped with the Vivato Wi-Fi AP/Bridge. Do not attempt to use a substitute power supply unless it has been approved by Vivato for use with this product.

Do not operate this product in an explosive atmosphere or in the presence of flammable gases or fumes, or in the presence of unshielded blasting caps.

To protect against fire, replace any fuses in the product with those of the same voltage, current rating, and type. Never short-circuit fuse holders or use modified fuses.

Keep away from energized circuits. Only qualified Vivato service personnel or its certified agent may remove the outer covers of the product. Hazardous voltages may be present any time a cover is removed, even if the product is not turned on.

Do not operate this product if damage is indicated. Refer servicing or repair to qualified Vivato personnel or its certified agent.

Do not service or adjust this product by yourself. It is recommended that someone else is present who can render first aid in the event that electrical shock or other injury occurs.

Do not substitute any parts or modify the product. Any unauthorized changes to the product could result in compromising the safety features or the correct operation of the product. Refer any service or repair to authorized Vivato personnel or its certified agent.

Operation With Antennas Not Included With The AP/Bridge

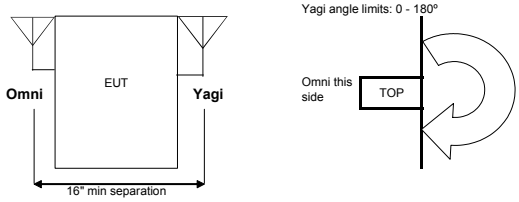
The combinations of antennas listed in **Table 1—Tested Antenna Configurations** on page 10 have been tested with the Vivato Wi-Fi AP/Bridge and have shown to comply with FCC Part 15 rules when used in the test configurations shown in **Figure 1— Test Configurations for Antenna Qualification** on page 10.

Table 1— Tested Antenna Configurations

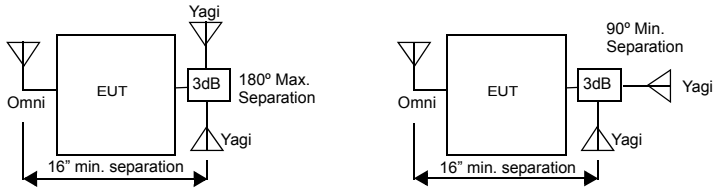
Test Config	Antenna 1					Antenna 2				
	Pattern	Brand	Model	Gain (dBi)	Polarization	Pattern	Brand	Model	Gain (dBi)	Polarization
1	Omni	MaxRad	MFB24011PTRPC	11	Vert	Yagi	MaxRad	MYP24010PTRPC	10	Horiz
2	Omni	MaxRad	MFB24011PTRPC	11	Vert	Yagi	MaxRad	MYP24010PTRPC	10	Horiz
3	Omni	SuperPass	SPHSG6O	8.5	Horiz	Panel	MaxRad	MP24008XFPTRPC	8	Horiz
4	Omni	SuperPass	SPHSG6O	8.5	Horiz	Omni	MaxRad	MFB24011PTRPC	11	Vert
5	Omni	SuperPass	SPHSG6O	8.5	Horiz	Yagi	MaxRad	MYP24010PTRPC	10	Vert
6	Panel	MaxRad	MP24008XFPTRPC	8	Horiz	Panel	MaxRad	MP24008XFPTRPC	8	Horiz

Figure 1— Test Configurations for Antenna Qualification

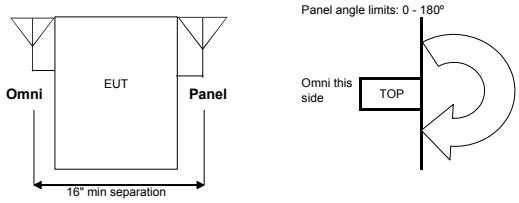
Configurations 1 and 5



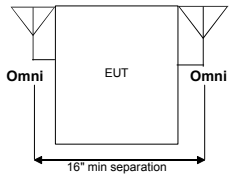
Configuration 2



Configuration 3

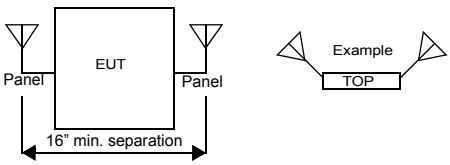


Configuration 4



Configuration 6

Panels must have at least 45° angular separation!



 Copyright © 2004, Vivato, Inc.

Conventions Used in This Document

The following conventions are used in this document:

Table 2 — Document Conventions

Convention Format	What it Indicates
computer entry	Text that you enter on the Wi-Fi AP/Bridge's web page or on a terminal when using the command line interface (CLI).
>	The > symbol indicates a menu navigation selection. For example, "select File > Save " means "select the File menu, and then select the Save option."
Labels	Items in a menu, such as the tabs shown on the configuration web pages.
<MD5|DES>	Indicates that you need to enter either term (MD5 or DES). Do not enter the <|> symbols.
Important	This symbol identifies critical information concerning Wi-Fi AP/Bridge operation. Failure to comply with this information may degrade or prevent Wi-Fi operation.
Caution	This symbol identifies information that must be complied with to keep the Wi-Fi AP/Bridge from being damaged.
Warning	This symbol identifies information that must be complied with to reduce the possibility of electrical shock or other injury.

Contact Information

For customer support:

For technical support, contact your Vivato reseller or visit the Vivato Customer Support website.

Go to www.vivato.net and select the **Customer Support** link. Enter the required information for setting up a user account. A support password is e-mailed to you after validating the information. You can then search the online knowledge base for information by clicking on "**Find Answers / Questions**". You can also access that latest firmware downloads and user documents from the support site.

To provide feedback on our documentation:

Feedback on the documentation shipped with the Vivato Wi-Fi Wi-Fi AP/Bridge is greatly appreciated, and will always be reviewed by our Technical Publications department. Please send your suggestions to **manuals_feedback@vivato.net**or click on the "*Send Documentation Feedback*" link at the bottom of each online documentation page on the Vivato CD (Please use the Customer Support link mentioned above for product support issues.)

 Copyright © 2004, Vivato, Inc.

VIVATO, INC. END USER LIMITED WARRANTY AND LICENSE TERMS 3

Safety Information 9
FCC Declaration of Conformity 9
Conventions Used in This Document 12
Contact Information 13

Introduction 23
Powered Ethernet 24
Omni-directional Antennas 24
Ethernet and Serial Ports 24
Reset To Factory Defaults 24
Metal Enclosure 24
IEEE 802.11 ISM-Band Channel Operation 24
Multi-AP/Bridge Operation for Extended Coverage 24
Basic Service Set Operation 25
Web Page or Command Line Interface Configuration 25
Network Configuration Examples 26
Specifications 27
Shipping Contents 27

Installation 29
Where to Position The AP/Bridge 29
Antenna Polarization and Positioning 29
Interfering Signal Sources 30
Access Point Positioning 30
Coverage Filler Positioning 31
Wireless Backhaul Positioning 31
Range Extension Positioning 32
Preparing the AP/Bridge for Operation 33

Initial Configuration Using the Built-In Web Pages 35
Steps to Configuring the Vivato Wi-Fi AP/Bridge 35
Default Configuration 36
Configuration Connections 36
Enabling Your Computer's Network Adapter to Access the Wi-Fi AP/Bridge 37
Using APIPA to Assign a Usable IP Address For Your Client 37
Wired Connection to Access the Configuration Web Page 39
Wireless Configuration Connection 41
Entering the Initial Configuration Information in the Quick Setup Pages 43
Setup Type 43
Read Password Setup 44

Enable Password Setup 45
Basic Network Setup 46
Basic Security Setup 47
Wireless Options Setup 48
Rebooting the Wi-Fi AP/Bridge 49
Where Do I Go From Here? 50

Using the Main Configuration Web Pages 51
Navigating the Main Web Page Configuration Screens 51
Status Indicators 52
Home 52
Home>Summary 52
System Information 52
Currently Associated Clients 53
Network Information 53
Monitoring Information 53
Security Information 53
Services Information 53
Home>Quick Setup 53

Network Configuration Web Pages 55
Network Settings 55
Network>Summary 56
Network>General 57
Create a New Route 57
Current Routing Information 57
Create a New Nameserver 58
Current NameServer Information 58
Create a New Host 59
Current Host Table 59
Network>Bridge 60
Create/Add to Bridge 60
Available Bridges 61
Network>DHCP 63
Network>Ethernet Interface 65
Network>Wireless Interfaces 66
Configuring Wireless Interfaces Individually 66
Configuring the Wireless Interfaces As a Group 67
Network>WDS 68
WDS Creation 68
Current WDS Information 69

Security Configuration Web Pages 71
Security Settings 71

 Copyright © 2004, Vivato, Inc.

Security>Summary 71
Security>WEP 71
Security>802.1x 72
Important Considerations When Using 802.1x. 73
Optimizing Your Wireless Client For Secure Communications 73
Configuring WEP in Your Client 75
Configuring 802.1x in Your Client. 76

Monitoring Clients and System Operations 79
Monitoring Settings 79
Monitoring>System Messages 79
System Logging Configuration. 80
Monitoring>SNMP Monitoring 80
Base SNMP Options 80
Create an SNMP Community 81
SNMP Version 3 Configuration Settings 82
SNMP Version 2 Trap Sinks 83
SNMP Version 1 Traps. 83
Monitoring>Associated Clients 83

Services, Password, Config, and Firmware Web Pages 85
System Settings 85
System>Summary 85
System>Services 86
Set System Hostname 86
Reboot System 86
Reset System to Default Settings 86
SSH Services Configuration 87
HTTP Services Configuration 87
System>Password 88
System>Config 88
System>Firmware 90
Local Firmware Options 90
System>Quick Setup 91

Diagnostics Web Screen and Help 93
Diagnostics 93
Diagnostics>Tools 93
Ping 93
Traceroute 94
Diagnostics>Arp 94
Help 94

Configuration Using The Command Line Interface 95
Command Levels 95
Connections and Terminal Settings 96
Accessing the CLI 97
Accessing the Configuration Level 98
Configuration Example 99
Navigating the CLI 100
Moving the Cursor Around on the Command LIne 100
Using the "?" to Get Online Command Help 100
Using the Tab Key to Complete a Command 101
Command Mode Access and Prompts 101
Command Conventions 102
Entering Commands on the Command Line 102
Reading the Command Listing 102
Entering Variables 102
Optional Entries 102
Read Level Command Descriptions 102
enable 102
exit 103
Ping 103
ping <ipaddress|hostname> 103
ping flood <ipaddress|hostname> 103
ping flood 103
ping flood count <1-100000> <ipaddress|hostname> 103
ping count ..... <1-100000> <ipaddress|hostname> 103
ping count ..... <1-100000> flood <ipaddress|hostname> 103
Show Commands 104
show arp 104
show cpu 104
show dhcp-server interface bridge <0-4094> 104
show dhcp-server interface ethernet <0> 104
show dhcp-server interface wireless <0-1> 105
show eap 105
show http-server 105
show iccf 105
show interfaces 105
show interfaces bridge [0-4094] 105
show interfaces bridge <0-4094> fdb 106
show interfaces bridge <0-4094> stp 106
show interfaces ethernet [0] 106
show interfaces wireless [associations] 108
show interfaces wireless <0-1> associations 108
show interfaces wireless <0-1> 109
show interfaces wireless < 0-1> wds <1-6> 110
show ip domainname 111

 Copyright © 2004, Vivato, Inc.

show ip host . . . 111
show ip hostname . . . 111
show ip nameserver . . . 111
show ip route . . . 111
show ip ssh . . . 111
show logging . . . 111
show memory . . . 111
show serial . . . 112
show snmp-server . . . 112
show uptime . . . 112
show version . . . 112
show wds . . . 112
show flash: . . . 113
show running-config . . . 113
traceroute <ipaddress|hostname> . . . 113
Enable Level Command Descriptions . . . 114
configure [terminal] . . . 114
Commands for Managing Configuration Files . . . 114
configure network flash: . . . 114
copy flash: flash: . . . 115
copy flash: scp: . . . 115
copy flash: tftp: . . . 115
copy scp: firmware: . . . 116
copy scp: flash: . . . 116
copy tftp: firmware: . . . 117
copy tftp: flash: . . . 117
delete flash: <filename> . . . 117
dir . . . 117
rename flash:<filename> flash:<new filename> . . . 118
write [memory] . . . 118
write network flash: . . . 118
write network scp: . . . 118
write terminal . . . 118
Configure Crypto (Generate Keys) Commands . . . 118
crypto key generate <dsa|rsa|rsa1> . . . 118
Configure Enable Secret Commands . . . 119
enable secret [<password type (0|5)>] <password text> . . . 119
Configure HTTP-Server Commands . . . 119
http-server . . . 119
no http-server . . . 119
Configure Interface Commands . . . 119
interface bridge <0-4094> . . . 120
interface ethernet 0 . . . 126
interface wireless < 0-1|all> . . . 127
Configure No Interface Commands . . . 133

no interface bridge <0-4094> 134
Configure IP Commands 134
ip domainname <text> 134
ip host <hostname> <ipaddress> 134
ip hostname <hostname> 134
ip name-server <ipaddress> 134
ip route <destination prefix> <destination mask> <forwarding router address> . . . 134
ip routing. 134
ip ssh genkey. 135
ip ssh server 135
ip ssh bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>) 135
no ip ssh bind [interface (wireless <0-1>|ethernet 0|bridge <0-4094>] 135
Configure Log Commands.....135
logging local 135
logging remote <ipaddress|hostname> 135
no logging local 135
no logging remote 135
Configure Multicast/Broadcast Rate Limiting.....135
rate-limit <broadcast|multicast> 136
Configure SNMP-Server Commands 136
snmp-server 136
snmp-server bind interface (wireless < 0-1>|ethernet 0|bridge <0-4094>) 136
snmp-server community <community name> RO|RW [<source ip address>]. 136
snmp-server contact <text>. 136
snmp-server engineID <engine identifier> 136
snmp-server host <hostname|ipaddress> traps version 1 <community name> 136
snmp-server host <hostname|ipaddress> traps|informs version 2c <community name>
136
snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth
MD5|SHA <password> [priv DES <password>]] 137
snmp-server location <text> 137
snmp-server name <text> 137
snmp-server user <username> [auth MD5|SHA <password> [priv DES [<password>]]]
137
Configure No SNMP-Server Commands 138
no snmp-server 138
no snmp-server community <community name> 138
no snmp-server contact 138
no snmp-server engineID 138
no snmp-server host <hostname|ipaddress> traps|informs version <1|2c|3> 138
no snmp-server location 138
no snmp-server name 138
no snmp-server user <username> [auth MD5|SHA <password> [priv DES <pass-
word>]] 139
Configure Username Admin (Read Level) Secret.....139

username admin secret [<password type (0|5)> <password text> 139
Configure WDS (Wireless Distribution System) 139
exit 140
ip address <ip address> <subnet mask> [secondary] 140
no ip address <ip address> <subnet mask> [secondary] 140
ip address dhcp 140
no ip address dhcp. 140
ip address dhcp renew 140
ip address dhcp release 141
ip broadcast-address <ip address> [secondary] 141
no ip broadcast-address <ip address> [secondary] 141
peer-address <mac address> 141
shutdown 141
no shutdown 141
disable 143
edit flash: 143
exit 143
no <configuration command> 143
reboot 143
support 143

Network Monitoring 145
SNMP Operations 145
Supported MIB 146
RFC1213-MIB.txt. 146
Enabling SNMP Operation 146

Verifying Wi-Fi Operation 149
Verification Process 149
Wireless Client Does Not “Find” the Vivato Wi-Fi AP/Bridge 150
Variations in Client Performance Due to Physical Orientation 150
Wireless Client Can’t Access Wi-Fi AP/Bridge Configuration Web Page 151
Wireless Client Cannot Access the Local Wired Network 151
Wireless Client Cannot Access an Outside Network 152
Unauthorized Clients Are Able to Associate With The Wi-Fi AP/Bridge 152
Connecting Through a WDS Connection 152

Dynamic Assignment of Client IP Addresses 153
How Does DHCP Work? 153
What is Network Address Translation? 154
“Breaking the Bridge” 155
Configuring DHCP Server Operation on the AP/Bridge 156
DHCP Server Configuration Example 157

Updating AP/Bridge Firmware 159
Updating Firmware Using the Command Line Interface (CLI) 159
Example TFTP Server Operation Using PumpKIN 160
Configuring PumpKIN to “Put” a Firmware Image 160
Starting the TFTP File Transfer 161

 Copyright © 2004, Vivato, Inc.

Introduction

The Vivato Wi-Fi AP/Bridge is a two channel unlicensed (FCC Part 15) wireless device operating in the 2.4 GHz Industrial/Scientific/Instrumentation (ISM) band, providing network connections to Wi-Fi (IEEE 802.11b) client devices.

The Vivato Wi-Fi AP/Bridge, as part of the Vivato Wi-Fi System, replaces previous micro cellular style Wi-Fi deployments, while providing the highest level of wireless security and system management.

The Wi-Fi AP/Bridge allows point-to-multipoint packet transmission to client devices through standard 2.0 dBi antennas. The integrated radio cards have a higher transmit power (200mW) than most conventional Access Points. This design allows one Wi-Fi AP/Bridge to provide high bit rate network coverage to larger spaces requiring Wi-Fi coverage.

The Vivato Wi-Fi AP/Bridge is intended solely for indoor use, but can be combined with either version of the Vivato Wi-Fi Base Station (indoor or outdoor) to provide Wi-Fi service in almost any environment.

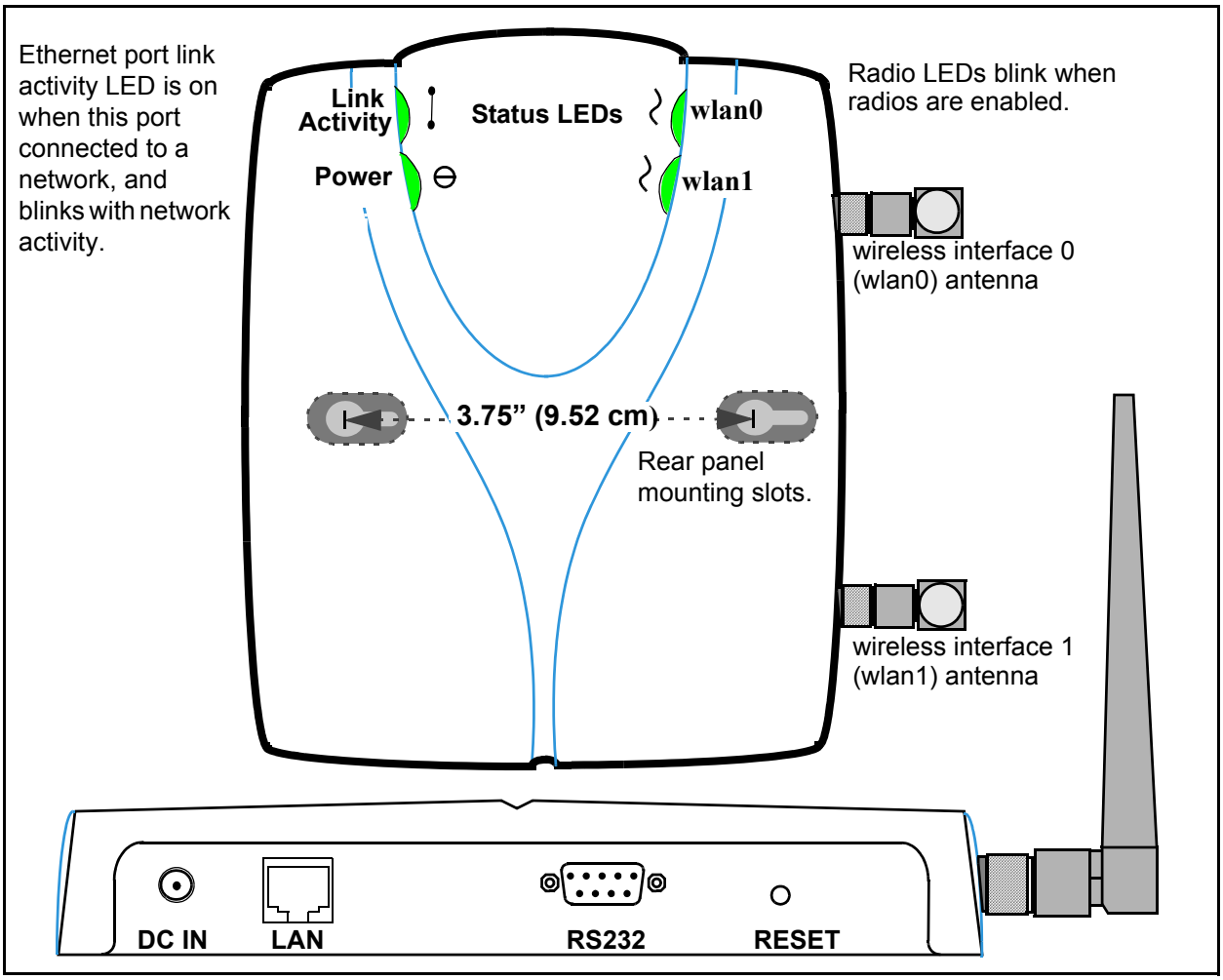


Figure 1—Connectors and Indicators

Powered Ethernet

The AP/Bridge can be powered over an Ethernet cable, eliminating the need for separate power and Ethernet cabling. Contact your Vivato added reseller, or view the list of accessories on the Vivato.net website, for information about various powered Ethernet solutions.

Omni-directional Antennas

The AP/Bridge is equipped with two reverse-polarity TNC antenna connectors and includes two omni-directional antennas.

Ethernet and Serial Ports

The **LAN** (Ethernet) port accepts an RJ-45 connector, linking the AP/Bridge to a 10/100 Ethernet LAN. This connection can also be used to provide power to the AP/Bridge.

The **RS232** (serial) port provides console access to the management system in the AP/Bridge by connecting the supplied serial cable to a computer's RS-232 (COM) port and running a terminal emulator program.

Reset To Factory Defaults

Pressing and holding the **RESET** button in for at least three seconds re-configures the AP/Bridge to use the factory default settings, and deletes the previous configuration file.

Metal Enclosure

The AP/Bridge is enclosed in a metal case which has adequate fire resistance and low smoke-producing characteristics suitable for operation in an indoor environment.

IEEE 802.11 ISM-Band Channel Operation

The Vivato Wi-Fi AP/Bridge can communicate on any two channels in the IEEE channel set (although the default channel assignment of 1 and 11 should be used for best results). Both channels can operate at the maximum data rate of up to 11 Mbps. The AP/Bridge can be configured to communicate with clients and with a Vivato Wi-Fi Base Station (using a Wireless Distribution System (WDS) connection) .

Multi-AP/Bridge Operation for Extended Coverage

Each Wi-Fi AP/Bridge contains one 10/100 Base-T Ethernet port and two wireless interfaces. Multiple Wi-Fi AP/Bridges can be connected using a wired or a wireless connection to extend Wi-Fi coverage and provide maximum deployment flexibility.

 Copyright © 2004, Vivato, Inc.

Basic Service Set Operation

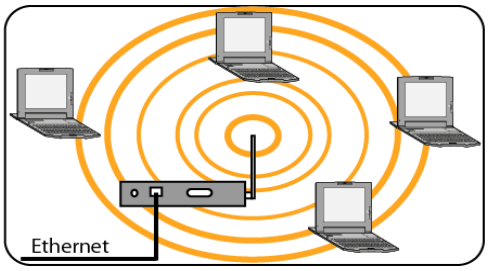
The Wi-Fi AP/Bridge supports infrastructure basic service set (BSS) operation, providing all network communications between Wi-Fi clients and the wired network within the area of coverage.

Web Page or Command Line Interface Configuration

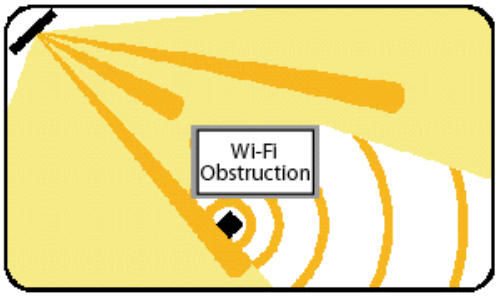
The Vivato Vision™ web interface Quick Setup pages are used for the initial configuration to get the AP/Bridge configured for your network. The main configuration web pages are used to configure additional features not included on the Quick Setup pages. The command line interface (CLI) allows experienced users to quickly make the required configuration changes at one time.

Network Configuration Examples

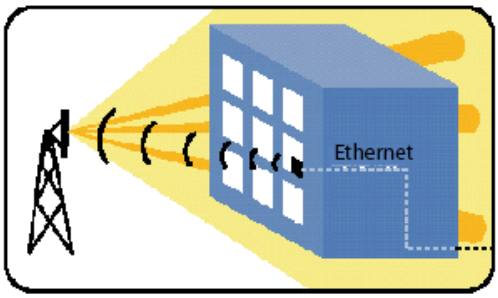
The AP/Bridge can be deployed in four wireless network configurations:



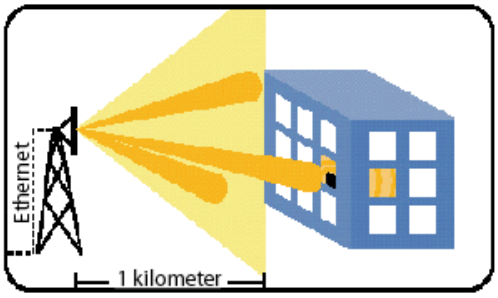
• **Access Point** (AP). As an access point (AP) connected directly to a wired LAN, the AP/Bridge provides a connection point for wireless users and, if more than one AP is connected, users can roam from one area to another without losing their connection to the network. See **"Access Point Location"** on page 30.



• **Coverage Filler** for a Vivato Wi-Fi Base Station using WDS. With radio frequency (RF) systems, there can be coverage gaps or voids due to physical barriers or radio interference. Combining the Vivato VP1200 Wi-Fi Base Station with the Vivato Wi-Fi AP/Bridge can provide effective coverage in an area with poor quality or inadequate coverage. By placing the Wi-Fi AP/Bridge within the line of sight of the Vivato Base Station, the Vivato Wi-Fi AP/Bridge can propagate Wi-Fi to areas with weak or blocked coverage. See **"Hole Filler Location Example"** on page 31.



• **Wireless Backhaul** to a Wi-Fi Base Station. With a Vivato VP1210 Wi-Fi Base Station, the only external connections required are AC power and Ethernet. AC power is often readily available outside buildings, but providing Ethernet to an outdoor environment is not always possible. The AP/Bridge can connect to Ethernet inside a building to provide wireless backhaul for the outdoor base station using one Wi-Fi channel, leaving another channel free for client connections through the outdoor base station. See **"Wireless Backhaul Example"** on page 32.



• **Repeater** to provide range extension. The Wi-Fi AP/Bridge can extend the range of a base station when acting as a repeater, either in conjunction with a Vivato Wi-Fi Base Station or with other Vivato AP/Bridges. One radio is used to establish a long-range connection with the Wi-Fi Base Station or AP/Bridge, and the other radio is used for Wi-Fi (BSS) service. This can expand the distance and coverage area for enhanced flexibility. See **"Range Extension Positioning"** on page 32.

 Copyright © 2004, Vivato, Inc.

Specifications

The following specifications were accurate at the time that this document was released:

- Size 6.75” wide X 8.75” deep X 1.5” high.
- Connectors: One RJ-45 jack for 10/100 Ethernet connection; a nine-pin serial connector; a power connector (plug-in AC adapter)
- Power Supply: Input power 120 VAC, 60 Hz., Output power: 12 VDC @ 1 Amp
- Operating temperature range 32 to 131F (0 to 55C)
- Radio Power output 200 mW
- Frequency 2.412 to 2.462 GHz
- Range Indoor:
  - 300 ft at 11 Mbps
  - 500 ft at 1 Mbps
- Antennas: Two RP-TNC connectors
- Operates license-free under FCC Part 15 and complies as a Class B computing device.
- Complies with DOC regulations.

Shipping Contents

The following items are included in the Vivato Wi-Fi AP/Bridge shipping container:

- Product invoice
- User Guide CD-ROM: Includes user documentation, support files, and a PDF copy of the *Command Line Interface Quick Reference* (print using 11”x17” paper, landscape orientation, 2-sided). *Go to the Vivato Customer Support website to download the latest documentation for the AP/Bridge.*
- Two antennas
- DB-9 null modem cable
- RJ-45 Crossover Ethernet cable
- Power supply
- AP/Bridge stand - allows the AP/Bridge to be positioned on its side when desired.
- Vivato Wi-Fi AP/Bridge

 Copyright © 2004, Vivato, Inc.

Installation

We recommend that you prepare your Vivato Wi-Fi AP/Bridge for operation in the following order:

Step 1. Verify the contents of the shipping container (see **"Shipping Contents"** on page 27).

Step 2. Register your Vivato AP/Bridge. You can select **Register Online Now!** here if you currently have an internet connection and are using the online version of the User Guide, or go to **http://www.vivato.net/wifiregistration.html.**

Step 3. Analyze your site to estimate the best place to deploy the AP/Bridge. See **Where to Position The AP/Bridge**.

Step 4. Attach the two antennas.

Step 5. Configure the AP/Bridge. You can configure it before or after positioning it.

Step 6. Connect the AP/Bridge to your network.

Step 7. Verify AP/Bridge operation using a Wi-Fi client. See **"Verifying Wi-Fi Operation"** on page 149.

Where to Position The AP/Bridge

Where you position the AP/Bridge depends on your intended application and the physical surroundings. The applications are described in **"Network Configuration Examples"** on page 26.

The following conditions must be considered regardless of your application:

- Availability of mains (AC) power and LAN connections.
- Wall construction materials and other wireless signal obstructions (elevator shafts, metal panels, water pipes...).
- Interfering signal sources (microwave ovens, 2.4 GHz cordless phones, other 802.11b devices...).
- Temperature and humidity (see **"Specifications"** on page 27).

Antenna Polarization and Positioning

Antenna “polarization” describes how radio waves are propagated by an antenna; either up and down (vertically) or side to side (horizontally). Devices with the same antenna polarization can communicate more efficiently than devices with different polarization.

The AP/Bridge’s antennas can be adjusted 90 degrees to allow transmission and reception of signals that are vertically or horizontally polarized. The Vivato Wi-Fi Base Station’s antenna is horizontally polarized, however this orientation can be affected somewhat by its signals being reflected off of hard surfaces. Whenever you are using the AP/Bridge, especially with a Wi-Fi Base Station, you should always adjust the antennas on the AP/Bridge to obtain the strongest signal level at the receiving device(s).

When using a wireless distribution system (WDS) link between the AP/Bridge and a Vivato Wi-Fi Base Station, use the "wireless associations" function in the base station to monitor the signal strength of the WDS signal at the wireless interface used for the WDS link. Adjust the antenna on the AP/Bridge to maximum the received signal level at the base station.

Interfering Signal Sources

IEEE 802.11b devices share the same unlicensed frequency band as other common devices, such as some radio frequency identification (RFID) systems, many newer cordless telephones, and microwave ovens. These devices produce radio frequency (RF) energy that can interfere with the Wi-Fi AP/Bridge's signal. Whenever possible, you should eliminate or minimize the use of these devices within the AP/Bridge's operating area in order to maximize Wi-Fi data rates.

The Vivato Wi-Fi AP/Bridge also uses the same frequencies as conventional access points (APs). All 802.11b devices must use clear channel assessment, making sure that no other device is transmitting so that only one device is transmitting at a time. This prevents multiple devices on the same radio frequency (RF) channel in the area from interfering with each other, but requires these devices to take turns, reducing the overall available throughput for each device.

When using the AP/Bridge with a Vivato Wi-Fi Base Station, use the Wi-Fi Base Station's rogue access point detector (RAPD) to determine which channel has the least traffic and the least interference, and set the Wi-Fi Base Station to use that channel. Refer to the *Vivato Outdoor Wi-Fi Base Station Deployment Guide* on the Vivato Customer Support website for more information on the possible sources of interference and their effects on Wi-Fi operation.

Access Point Positioning

When used as a stand-alone access point, position the AP/Bridge to provide the greatest line-of-sight access to the most clients. Whenever possible, mount the AP/Bridge in a central location that is above cubicle walls or other obstacles.

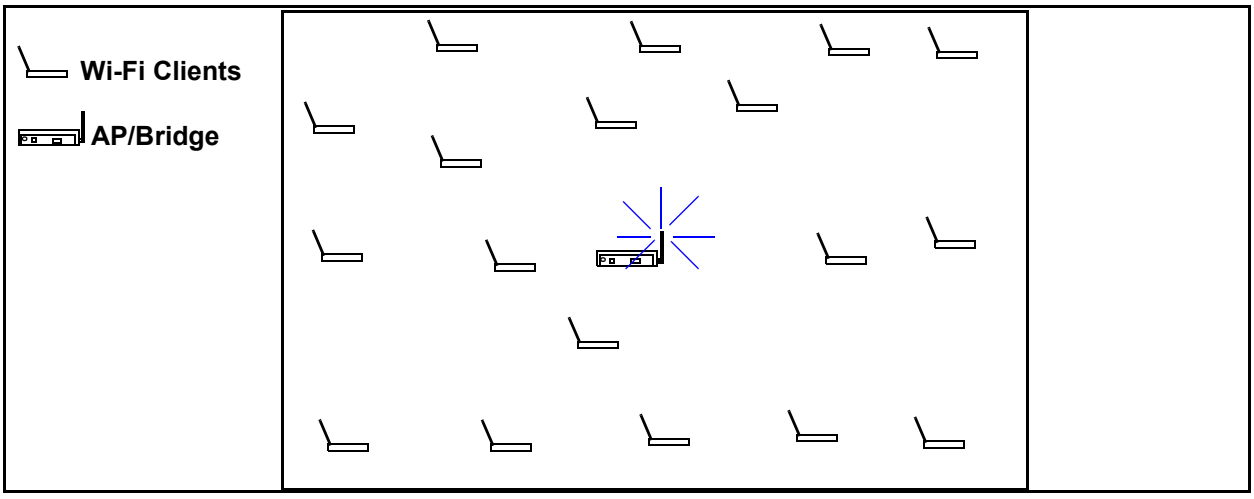


Figure 2—Access Point Location

 Copyright © 2004, Vivato, Inc.

Coverage Filler Positioning

When used with the Vivato Indoor Wi-Fi Base Station to fill a blocked area of Wi-Fi coverage, position the AP/Bridge where it has a good signal from the Wi-Fi Base Station (clear line-of-sight path when possible) and close to the clients that associate with it.

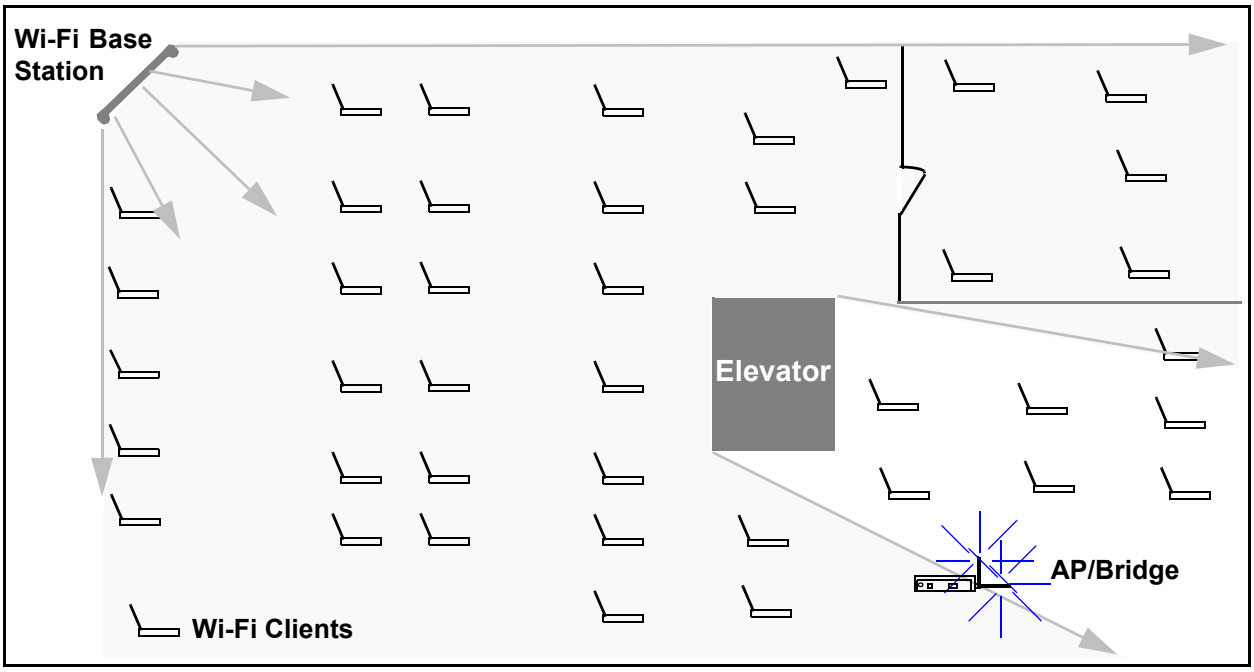


Figure 3—Hole Filler Location Example

Wireless Backhaul Positioning

When used to provide a wireless backhaul connection to a Vivato Wi-Fi Base Station that only has a power connection, position the AP/Bridge as close as possible to the Wi-Fi Base Station (clear

line-of-sight path when possible). When used with an outdoor Wi-Fi Base Station, this is often achieved by putting the AP/Bridge next to a window with a clear view of the Base Station.

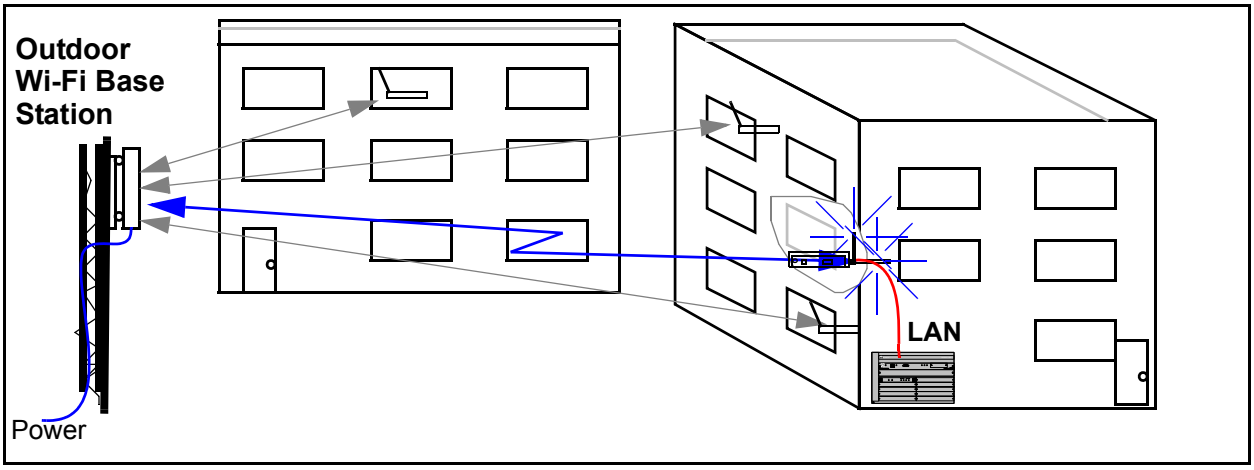


Figure 4—Wireless Backhaul Example

Range Extension Positioning

When used to extend the range of a Vivato Wi-Fi Base Station's Wi-Fi area, position the AP/Bridge as close as possible to the Wi-Fi Base Station (clear line-of-sight path when possible). When used with an outdoor Wi-Fi Base Station, this is often achieved by putting the AP/Bridge next to a window with a clear view of the Base Station.

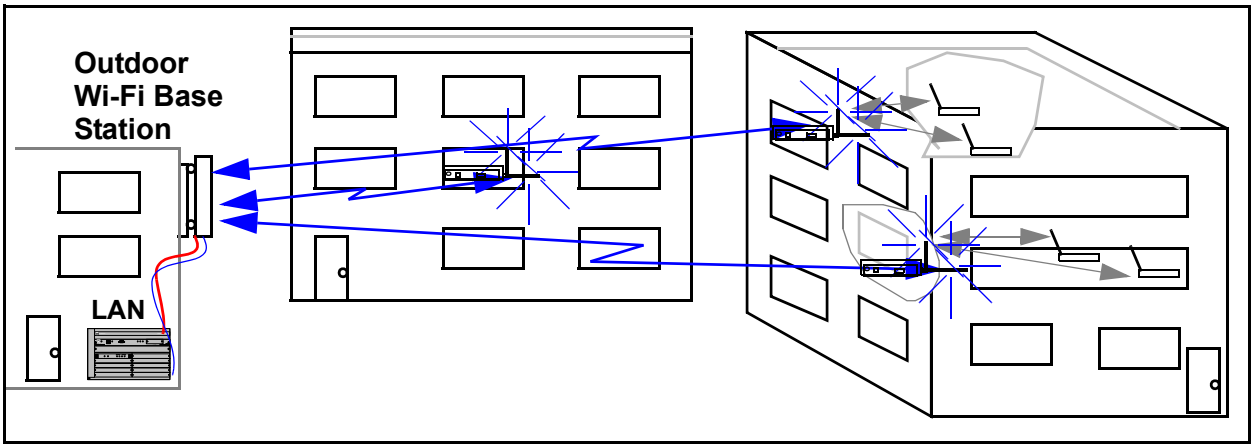


Figure 5—Wireless Backhaul Example

 Copyright © 2004, Vivato, Inc.

Preparing the AP/Bridge for Operation

To prepare the AP/Bridge for use:

Step 1. Thread the two supplied antennas finger tight into their connections (do not over tighten).

Step 2. Plug the power supply into a wall outlet that matches voltage range labeled on the power supply shipped with your AP/Bridge, and insert the power supply terminal into its connector on the Wi-Fi AP/Bridge.

Caution

Unless the Wi-Fi AP/Bridge is going to be configured using a wireless connection, never use a powered Ethernet connection to power the AP/Bridge during the initial configuration. Connecting a PC, hub, or other device to the powered Ethernet line may permanently damage it if it was not designed for this type of operation!

Step 3. Configure the AP/Bridge, using either the built-in Web interface or the command line interface. Refer to **"Initial Configuration Using the Built-In Web Pages"** on page 35 or **"Configuration Using The Command Line Interface"** on page 95.

Step 4. Connect a LAN cable from the Ethernet port to your wired network.

Initial Configuration Using the Built-In Web Pages

The Vivato Wi-Fi AP/Bridge can be quickly configured using its built-in VivatoVision™ web pages

Using the supplied Ethernet crossover cable and a computer with a network interface card that is set up for TCP/IP communication, you can quickly access the web pages to start configuration. If your computer has an IEEE 802.11b wireless client interface card installed and configured, you can access the configuration web page over the wireless connection.

Caution

Security settings are initially disabled to allow your computer or client to access the web pages and configure the Wi-Fi AP/Bridge. To ensure Wi-Fi security before putting the AP/Bridge into service, make the necessary changes to the security settings during the initial configuration. See **"Security Configuration Web Pages"** on page 71.

Steps to Configuring the Vivato Wi-Fi AP/Bridge

Step 1. Connect a computer to the Wi-Fi AP/Bridge and access the Vivato Vision© web pages. See **"Configuration Connections"** on page 36.

Step 2. Enter the initial configuration information on the Quick Setup pages. See **"Entering the Initial Configuration Information in the Quick Setup Pages"** on page 43.

Step 3. Reboot the Wi-Fi AP/Bridge. The settings on the Quick Setup pages do not take effect until after the Wi-Fi AP/Bridge has been rebooted.

Step 4. Using the IP address and Read password that you specified during the Quick Setup, access the Vivato Vision web pages again.

Step 5. Click on "**Enable Mode**" (upper right corner) and enter the Enable password you entered during the Quick Setup.

Step 6. Edit the security settings as needed to secure your network. See **"Security Configuration Web Pages"** on page 71.

Step 7. Review the **Default Configuration** information to see if there are other changes that need to be made to the configuration that are not part of the Quick Setup settings.

Step 8. Connect a cable from your LAN to the Wi-Fi AP/Bridge's LAN port.

Step 9. With your 802.11b clients properly configured, you should now have secure Wi-Fi operation between your clients and your LAN. See **"Verifying Wi-Fi Operation"** on page 149 to see how you can make sure that everything is working as expected.

Default Configuration

The Wi-Fi AP/Bridge is delivered with the following settings pre-configured. Until you change *and save* the configuration, these settings are used anytime the Wi-Fi AP/Bridge is rebooted. Pressing and holding the **RESET** button for at least three seconds will remove a saved "startup-config" file and restore these original defaults:

- **All client security features are disabled**. *Unless your network is intended to be open to anyone who wants to access it, you should enable security in the Wi-Fi AP/Bridge before putting it into service.* This can be done by selecting **Security Options** on the Quick Setup web pages. You can also select the **Security** tab from the Vivato Vision Home page.
- **A default bridge (called br0) connects the RJ-45 Ethernet interface to the wireless interfaces**. This allows either a 10/100 Ethernet port or a wireless interface to be used for configuration, and provides immediate Wi-Fi operation with 802.11b clients. However, until you have configured your preferred method of security, you should not connect the Wi-Fi AP/Bridge to your wired network.
- **A static IP address of 169.254.20.1 and a net mask of 255.255.0.0 are assigned to the default bridge (br0).** *You usually need to change the IP address and net mask to operate with your network.* This is one of the settings you can change on the Quick Setup web pages.
- **The default ESSID, the name that appears on wireless clients to identify the Wi-Fi AP/Bridge, is set to "Vivato"**. You do not have to change this entry, but you would typically set it to a name that would identify your system. This is one of the settings you can change on the Quick Setup web pages.
- **Wi-Fi channel 1 is assigned to wireless interface 0 (wlan0), and wireless interface 1 (wlan1) is disabled.** If necessary, channel assignments can be changed using the Quick Setup pages by selecting **Wireless Options**, or by using the **Network>Wireless** web page. For more information, see **"Network>Wireless Interfaces"** on page 66.
- **A secure shell key has been generated, and secure shell operation is enabled to allow configuration using a secure shell program.**
- **Hyper-text transfer protocol security (HTTPS) operation is enabled to allow access to the built-in configuration web pages.**

Configuration Connections

You can access the Vivato Vision web pages in the Wi-Fi AP/Bridge using either a wired or a wireless connection. Once the connection has been established, the procedure to configure the Wi-Fi AP/Bridge is the same for either type of connection.

The Wi-Fi AP/Bridge should be powered on for at least 30 seconds before configuration.

 Copyright © 2004, Vivato, Inc.

Enabling Your Computer's Network Adapter to Access the Wi-Fi AP/Bridge

The default IP address of the Wi-Fi AP/Bridge is 169.254.20.1, with a netmask of 255.255.0.0. Your computer's network interface must be assigned an IP address within the range of 169.254.0.1 to 169.254.255.254 (such as 169.254.20.2) to initially access the configuration web pages or to access the command line interface using a secure shell.

You can set your interface's IP address manually by accessing the TCP/IP settings for the interface, disabling DHCP operation, and specifying an IP address in this range. You can also use automatic private IP addressing (APIPA) to set the network interface's IP address within the necessary range.

APIPA assigns an IP address to a network interface if dynamic host configuration protocol (DHCP) is enabled for the interface but a DHCP server is not found within about one minute after the computer is powered on. Microsoft® Windows® 2000, XP, and 98SE support this feature.

Important	To ensure a quick connection to the Wi-Fi AP/Bridge for the initial configuration, disconnect your computer from any networks. This prevents a DHCP server on your network from interfering with the process of assigning the appropriate IP address to the network interface being used for the configuration connection.

For more information on APIPA, go to the following link:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dniph/html/pnpip.asp

After you have accessed the configuration pages or command line interface, you can change the IP address of the Wi-Fi AP/Bridge to operate in your network.

Using APIPA to Assign a Usable IP Address For Your Client

To get APIPA to assign an IP address to your interface that is accessible by the Wi-Fi AP/Bridge, use the following steps and refer to **Figure 1—Enabling Automatic IP Address Assignment on Your Wireless Client**:

Step 1. Verify that DHCP is enabled for the interface (see below). In Windows, go to **Start** > **Settings** > **Network Connections**, and right-click on the interface connection to configure.

Step 2. Left-click on **Properties**.

Step 3. Select **Internet Protocol (TCP/IP)** and left-click on **Properties**. Make sure **Obtain IP Address Automatically** is checked.

Step 4. Select the **Alternate Configuration** tab, and verify that **Automatic private IP address** is checked.

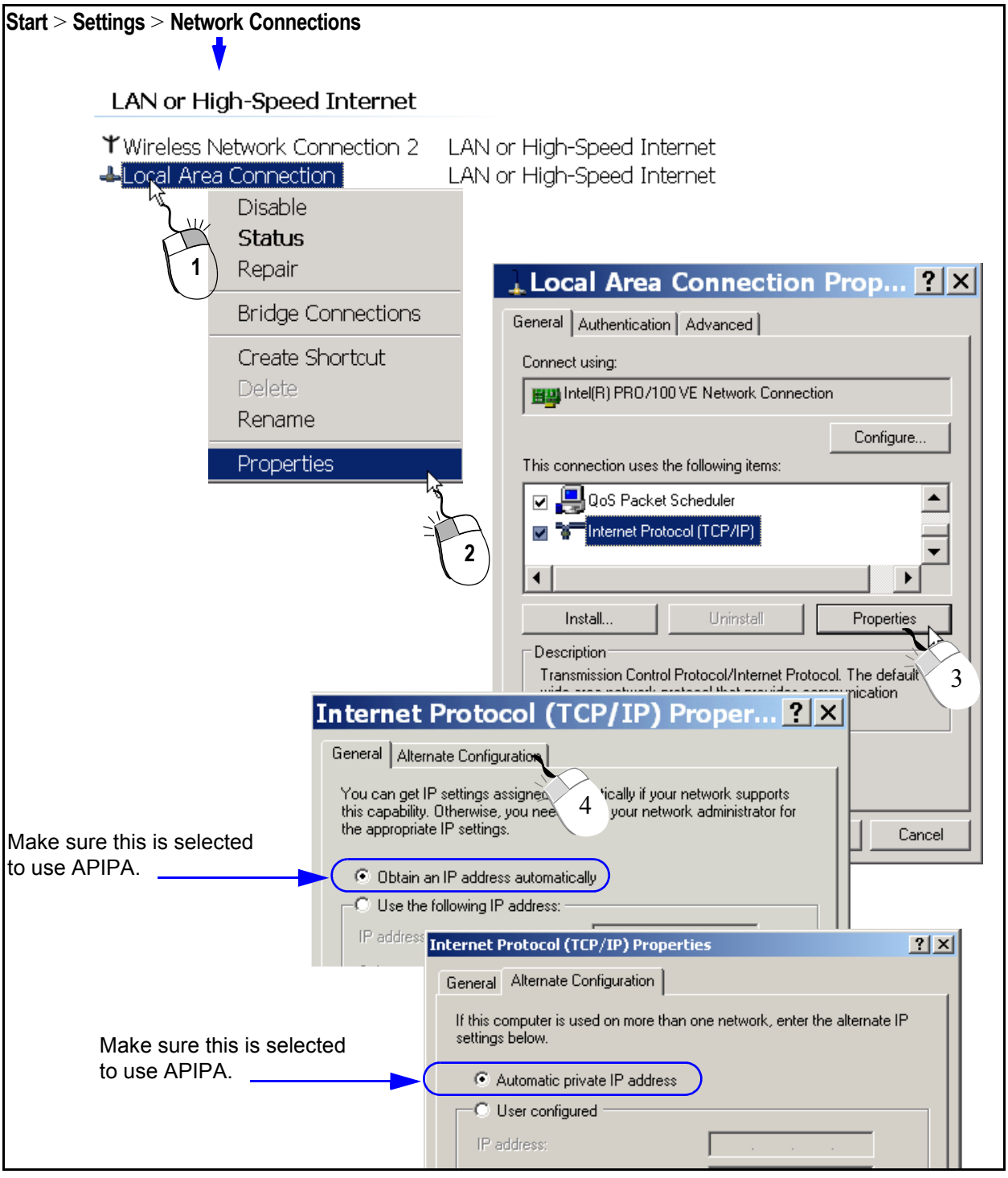


Figure 1—Enabling Automatic IP Address Assignment on Your Wireless Client

Step 5. Shut down your computer.

Step 6. Follow the steps described below for the type of connection you are using (wired or wireless).

 Copyright © 2004, Vivato, Inc.

Wired Connection to Access the Configuration Web Page

After the Wi-Fi AP/Bridge has been powered on for at least 30 seconds, connect the supplied crossover Ethernet cable between your computer's network interface card (NIC) and the Wi-Fi AP/Bridge's Ethernet port.

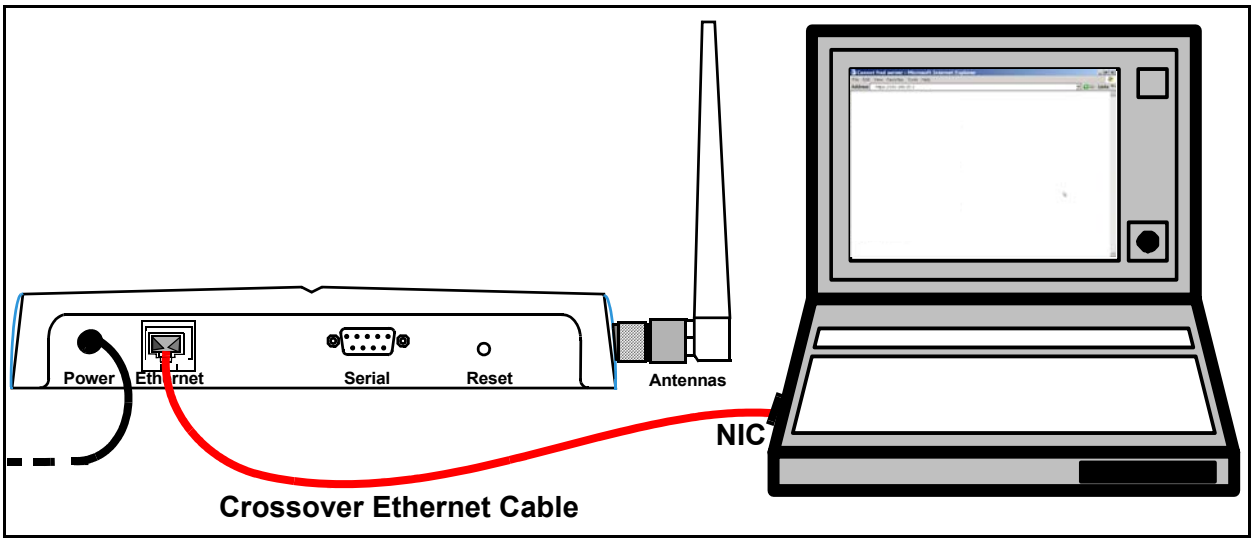


Figure 2—Wired Connection To Access The Configuration Web Page

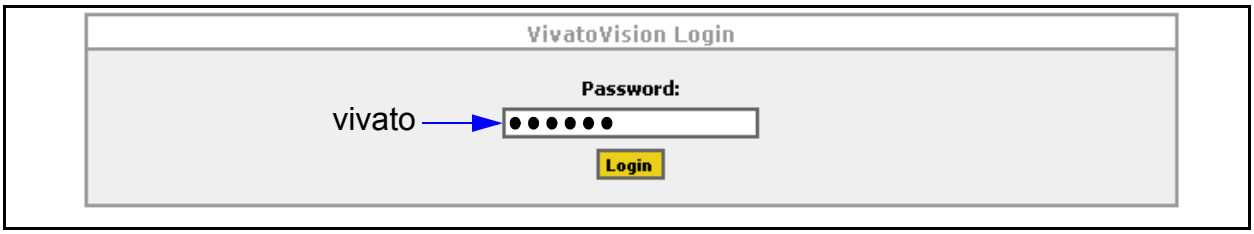
Step 1. Turn on your computer.

Step 2. If APIPA is being used to assign an IP address for the NIC, wait for the DHCP server search to time-out and issue an address to the interface (about one minute). If APIPA is not being used, assign a static IP address of 169.254.20.2 to your NIC.

Step 3. Launch a web browser in your computer. All popular browsers are supported. The minimum recommended display resolution is 800 x 600 pixels. The webpages are configured using a secure socket layer (SSL) connection.

Step 4. Enter the following Wi-Fi AP/Bridge IP address in the Address/Location field in your browser: **https://169.254.20.1**. A "Security Alert" may be displayed (shown below), asking if you want to proceed with connecting to the Wi-Fi AP/Bridge. Select "Yes".

Step 5. The Wi-Fi AP/Bridge’s login prompt appears on your browser. Enter the default password: **vivato**



Important	Only the “Read” level password is needed *the first time* you access the Quick Setup web pages to configure and reboot the Wi-Fi AP/Bridge. However, the next time you access the Quick Setup pages you are also required to enter the Enable password before you are allowed to make any changes to the configuration. The Enable password is created during the initial configuration.

Step 6. Click on **Login** to display the initial Quick Setup page. See **"Entering the Initial Configuration Information in the Quick Setup Pages"** on page 43.

 Copyright © 2004, Vivato, Inc.

Wireless Configuration Connection

Step 1. Disconnect any wired network connections to your computer.

Step 2. Turn your computer on and provide power to the AP/Bridge.

Step 3. Enable your computer's wireless client. In the Microsoft Windows environment, this is typically done by selecting **Start > Settings >Network Connections > Wireless Network Connection**.

Step 4. If APIPA is being used to assign an IP address for the wireless interface, wait for the DHCP server search to time-out and issue an address to the interface (about one minute). If APIPA is not being used, assign a static IP address of 169.254.20.2 to your interface.

Step 5. Using your client's "Available Networks" or other search function, select the "**Vivato**" entry.

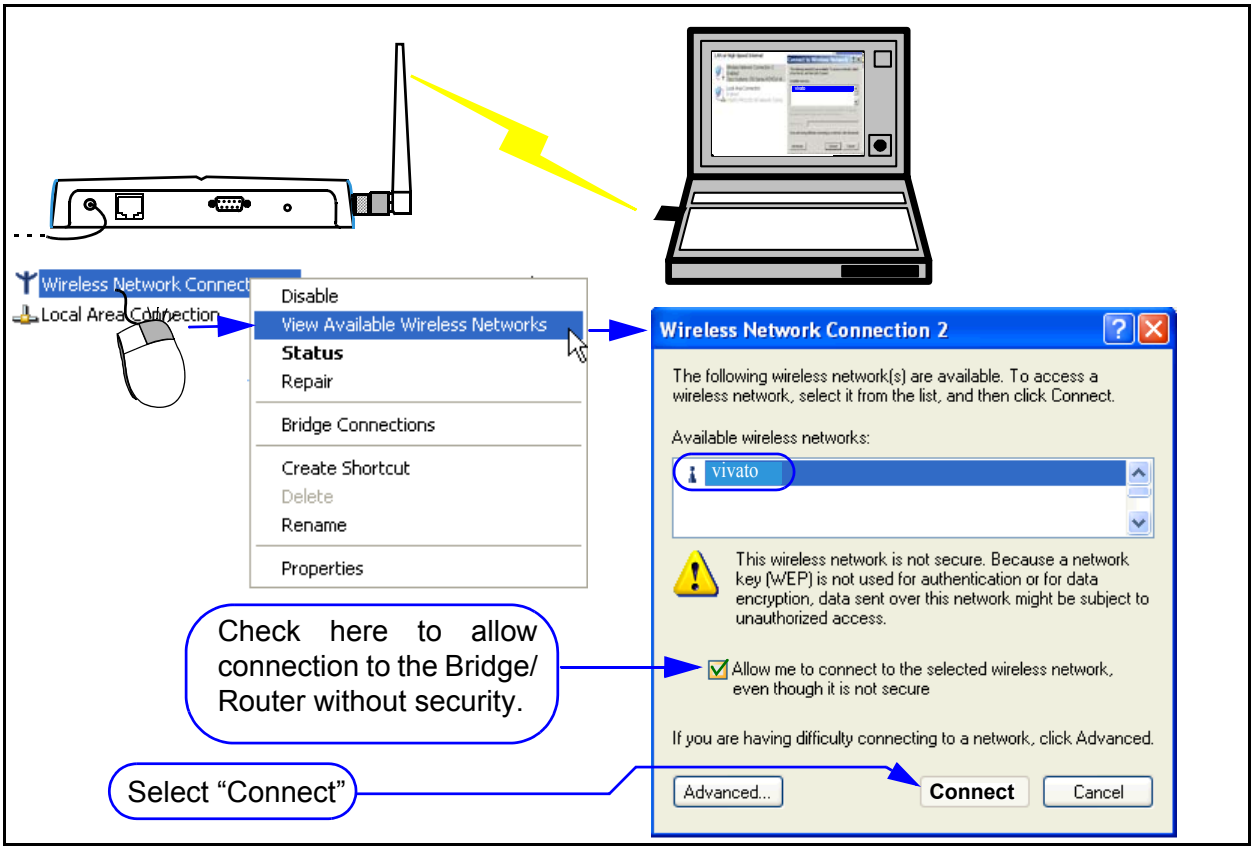


Figure 3—Wireless Connection to Access the Configuration Web Pages

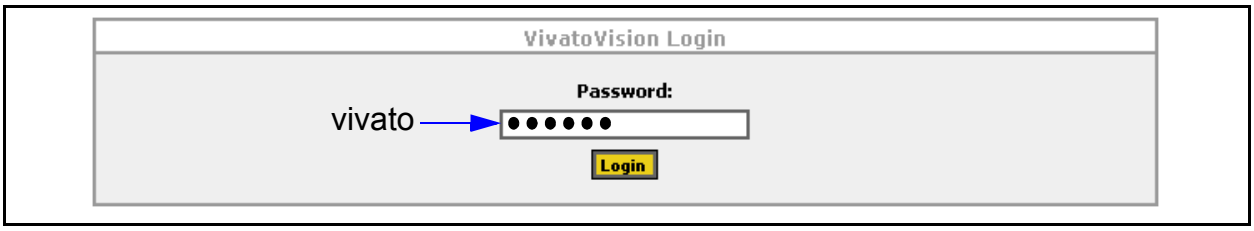
Because the Wi-Fi AP/Bridge is delivered with wireless security disabled to allow configuration through a wireless connection, you may need to confirm using an unsecured connection.

Note: As you are configuring the Wi-Fi AP/Bridge's security settings, you will have to enable each corresponding security setting in your client to re-enable wireless access to the Wi-Fi AP/Bridge. For example, after enabling WEP on the Wi-Fi AP/Bridge during the initial configuration, the AP/Bridge will require the use of WEP and the correct encryption key on your client to re-access the Wi-Fi AP/Bridge after reboot.

Step 6. Select "**Connect**" to begin associating with the Wi-Fi AP/Bridge.

Step 7. Launch a web browser in your computer. All popular browsers are supported. The minimum recommended display resolution is 800 x 600 pixels. The webpages are accessed using a secure socket layer (SSL) connection.

Step 8. Enter the following Wi-Fi AP/Bridge IP address in the Address/Location field in your browser: **https://169.254.20.1**. The Wi-Fi AP/Bridge's login prompt appears on your browser.



Step 9. Enter the default password: **vivato**

Important	Only the "Read" level password is needed *the first time* you access the Quick Setup web pages to configure and reboot the Wi-Fi AP/Bridge. However, the next time you access the Quick Setup pages you are also required to enter the Enable password before you are allowed to make any changes to the configuration. The Enable password is created during the initial configuration.

Step 10. Click on **Login** to display the initial Quick Setup page.

 Copyright © 2004, Vivato, Inc.

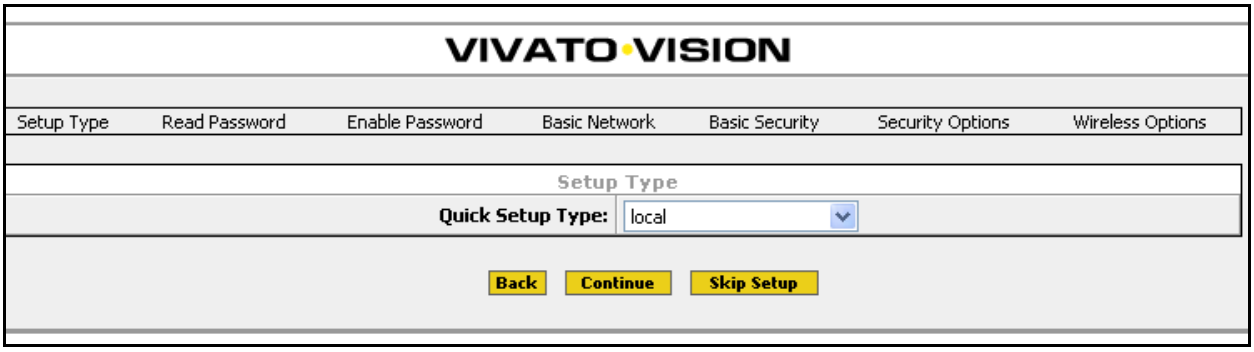
Entering the Initial Configuration Information in the Quick Setup Pages

Enter the information in the **Setup Type** screen and select **Continue** to continue to the **Read Password** settings. Continue to fill in the requested information on each screen until all of the Quick Setup screens have been configured and the Wi-Fi AP/Bridge is rebooted using the new settings. It is important that you do this before proceeding to change any other configuration settings when you first configure the Vivato Wi-Fi AP/Bridge.

The Quick Setup screens are displayed automatically the first time you access the configuration web pages. To access the Quick Setup screens at a later time, select **Quick Setup** on the **Home** configuration page.

Setup Type

The settings made on the Quick Setup screens can be used to configure the Wi-Fi AP/Bridge before using it, or to create a template to use as a starting point for future configuration.



Quick Setup Type

- Select "**local**" to use the Quick Setup settings to configure the Wi-Fi AP/Bridge.
- Select "**save locally as template**" to save the Quick Setup configuration as a file called "template-config" without actually changing the AP/Bridge's configuration. This allows you to create a configuration file to use as a base line for configuring other Wi-Fi AP/Bridges, or to use this file in the future to configure this Wi-Fi by renaming it "startup-config" and rebooting this AP/Bridge.

Read Password Setup

The read password protects unauthorized viewing of configuration settings.

Figure 4—Read Password Setup Page

- **Current "Read" Password**: Enter the current password used to allow you to view, but not alter, the Wi-Fi AP/Bridge's configuration. **The password is "vivato" when the Vivato Wi-Fi AP/Bridge is delivered.**
- **New "Read" Password**: Enter a new password to allow you to view the configuration web pages.
- **New "Read" Password Verification**: Enter the new password again.
- **Back**: Return to the initial Quick Setup screen.
- **Continue**: Select this control after entering all of the requested information. The settings on this form will not take effect until you select this command.
- **Skip Setup**: Selecting this control takes you to the configuration web pages without changing any of the settings on the Setup screen. You should only use this function after you have already filled out all of the information on the Setup screen before and have selected Continue to enter those settings.

 Copyright © 2004, Vivato, Inc.

Enable Password Setup

The enable password lets you change, save, and load configuration settings.

Figure 5—Enable Password Setup Page

- **Current "Enable" Password**: No default password is configured, therefore leave this field empty the first time you access this screen. If you have already created an enable password using the command line interface or by using the web interface's **System>Password** settings, enter that password.
- **New "Enable" Password**: Enter a new password used to let you to alter the Wi-Fi AP/Bridge's configuration.
- **New "Enable" Password Verification**: Enter the new password again.

Basic Network Setup

Basic Network settings identify your Wi-Fi AP/Bridge and specify settings needed to communicate on the local network.

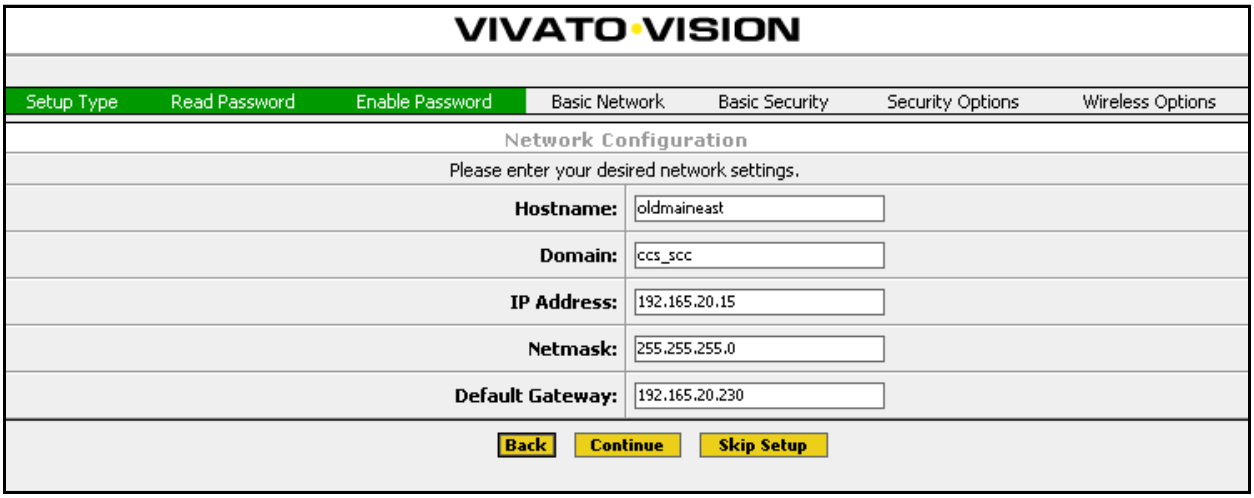


Figure 6—Basic Network Setup Page

- **Hostname**: Enter a name to be used to refer to the Wi-Fi AP/Bridge in your *wired* network. For your network to be able to identify the Wi-Fi AP/Bridge using this name it typically needs a domain name service (DNS) server.

  Note: This entry is NOT the name that *wireless* users see when searching for the wireless network; that name is specified for the extended service set identifier (ESSID).

- **Domain**: Enter the name of the domain where the Wi-Fi AP/Bridge will be used.

- **IP Address**: Enter a static IP address for the Wi-Fi AP/Bridge. The Quick Setup pages do not support DHCP client operation to obtain an automatic IP address; however, you can use the command line interface (CLI) to enable DHCP assignment of the IP address.

  Note: *The IP address and Netmask are assigned to the default bridge (br0) during the Quick Setup process. If you need to delete the default bridge for your desired configuration, enter the standard information in the Quick Setup pages and reboot the Wi-Fi AP/Bridge, then access the configuration pages again and select the* **Network** *tab. Assign the IP address to the desired interface (logical or physical) before deleting the bridge.*

- **Netmask**: Enter an IP net mask for the Wi-Fi AP/Bridge.

- **Default Gateway**: Enter the IP address of the default gateway for your wired network.

 Copyright © 2004, Vivato, Inc.

Basic Security Setup

The Basic Security settings are used to enable wired equivalent privacy (WEP) security. Unless your network is intended to be totally open for use by any 802.11b client, you should always WEP.

Note: To use 802.1x security, select **No Security** and proceed to the **Wireless Options** setup page and reboot the Wi-Fi AP/Bridge when prompted. 802.1x security is not configurable from the VivatoVision web interface in this firmware release, but can be configured using the command line interface.

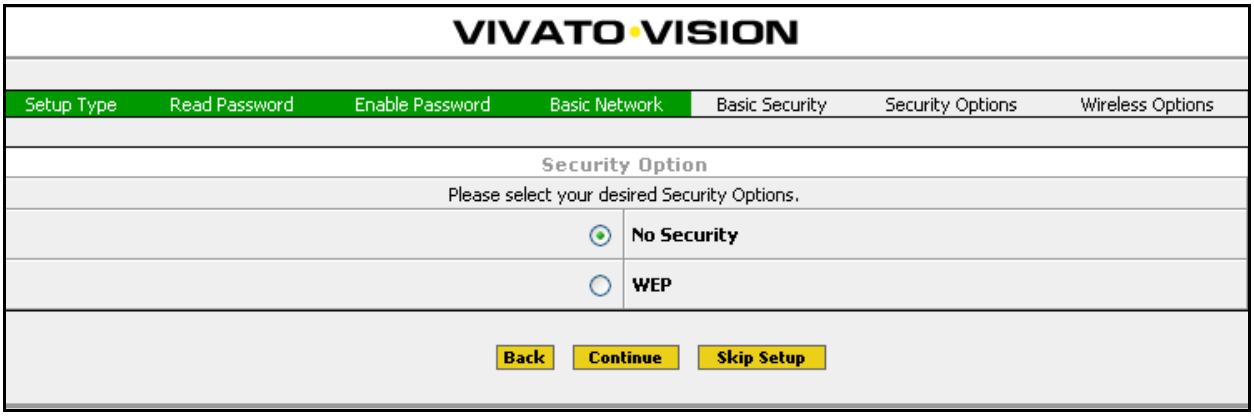
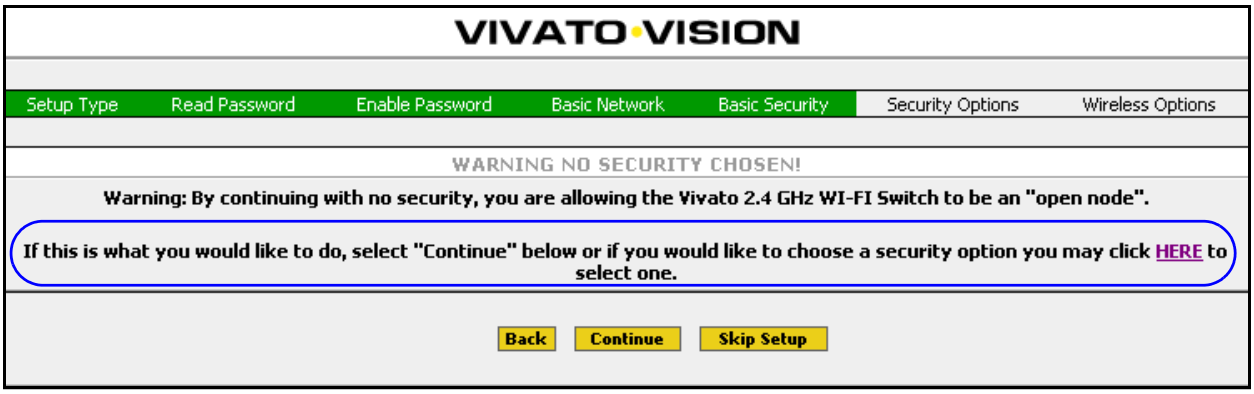


Figure 7—Basic Security Setup Page

- **No Security**: This setting allows any wireless client to associate with the Wi-Fi AP/Bridge without using passwords, data encryption, or authentication. Unless you are providing open Wi-Fi operation to anyone who desires it, this setting is not recommended. As shown below, you can select a link to take you back to the previous screen in order to select and configure WEP security.



- **WEP**: Use wired equivalent privacy. When WEP is selected, clicking on **Continue** causes a WEP setup screen to be displayed (see below). Select the **Key Type** (String or Hex), the **Key Index** (up to four WEP keys can be defined), and enter the **Key Value** (valid entries are 5 or 13 String characters or 10 or 26 hex digits).

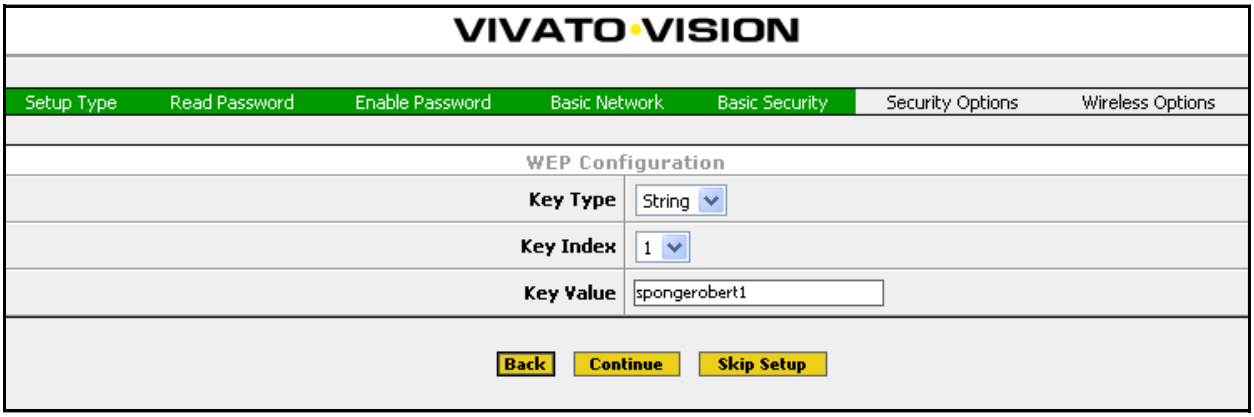
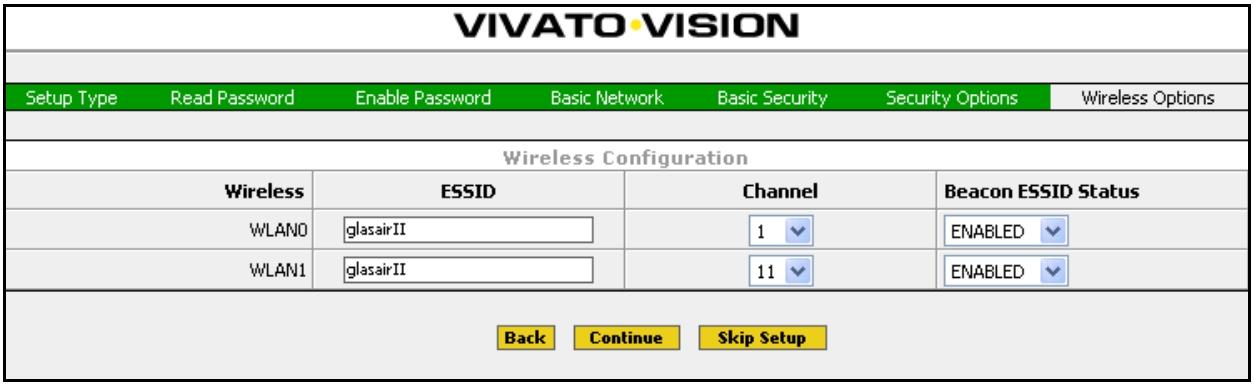


Figure 8—WEP Security Configuration During Quick Setup

Wireless Options Setup

Wireless options specify the extended service set identifier (ESSID) that the Wi-Fi AP/Bridge uses to identify itself to 802.11b clients and the channel number for both wireless interfaces. You can also prevent the ESSID from being sent to prevent unwanted clients from being able to identify the Wi-Fi AP/Bridge's signals.



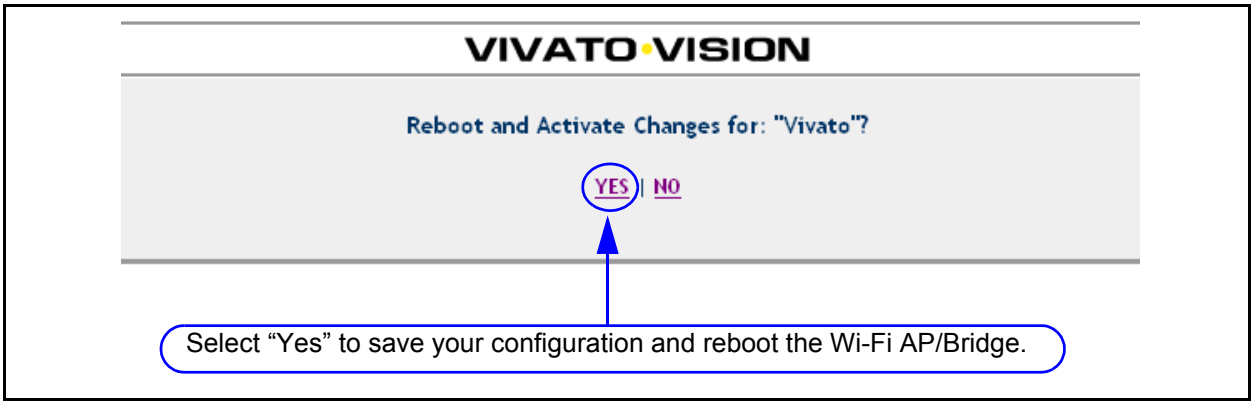
 Copyright © 2004, Vivato, Inc.

- **ESSID**: Enter the service set identifier for both wireless interfaces. When one interface is used as an access point for clients, and the other interface is used for a WDS connection to a Wi-Fi Base Station, you should use a different ESSID for each interface to differentiate their signals. Keep in mind that each client typically has a list of preferred SSIDs[1], and that each of the Wi-Fi AP/Bridge's ESSIDs intended for client connections must be added to that list to be able to move from the area serviced by one ESSID to the an area serviced by a different ESSID without losing service indefinitely.
- **Channel**: Select the channel number to use for both wireless interfaces. You should typically have one interface set to channel 1 and the other interface set to channel 11 (the default).
- **Beacon ESSID Status**: When set to "DISABLED", the ESSID is not sent on the beacons from the Wi-Fi AP/Bridge to the clients. This prevents Wi-Fi clients from being able to see the Wi-Fi AP/Bridge's ESSID in its "Available Networks" list. When beacons are disabled, the only way a client can associate with the Wi-Fi AP/Bridge is if the ESSID is known and is manually entered into the client's list of preferred networks.

Rebooting the Wi-Fi AP/Bridge

After entering your configuration information on all of the Quick Setup screens, you are prompted to reboot the Wi-Fi AP/Bridge. You must select "**Yes**" for your configuration to take effect. If you select "No", your configuration is not saved and the default configuration screens are displayed.

After waiting a couple of minutes for the Wi-Fi AP/Bridge to reboot using the new configuration, it should be ready to operate on your network. Connect your LAN cable to the Wi-Fi AP/Bridge's Ethernet port. Wi-Fi clients should be able to access your LAN through the Wi-Fi AP/Bridge at this time if their security settings have been properly configured.



1. ESSID and SSID are essentially the same thing. The Vivato Wi-Fi Base Station and AP/Bridge can broadcast on two or more wireless interfaces, so they create an "extended" service set.

Where Do I Go From Here?

That depends on how you are going to use the AP/Bridge:

- **Access Point operation**: If you are using the AP/Bridge as a stand-alone Access Point with WEP security, it will associate with your WEP-enabled clients now. Your clients should be able access your network. See **"Optimizing Your Wireless Client For Secure Communications"** on page 73 and follow the steps for configuring WEP in your client.
- **Coverage Filler, Repeater, and Wireless Backhaul operation:** To use the AP/Bridge with a Wi-Fi Base Station, you need to configure one of the wireless interfaces in *both* devices to form a wireless distribution system (WDS) link between them. This involves enabling WDS on a wireless interface on both devices and setting them to the same channel number, and telling them to use the other devices' wireless interface Mac address as the other end of the link.

  To configure WDS using the CLI, see **"Configure WDS (Wireless Distribution System)"** on page 139. To use the Web configuration pages, see **"Network>WDS"** on page 68

To make additional changes to the Wi-Fi AP/Bridge's configuration, you can access the configuration web pages over your local wired network or by using a wireless connection. However, you need to use the new IP address that you assigned to the Wi-Fi AP/Bridge and the new Read and Enable passwords you entered in the initial setup to gain access. Rather than use the Quick Setup screens to make changes, you now use the main configuration pages for customizing your configuration. See **"Navigating the Main Web Page Configuration Screens"** on page 51.

 Copyright © 2004, Vivato, Inc.

Using the Main Configuration Web Pages

The Quick Setup screens are used to configure the Wi-Fi AP/Bridge for basic, secured Wi-Fi operation. All of the settings configured on the Quick Setup screens, and many additional settings, are available on the main configuration pages.

Navigating the Main Web Page Configuration Screens

The Home page is the default configuration screen that appears after initially configuring the Wi-Fi AP/Bridge. Select one of the tabs (such as **Security**) to view and configure other settings.

Each main topic screen contains links to access associated settings (see below). For example, the Home page has sub-menus titled **Summary** and **Quick Setup**. The sub-menu heading in bold (in this case "Summary") is the page currently being displayed.

In the upper-right corner of every page is the **Enable Mode** link. Unless you have already entered the enable password on the Quick Setup page during the current configuration session, you need to select **Enable Mode** and enter the enable password to change configuration settings. When you have finished configuring the Wi-Fi AP/Bridge, select **Logout of Vivato Vision** to end your configuration session.

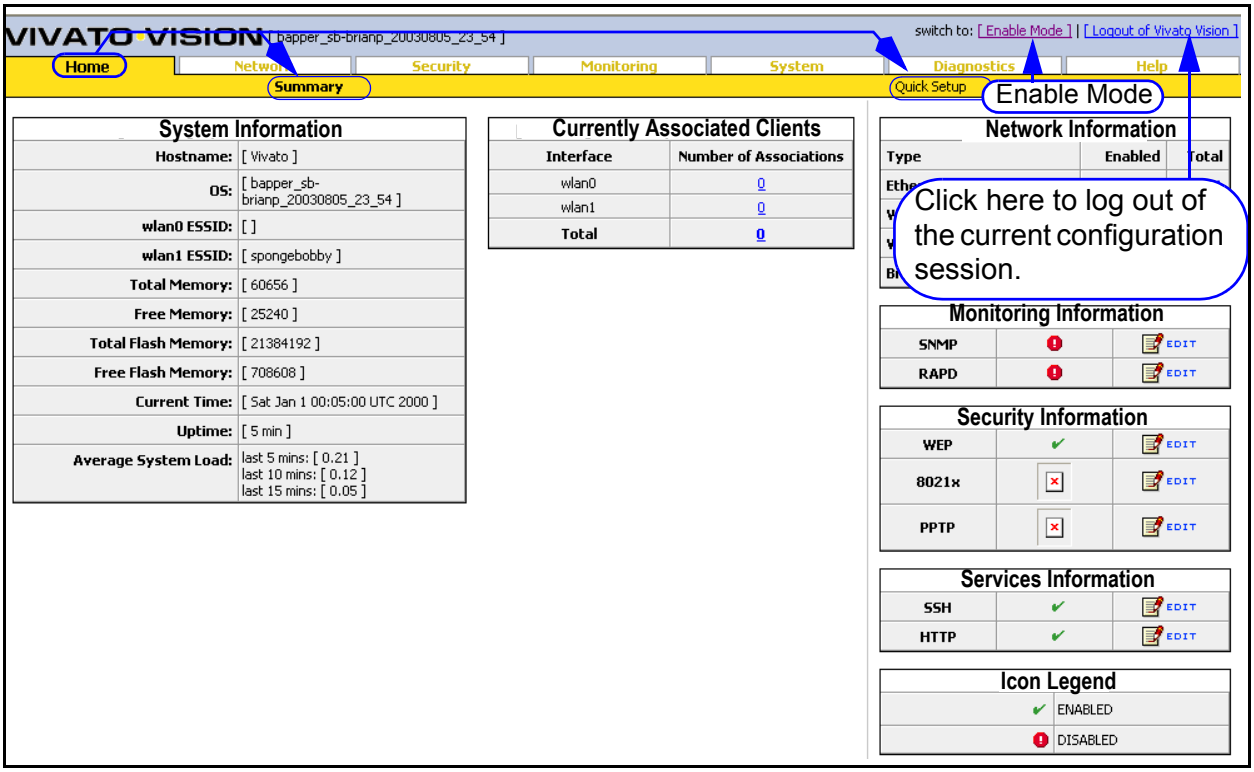


Figure 9—Accessing Settings From the Home Configuration Screen

Status Indicators

The following symbols are used to indicate the status of functions accessed on the configuration web pages:

indicates that the function is disabled.

indicates that the function is enabled.

click to edit this setting.

Home

The Home page is displayed each time the configuration web pages are accessed. The following settings are accessed from the Home page sub-menus:

Home>Summary

The Summary page displays an overview of Wi-Fi AP/Bridge hardware and system configuration (see **"Accessing Settings From the Home Configuration Screen"** on page 51).

System Information

This area displays an overview of the Wi-Fi AP/Bridge's resources and operation.

- **Hostname:** The Hostname that you assigned.
- **OS:** Version of the Wi-Fi AP/Bridge's software.
- **wlan ESSID**: The ESSID assigned to each wireless interface.
- **Total Memory**: Amount of memory in the AP/Bridge.
- **Free Memory**: Memory available for system use.
- **Total Flash Memory**: The total amount of flash memory used for storing the Wi-Fi AP/Bridge's firmware and configuration files.
- **Free Flash Memory**: The amount of flash memory available for storing another firmware version and/or configuration files.
- **Current Time**: Time of day.
- **Uptime**: Length of time that the Wi-Fi AP/Bridge has been up since its last reboot.
- **Average System Load:** Percentage load on the system processor for the last minute, five minutes, and 15 minutes.

 Copyright © 2004, Vivato, Inc.

Currently Associated Clients

This area displays the number of clients currently associating through each wireless interface. Clicking on the number of clients value displays details for the associating client(s).

Network Information

This area displays the number of physical and logical interfaces that are present. Clicking on a value takes you to the network settings used to configure the associated interface.

Monitoring Information

This area displays the status of simple network management protocol (SNMP) operation. Click on **Edit** to access the configuration settings.

Security Information

This area displays the status of each type of security available in the Wi-Fi AP/Bridge. Click on **Edit** to access the configuration settings.

Services Information

This area displays the status of the hypertext transfer protocol (HTTP) daemon, used to provide access to the web interface, and the secure shell (SSH) daemon, used to provide access to the command line interface using a secure shell program. Click on **Edit** to access the configuration settings.

Home>Quick Setup

Displays the initial Quick Setup menu used when first configuring the Wi-Fi AP/Bridge. If you selected **Skip Setup** when the Setup screen was first displayed, you can select the **Quick Setup** link to return to the setup screens to make those initial configuration settings.

 Copyright © 2004, Vivato, Inc.

Network Configuration Web Pages

The **Network** tab accesses screens for configuring all of the physical and logical interfaces within the Wi-Fi AP/Bridge. Settings for changing IP addresses and wireless interface channel numbers, creating bridges, and creating static IP routes are easily accessed.

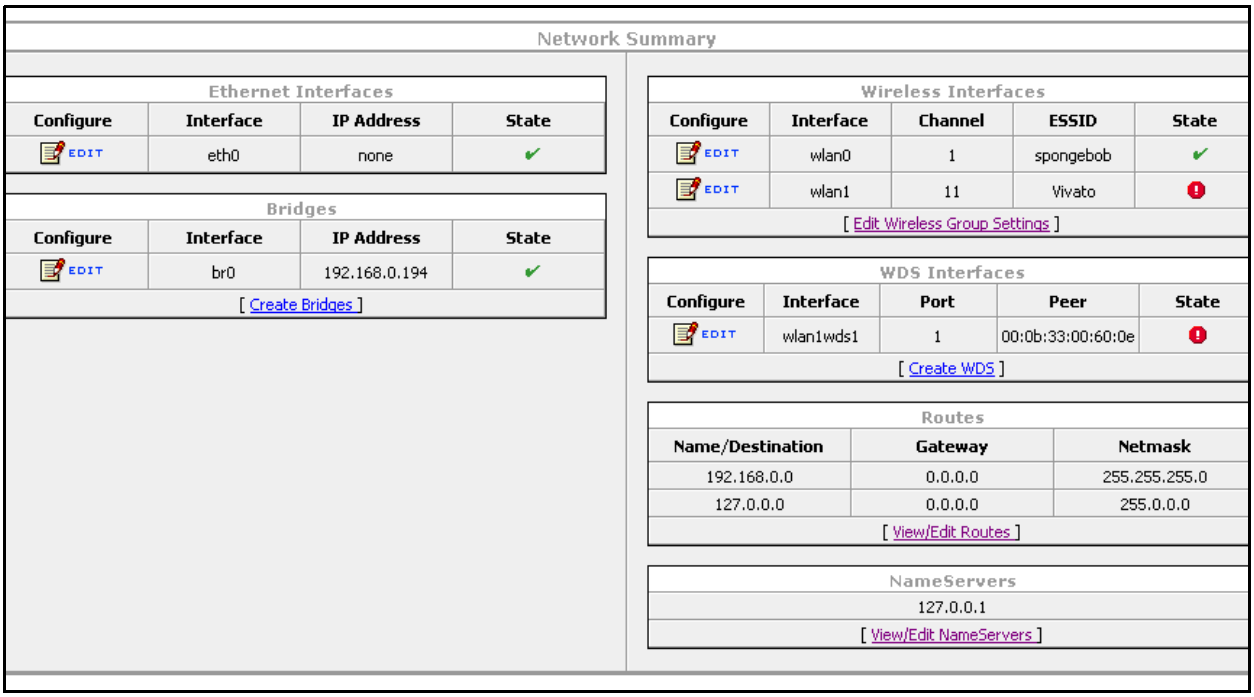
Network Settings

Network settings are arranged on the following configuration pages:

- **Network>Summary** - Summary of current interface settings and routes.
- **Network>General** - Configuration of static routes, name servers, and hosts.
- **Network>Bridge** - Configuration of bridges.
- **Network>DHCP** - Configuration of a dynamic host control protocol (DHCP) server for automatic IP addressing in clients.
- **Network>Ethernet Interface** - Configuration of the Ethernet interfaces.
- **Network>Wireless Interfaces**- Configuration of the wireless interfaces (channels, ESSID, bit rate...)
- **Network>WDS** - Configuration of wireless distribution system (WDS) operation with a Vivato Wi-Fi Base Station.

Network>Summary

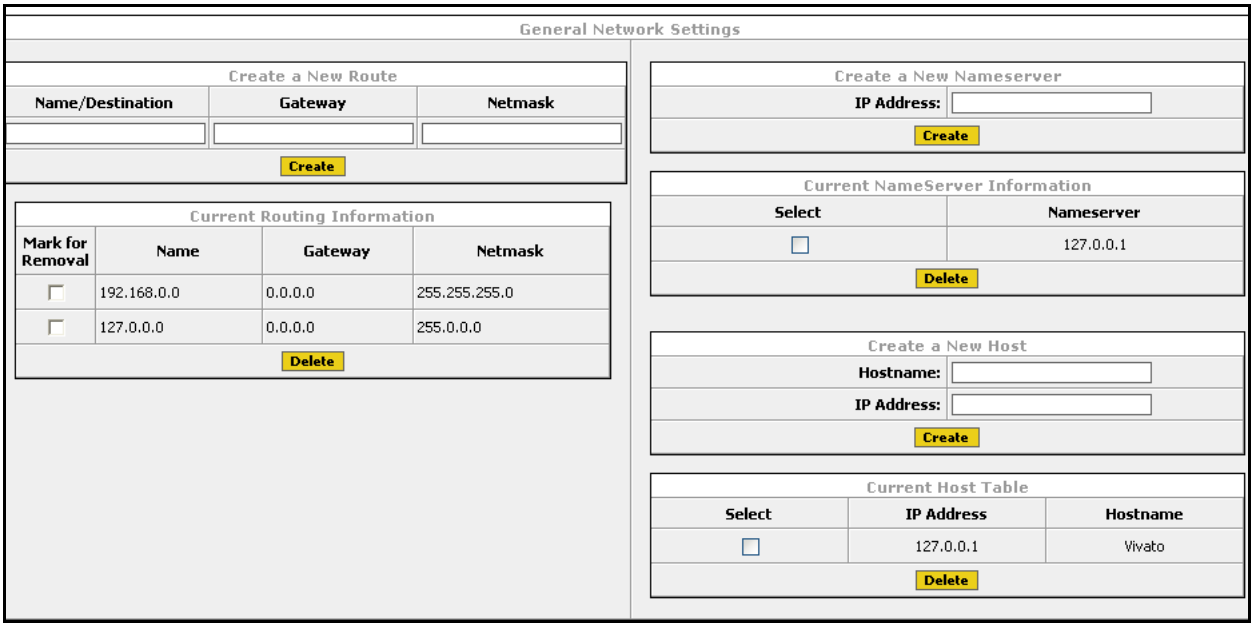
This page provides an "at a glance" overview of the network interfaces, and provides access to the those configuration settings. Click on EDIT for any interface to change its settings.



 Copyright © 2004, Vivato, Inc.

Network>General

The General Network Settings are used to specify other devices in your network that the Wi-Fi AP/Bridge must communicate and the routes used to get there.



Create a New Route

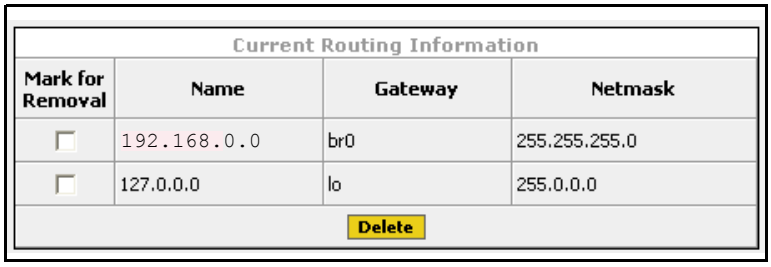
Routes tell the Wi-Fi AP/Bridge where to send packets destined for specified IP addresses.

- **Name/Destination**: Enter the host name or IP address prefix of the destination to which you are trying to connect. For example, if a host called “bonanza” is at IP address 192.163.20.17, you could either enter “bonanza” or “192.163.20.0”. When entering a host name, the host name and its IP address must first be entered into the host table using the **Create a New Host** function.
- **Gateway**: Enter the IP address of the gateway used to access addresses on the destination subnet.
- **Netmask**: Enter the subnet mask that defines the range of IP addresses for this route.

Current Routing Information

The Current Routing Information table indicates how packets within specified IP address ranges are directed (routed). In the example below, all packets addressed to the 192.165.0.0 base IP address that are within the Netmask of 255.255.255.0 are routed through the default bridge - br0.

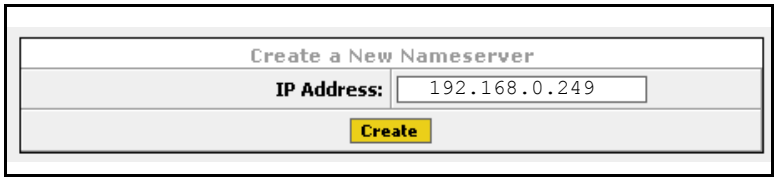
The 127.0.0.0 route is a loopback path used by the Wi-Fi AP/Bridge's host, and should not be deleted.



- **Mark for Removal**: Click in this box and select **Delete** to remove this route.
- **Gateway**: The interface that the Wi-Fi AP/Bridge uses to forward traffic to the destination address.
- **Netmask**: The subnet mask defining the range of IP addresses accessed through this route.

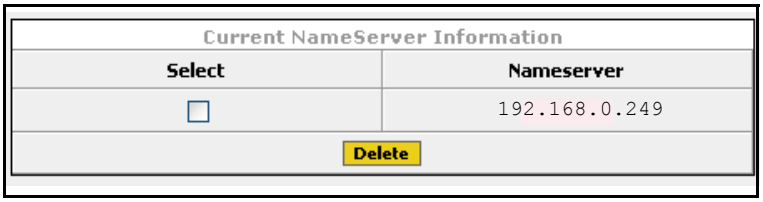
Create a New Nameserver

A domain name server (DNS) translates Internet domain names into their IP addresses, allowing domain names to be used in place of their IP addresses. Enter the IP address of a domain name server on your network and select **Create**. Up to three domain name servers can be specified.



Current NameServer Information

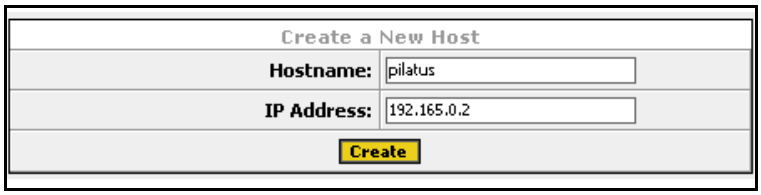
Up to three domain name servers can be used by the Wi-Fi AP/Bridge. To remove a name server from the configuration, check the **Select** box for that name server and select **Delete**.



 Copyright © 2004, Vivato, Inc.

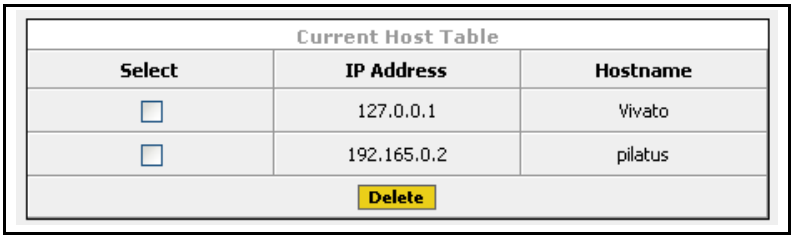
Create a New Host

When a host is created, its host name and IP address are added to the Wi-Fi AP/Bridge's host table. When host names are used during file transfers or other operations, the Wi-Fi AP/Bridge automatically associates that host name with its specific IP address.



Current Host Table

The Wi-Fi AP/Bridge's host table lists the hosts and their corresponding IP addresses that have been entered. To remove a host from the host table, check the **Select** box for that host and select **Delete**.



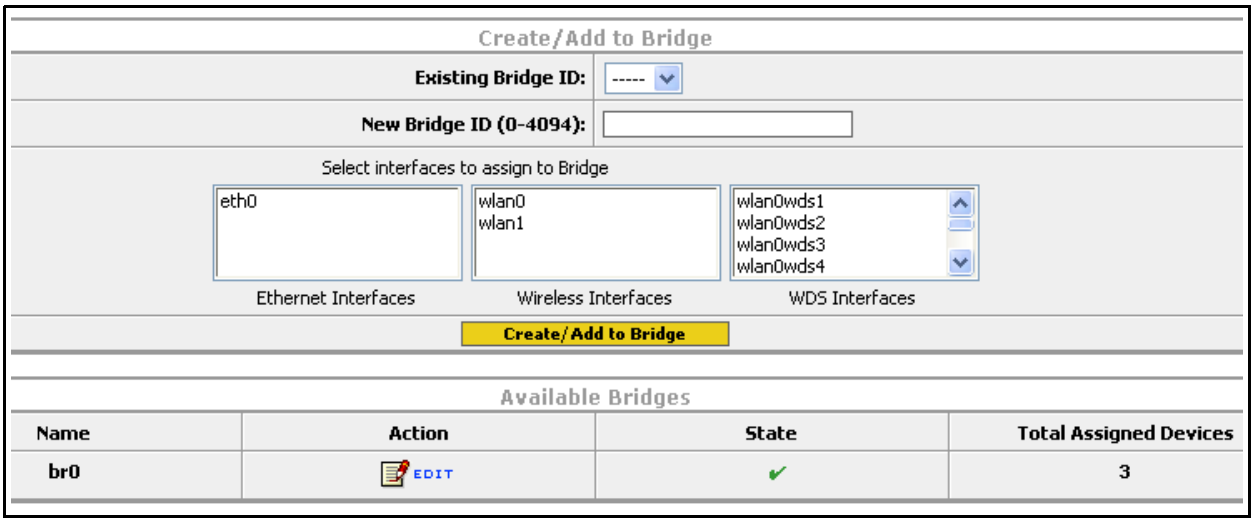
Network>Bridge

Bridges create pathways for data packets to travel freely between two or more interfaces within the Wi-Fi AP/Bridge. Bridges use both physical interfaces (such as the wireless interfaces) and logical interfaces (such as a WDS connection). An interface can only be a part of one bridge at a time.

A default bridge, called "br0", is configured to provide communications between the wired Ethernet interface (eth0) and the wireless interfaces (wlan0-wlan1). The default IP address of the Wi-Fi AP/Bridge is applied to this bridge for immediate access to these interfaces.

Create/Add to Bridge

The following menu is used to add an interface to an existing bridge and to create a new bridge.

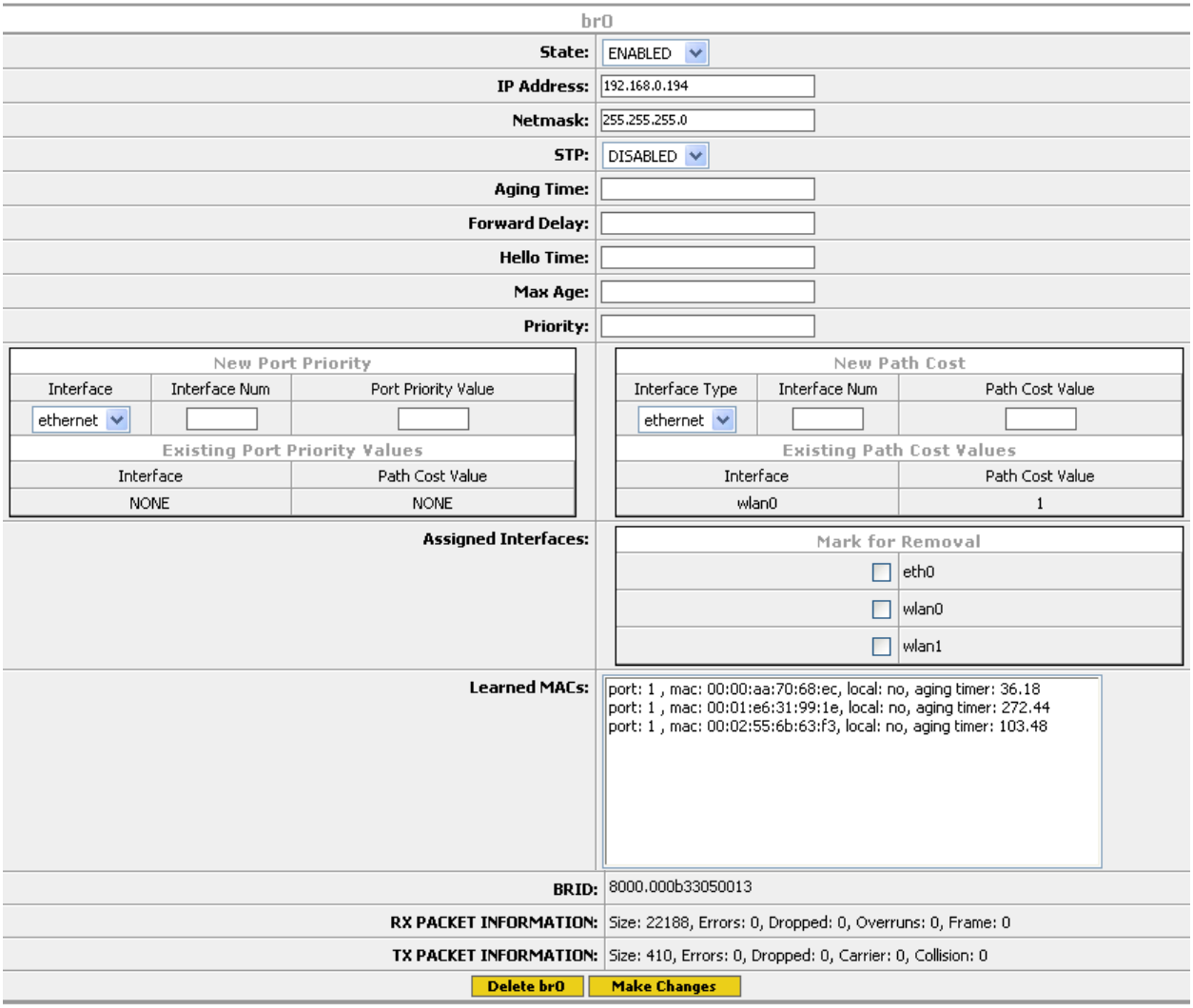


- **Existing Bridge ID**: Selecting an existing bridge to add one or more interfaces.
- **New Bridge ID (0-4094)**: Enter a number to identify a new bridge.
- **Select interfaces to assign to Bridge**: Click on an interface to highlight it and add it to the new or existing bridge. Multiple interfaces can be selected or de-selected by holding the Ctrl key down while selecting the interfaces.
- **Create/Add to Bridge:** Select this control to put bridge menu changes into effect.

 Copyright © 2004, Vivato, Inc.

Available Bridges

This area of the bridge menu is used to indicate existing bridges, and to review and edit a bridge's configuration. Clicking on EDIT causes a screen to be displayed that shows the configuration for that bridge.



- **State**: Enable or disable this bridge.
- **IP Address**: Enter an IP address for the bridge.
- **Netmask**: Enter a subnet mask for the bridge (if an IP address was specified).
- **STP**: Select "ENABLED" to use spanning tree protocol (STP) on this bridge. Bridges use spanning tree protocol to determine the best way to route packets using a number of parameters. The following settings are used when STP is enabled, and are saved in memory even if spanning tree protocol is disabled:

◊ **Aging Time**: Enter the number of seconds that network addresses of devices using the bridge are stored in the bridge table after receiving a packet. The range is 10-1000000 seconds. The default value is 300 seconds.

◊ **Forward Delay**: The forward time specifies how much time a bridge spends in the listening and learning states before forwarding a packet. This is used to prevent a bridge from starting to forward data packets over a link until the bridged network has been informed of the topology change and the affected links have been turned on or off. If you set this value too low, loops can exist until the spanning tree algorithm protocol re-configures the topology. Setting the value too high can cause delays until the spanning tree protocol re-configures the topology. The range is 4-200 seconds. The default setting is 15 seconds.

◊ **Hello Time**: The hello time is the period between the configuration messages generated by a root bridge. If you believe that configuration messages may be getting lost, shorten the hello time. To reduce the amount of overhead messages, increase the hello time. The range is 1-10 seconds. The default setting is 2 seconds.

◊ **Max Age**: The maximum age is used to determine when the bridge's stored configuration information is out of date and is removed. Setting the value too small causes the spanning tree protocol to reconfigure the bridge topology too often, which can cause a momentary loss of connectivity to the network. Setting the value too large can slow down the network because it is taking longer than necessary to adjust to a new spanning tree configuration for the bridge. A conservative value assumes a delay variance of 2 seconds per hop. The range is 6-200 seconds. The default value is 20 seconds.

◊ **Priority**: The bridge priority is used to determine which bridge to use for the root bridge and which to use for the designated bridge. In general, a lower bridge priority number results in the bridge being selected as the root bridge or a designated bridge. The range is 0-65535.

- **New Port Priority**: Not supported in this firmware release.
- **New Path Cost**: Enter the path cost for a specific interface on this bridge. The spanning tree algorithm adds this value to the root cost in configuration messages that are received on this port, and is used to determine the path cost to the root through this interface. Larger path cost values can result in the LAN being accessed through this interface to be lower in the spanning tree topology. This can result in less through traffic through this port. You should assign a large path cost to a LAN that has a lower bandwidth or where you want to minimize LAN traffic. The range is 0-65535.
- **Assigned Interfaces**: This area lists the interfaces in the AP/Bridge that are part of this bridge. To remove an interface from this bridge, check the box next to that interface and select **Make Changes**.
- **Learned Macs**: This area lists the source MAC addresses of packets that have been passed through this bridge.

 Copyright © 2004, Vivato, Inc.

- **BRID**: The bridge ID number displays two values: the bridge's priority setting is the value to the left of the decimal point (default is 8000), the lowest MAC address in the AP/Bridge is to the right of the decimal point. The priority setting is used by spanning tree protocol to determine which bridge has priority when multiple AP/Bridges are used in a network. If the priority setting of all bridges is the same, the lowest MAC address is used to determine priority.
- **RX PACKET INFORMATION**: This area lists information about packets that have been received by this bridge.
- **TX PACKET INFORMATION**: This area lists information about packets that have been sent by this bridge.
- **Delete (bridge name)**: Delete the specified bridge.

Caution

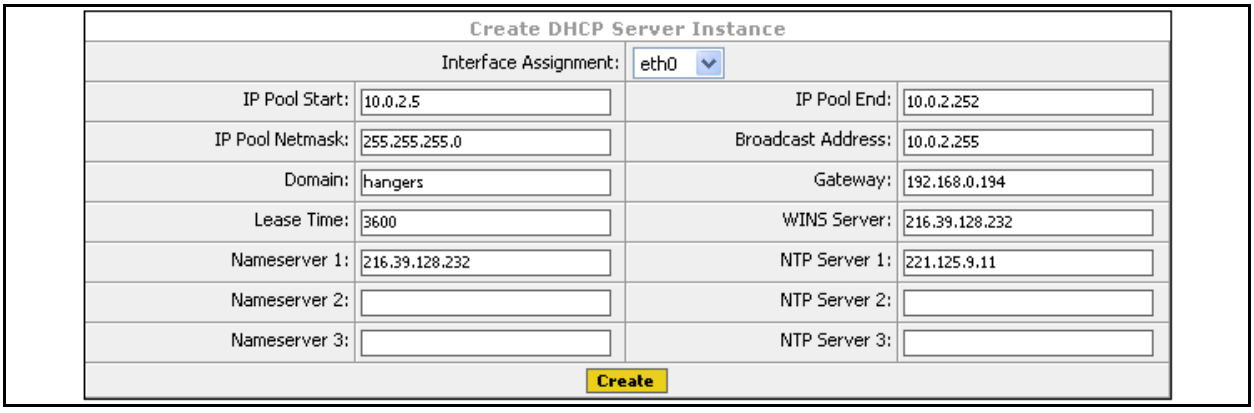
The IP address of the default bridge (br0) is used to access the AP/Bridge for initial configuration. If you delete this bridge before assigning an IP address to a different bridge, VLAN, or Ethernet interface, you will lose connection to the AP/Bridge when the bridge is deleted and you will not be able to re-access the configuration web pages. In this case, you have to configure the AP/Bridge using the command line interface (CLI) through the AP/Bridge's RS-232 serial port to assign an accessible IP address.

- **Make Changes**: Put your changes into effect.

Network>DHCP

The Wi-Fi AP/Bridge can assign IP addresses to other devices on the network using dynamic host control protocol (DHCP) server operation. This is typically used to assign IP addresses to wireless clients as they associate with the Wi-Fi AP/Bridge. See **"Dynamic Assignment of Client IP Addresses"** on page 153.

After being created, a DHCP server must be enabled before it can be used.



- **Interface Assignment**: Select the interface to use as the DHCP server.
- **IP Pool Start**: Enter the starting IP address in the range of address to assign to DHCP-enabled clients.

- **IP Pool Netmask**: Enter the subnet mask for the range of IP addresses specified in the IP Pool functions.
- **IP Pool End**: Enter the ending IP address in the range of address to assign to DHCP-enabled clients.
- **Lease Time**: Enter the number of seconds that an assigned IP address can be leased by a client before it must be renewed.
- **Nameserver 1, 2, 3**: Enter the IP addresses of up to three name servers to used with clients who get their IP addresses from this DHCP server.
- **Broadcast Address**: Enter the DHCP broadcast IP address. This is the address that is returned if a DHCP client requests the broadcast address from the DHCP server.
- **Gateway**: Enter the IP address of the interface used as the gateway for DHCP clients to connect to your wired network. This is often the IP address of the default bridge (br0).
- **Domain**: Enter a domain name to represent the range of IP addresses served by this DHCP server.
- **WINS Server**: Enter the IP address of a Windows internet naming service (WINS) server.
- **NTP Server 1, 2, 3**: Enter the IP address of a network time protocol (NTP) server. Up to three time servers can be specified.
- **Create**: Create the new DHCP server. The settings that you entered are then displayed in their own table (see below), and can be edited by entering the new values and selecting **Make Changes**.
  - ◊ **State**: Select **ENABLED** to start using the DHCP server, or select **DISABLED** to stop using this DHCP server. **Make Changes** must be selected before the new setting is used.
  - ◊ **Delete**: Deletes this DHCP server.

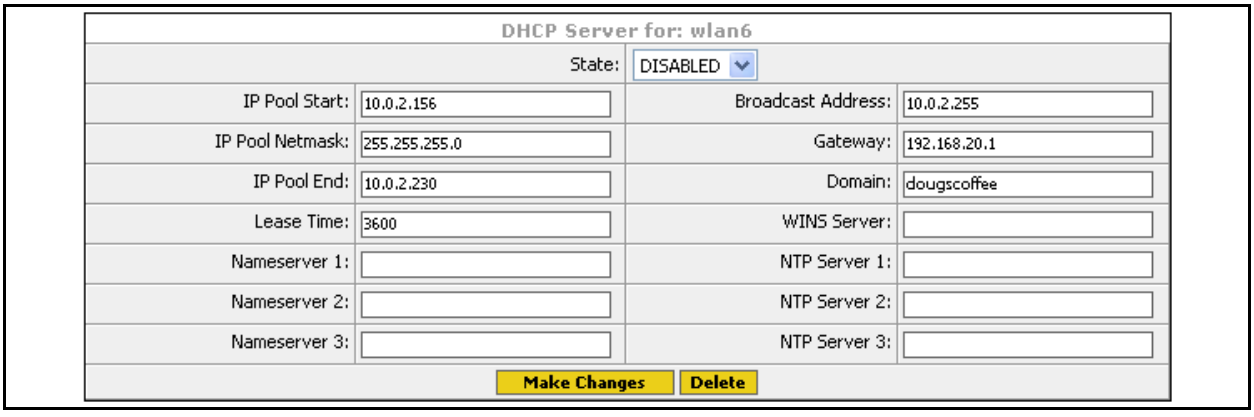


Figure 10—Editing or Deleting a Configured DHCP Server

 Copyright © 2004, Vivato, Inc.

Network>Ethernet Interface

The following settings can be configured for the wired Ethernet interface:

- **State**: Select ENABLED or DISABLED to use or disable this interface.
- **IP Address**: If needed, enter an IP address for this interface. Remember, if this interface is part of the default bridge (br0), the IP of bridge 0 should be used as the IP of the AP/Bridge to access it from another device; so this field would be left set to “none”.
- **Netmask**: Enter the subnet mask for this interface.
- **Secondary IP Address**: Enter a secondary IP address for this interface.
- **Secondary Netmask**: Enter the subnet mask for the secondary IP address.
- **RX/TX PACKET INFORMATION**: Refer to **"show interfaces wireless <0-1>"** on page 109.

After editing settings, select **Edit** to put the changes into effect.

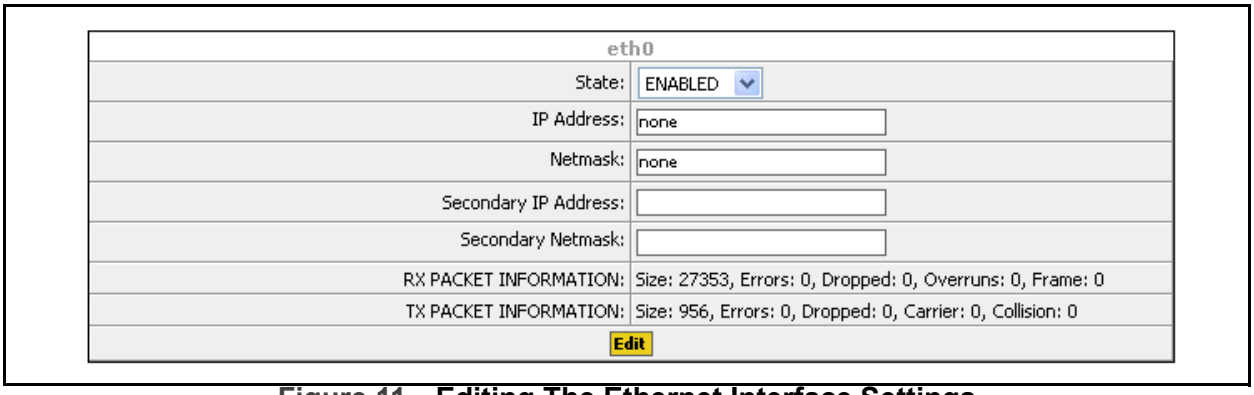
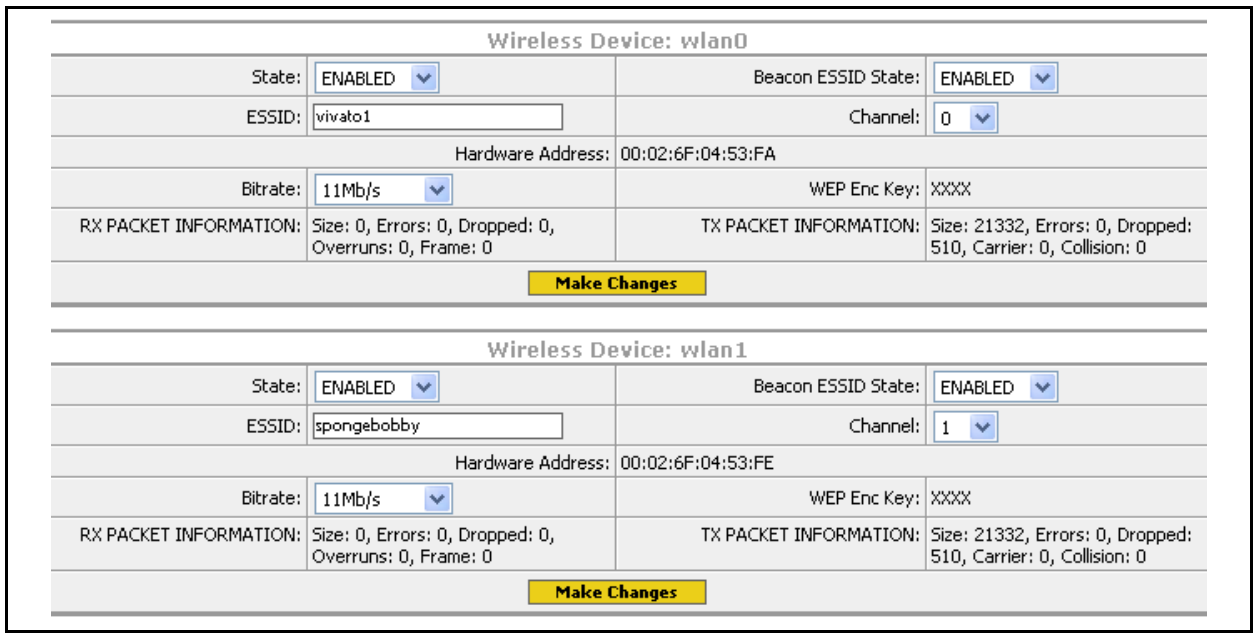


Figure 11—Editing The Ethernet Interface Settings

Network>Wireless Interfaces

The Wi-Fi AP/Bridge contains two wireless interfaces (wlan0 and wlan1) that can be individually configured.



Configuring Wireless Interfaces Individually

From the **Network>Wireless Interfaces** screen, you can edit the wireless port's settings and view statistics for that interface.

Each wireless interface table displays the hardware (MAC) address of that interface and some transmit and receive statistics (see **"show interfaces wireless <0-1>"** on page 109 for information on TX and RX statistics), and indicates if WEP is being used on that interface (shown as WEP Enc Key: XXXX). The following settings can be changed as needed:

- **State**: Select **ENABLED** to use this interface, or **DISABLED** to disable this interface.
- **ESSID**: Enter the name that clients will see from this interface when searching for wireless networks.
- **Bitrate**: Select the bit rate in megabits per second (Mbps) to use for all wireless communications through this interface, or set to 'auto' for automatic rate setting (the default). In standard 802.11b operation, the wireless interface automatically adjusts the bitrate according to the quality of the link with the wireless clients. There may be situations where you want to constrain the bit rate to a specific value, such as during a site survey or when collecting data on client performance. However, for typical Wi-Fi operation you should use the 'auto' setting.

 Copyright © 2004, Vivato, Inc.

- **Beacon ESSID State**: When set to **DISABLED**, the ESSID is not sent in beacons issued by this wireless interface. Since the ESSID is no longer sent, clients cannot display it in their list of available networks and automatically send it in a response to try to associate. Therefore, only clients that have had the ESSID manually entered into their preferred wireless network list can associate with the Wi-Fi AP/Bridge. The default state is to send the ESSID in beacons (**ENABLED**) until this command is sent.
- **Channel**: Select the channel to use for this wireless interface. You should use channels 1 and 11(the default) whenever possible.
- **Make Changes**: Start using the new settings for this interface.

Configuring the Wireless Interfaces As a Group

You can configure the wireless interfaces as a group from the **Network>Summary** screen by selecting "**Edit Wireless Group Settings**" at the bottom of the table of wireless interfaces (shown in the following figure).

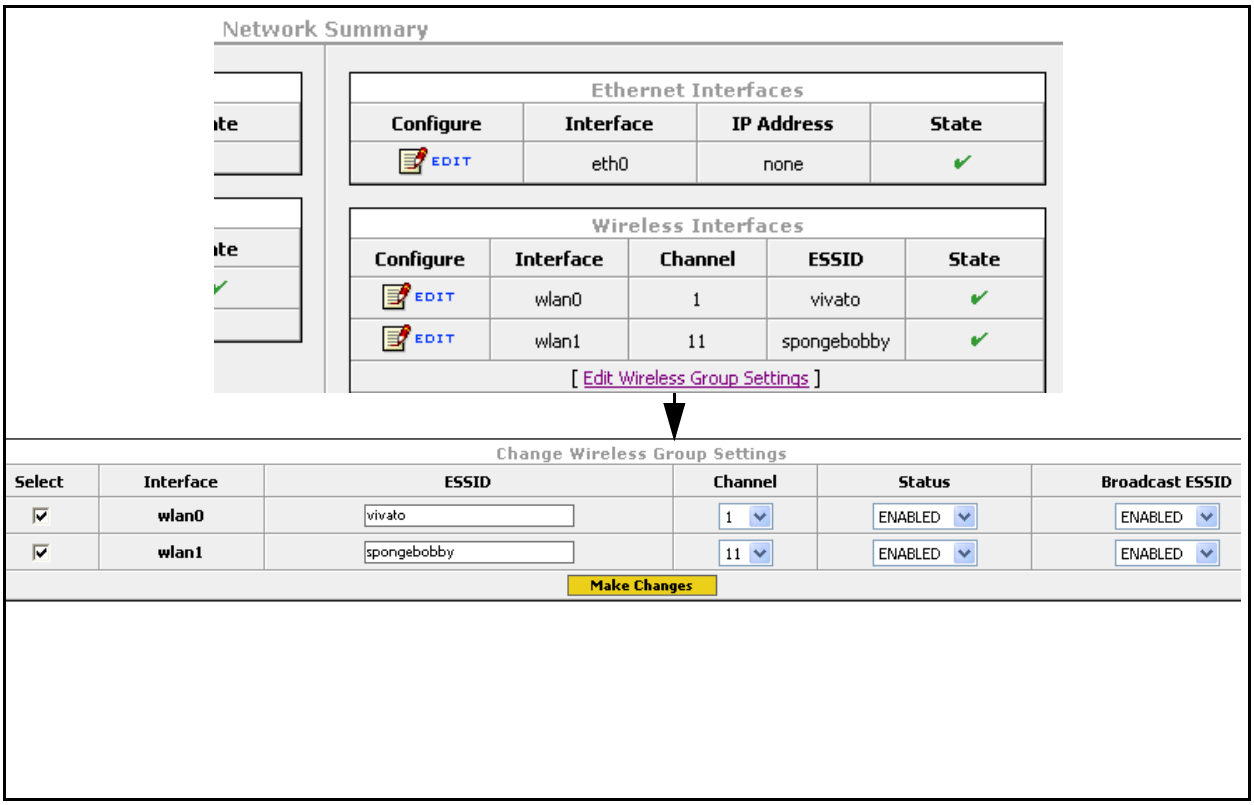


Figure 12—Editing Wireless Interface Settings As a Group

Configuring the Wireless Interfaces as a Group

Use these steps to configure several wireless interfaces at one time:

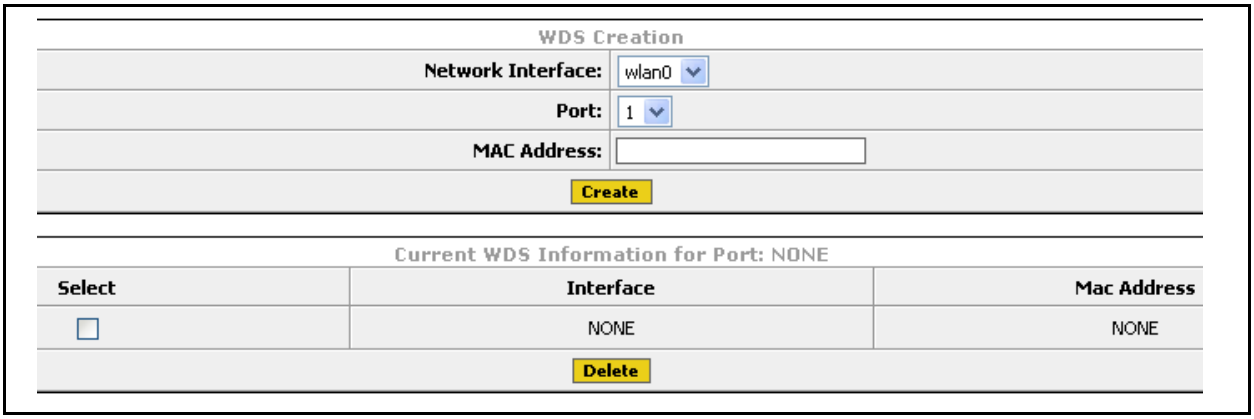
1. Enter the changes for the **ESSID**, **Channel**, **Status**, **Broadcast ESSID** for each interface. See **Configuring Wireless Interfaces Individually** for descriptions of each setting.
2. Click on the **Select** box for the interface(s) to configure using these changes.
3. Select **Make Changes**.

Network>WDS

Wireless distribution system (WDS) allows the AP/Bridge to connect to a Vivato Wi-Fi Base Station through a wireless interface from each device. The WDS connection is used instead of a wired LAN connection when deploying the AP/Bridge as a coverage filler, range extender, or to provide a wireless backhaul to a Wi-Fi Base Station. See **"Network Configuration Examples"** on page 26.

Important	After creating a WDS connection, be sure to add that connection to the bridge that connects to the wireless interface used for the WDS connection. For example, if you are using the default bridge (bridge 0) to connect the wireless interfaces to the Ethernet interface, add the WDS connection that you create here to bridge 0. See **"Create/Add to Bridge"** on page 60.

For more information on WDS operation, see **"Configure WDS (Wireless Distribution System)"** on page 139.



WDS Creation

A WDS connection must be created on the AP/Bridge and on the Wi-Fi Base Station to create the wireless link between them. The following settings must be configured on BOTH devices:

- **Network Interface**: Select the wireless interface to use for the WDS connection.
- **Port**: Up to 6 connections can be used on a wireless interface. Select a value, or use the default.
- **MAC Address**: Enter the MAC address of WDS-enabled wireless interface on a Wi-Fi Base Station (the “peer” address).

 Copyright © 2004, Vivato, Inc.

Current WDS Information

This area lists the WDS connections that have been configured on the AP/Bridge and the MAC address (peer address) of the wireless interface of the device on the other end of the connection. To remove a connection, check its "**Select**" box and click on **Delete**.

 Copyright © 2004, Vivato, Inc.

Security Configuration Web Pages

The **Security** tab accesses screens for configuring the various security features in the Wi-Fi AP/Bridge.

Security settings determine who is allowed network access through the Vivato Wi-Fi AP/Bridge. Security is initially turned off in the Wi-Fi AP/Bridge to allow access for configuration. Security should be configured when you access the configuration web pages for the first time and select the security method in the Quick Setup screens. For more information on configuring Microsoft® Windows XP® and Windows 2000® clients and a Windows 2000 Internet Access Server (Win2K IAS) for EAP or PEAP security, see ***Windows XP Win2kIAS Deployment.pdf*** on the Vivato 2.4 GHz Wi-Fi AP/Bridge CD-ROM.

Information on 802.1x security with Microsoft Windows XP® or Windows 2000® is also available at the following website:

http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/default.asp

Security Settings

Security settings are arranged on the following configuration pages:

- **Security>WEP** - Wired Equivalent Privacy
- **Security>802.1x** - Extensible Application Protocol (EAP/PEAP)

Security>Summary

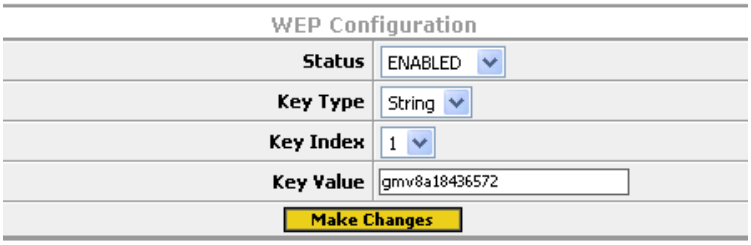
The Security Summary table lists the types of security that are available and if they are enabled or disabled at this time. Clicking on the type of security accesses its settings.

Important	WEP is used by 802.1x, and is automatically enabled when 802.1x is enabled. Therefore, do not attempt to disable WEP after enabling 802.1x. If you were previously using WEP, but are now changing to using 802.1x, disable your WEP configuration *before* configuring and enabling 802.1x. 802.1x security is not configurable from the VivatoVision web interface with this firmware release, but can be configured using the command line interface.

Security>WEP

Wired equivalent privacy (WEP) is a method of data encryption for wireless networks, originally developed to provide approximately the same level of security provided by wired networks. Data encryption keys are shared between the Wi-Fi AP/Bridge and the wireless clients to try to provide

a secure link between them. See **"Optimizing Your Wireless Client For Secure Communications"** on page 73 for information on configuring your 802.11b client to use WEP.



WEP has been shown to be somewhat susceptible to wireless interception and fraud by those skilled at breaking into networks. Where needed, use 802.1x to provide greater levels of security. See **"Security>802.1x"** on page 72.

WEP configuration includes the following settings:

- **Status**: Select ENABLED or DISABLED to turn WEP on or off, respectively.
- **Key Type**: Select the character type for the WEP key: String (ASCII) or HEX.
- **Key Index**: Up to four WEP keys can be configured. The key index represents which key value you are using. The key indexes and the key values for clients must match those of the Wi-Fi AP/Bridge. In most client's configuration settings, the WEP key index ranges from 1 to 4; just like the Wi-Fi AP/Bridge. However, some clients use indexes from 0 to 3 instead. In this case, use the key index of the same relative order when configuring your client. For example; if the Wi-Fi AP/Bridge is set to use a key index of 1, set your client to use a key index of 0, and so on.
- **Key Value**: Enter the WEP key value. Valid entries are 5 or 13 String (ASCII) characters or 10 or 26 hex digits.
- **Make Changes**: Change the Wi-Fi AP/Bridge's configuration to use the specified key value on the specified interface.

Security>802.1x

802.1x security is not configurable from the VivatoVision web interface using the new (vino.br.1.1) firmware release, but can be configured using the command line interface.

Extensible Authentication Protocol is used with a remote authentication dial-in user service (RADIUS) to provide IEEE 802.1x security. In this configuration, the identity of the client and the intended server are verified before data can be exchanged. It is available for clients running on most Microsoft® Windows platforms, such as Windows 2000 Service Pack 3 and Windows XP Service Pack 1 (visit Microsoft's website for 802.1x upgrades for your operating system).

For information on configuring the Windows 2000 Internet Access Server to work with the Vivato Wi-Fi AP/Bridge's 802.1x configuration, see **"EAP Commands (802.1x security)"** on page 128.

See **"Optimizing Your Wireless Client For Secure Communications"** on page 73 for information on configuring your 802.11b client to use 802.1x.

 Copyright © 2004, Vivato, Inc.

Important Considerations When Using 802.1x

The following conditions must be considered when configuring 802.1x in the Wi-Fi AP/Bridge, clients, and the services supporting 802.1x.

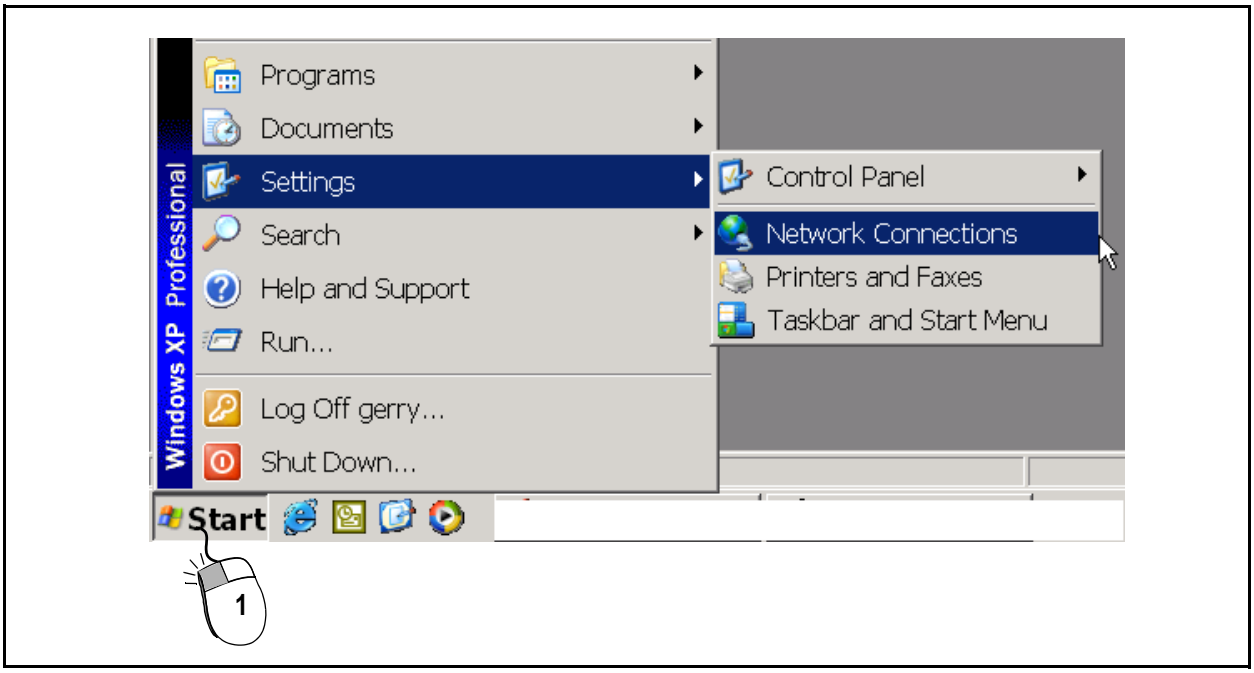
- If a Win2K Internet Authentication Server (IAS) is used with the Vivato Wi-Fi AP/Bridge for 802.1x operation, set the 802.1x policies in the IAS to use either "Strongest" (128-bit) or "Basic" (64-bit) encryption. The "Strong" and "No Encryption" settings are not supported at this time.
- When configuring Windows XP, Windows XP+SP1 or Win2000+SP3 client for 802.1x, *do not* select "Authenticate as computer when computer information is available." or "Authenticate as guest when user or computer information is unavailable". If these options are selected, a wireless interface on the Wi-Fi AP/Bridge may be left open when the user logs off. This presents the potential for unauthorized access to the Wi-Fi AP/Bridge.

Optimizing Your Wireless Client For Secure Communications

The following client configuration information is provided as a reference for setting up WEP. Some operating systems do not support all types of security. Refer to your client's documentation for configuring it to match the recommended settings provided below.

The examples below use the Microsoft Windows XP® Network Connections feature to access and change the client configuration. *The client interface must be enabled to be able to access the client's security settings. If the AP/Bridge's wireless interface is not enabled, its ESSID cannot be seen by the wireless client card, but the ESSID can still be configured manually.*

Step 1. Select **Start > Settings > Network Connections**.



Step 2. Right-click on **Wireless Network Connection**.

Step 3. Left-click on **Properties**.

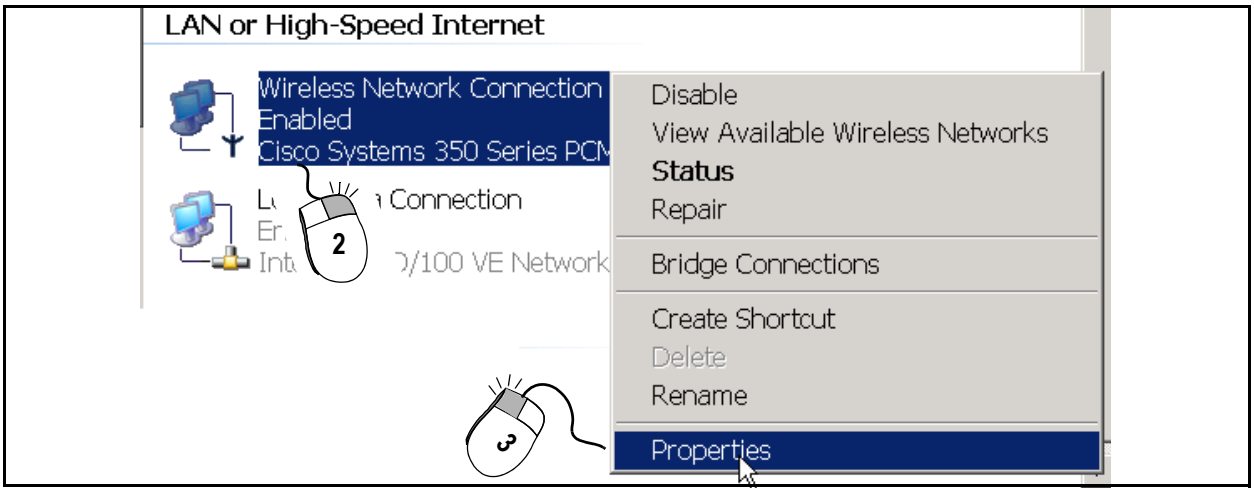


Figure 13—Accessing the Wireless Network Connections Configuration

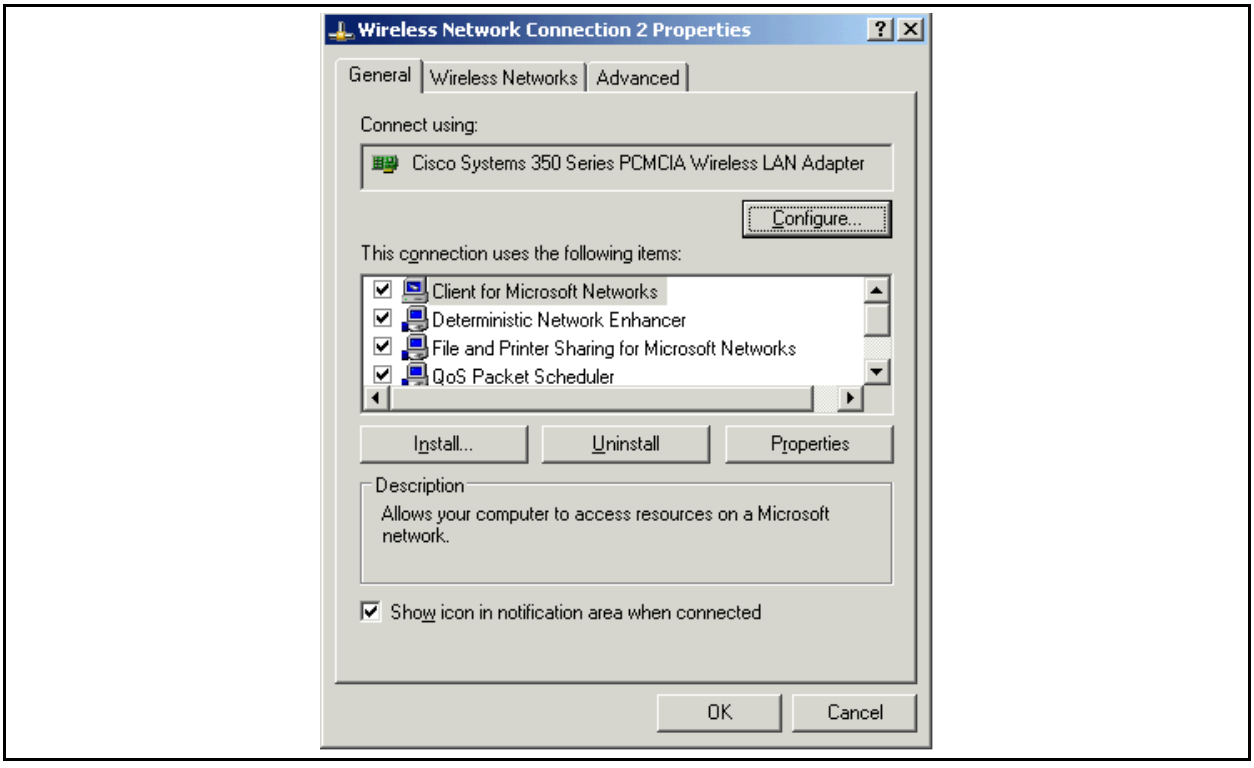


Figure 14—Windows XP Wireless Network Connections Screen (With the Client Enabled)

 Copyright © 2004, Vivato, Inc.

Configuring WEP in Your Client

See **"Security>WEP"** on page 71 for a description of WEP.

With the *client enabled* and close enough to the Wi-Fi AP/Bridge to receive its wireless signal, use the following steps to configure WEP after accessing the Wireless Network Connection Properties (described in the previous section). *If the AP/Bridge is not close enough to the client to receive its signals, or the AP/Bridge is turned off, you can manually enter its ESSID in the "Network name (SSID):" field.*

Step 1. Click on the Wireless Networks tab in the Wireless Network Connection window and select the Vivato entry (see **Figure 15— Configuring WEP in Your Client on page 75**). If the ESSID for the Wi-Fi AP/Bridge's wireless interfaces has been changed, use that entry instead.

If you are not receiving the Wi-Fi AP/Bridge's signal (no ESSID is shown), verify that a wireless interface has been enabled on the Wi-Fi AP/Bridge. See **"Network>Wireless Interfaces"** on page 66.

Step 2. Click Configure to display the WEP settings.

Step 3. Check the box next to "Data encryption (WEP enabled)".

Step 4. Un-check the box for automatic WEP key assignment and enter the WEP key(s). WEP keys are automatically assigned only when using 802.1x security.

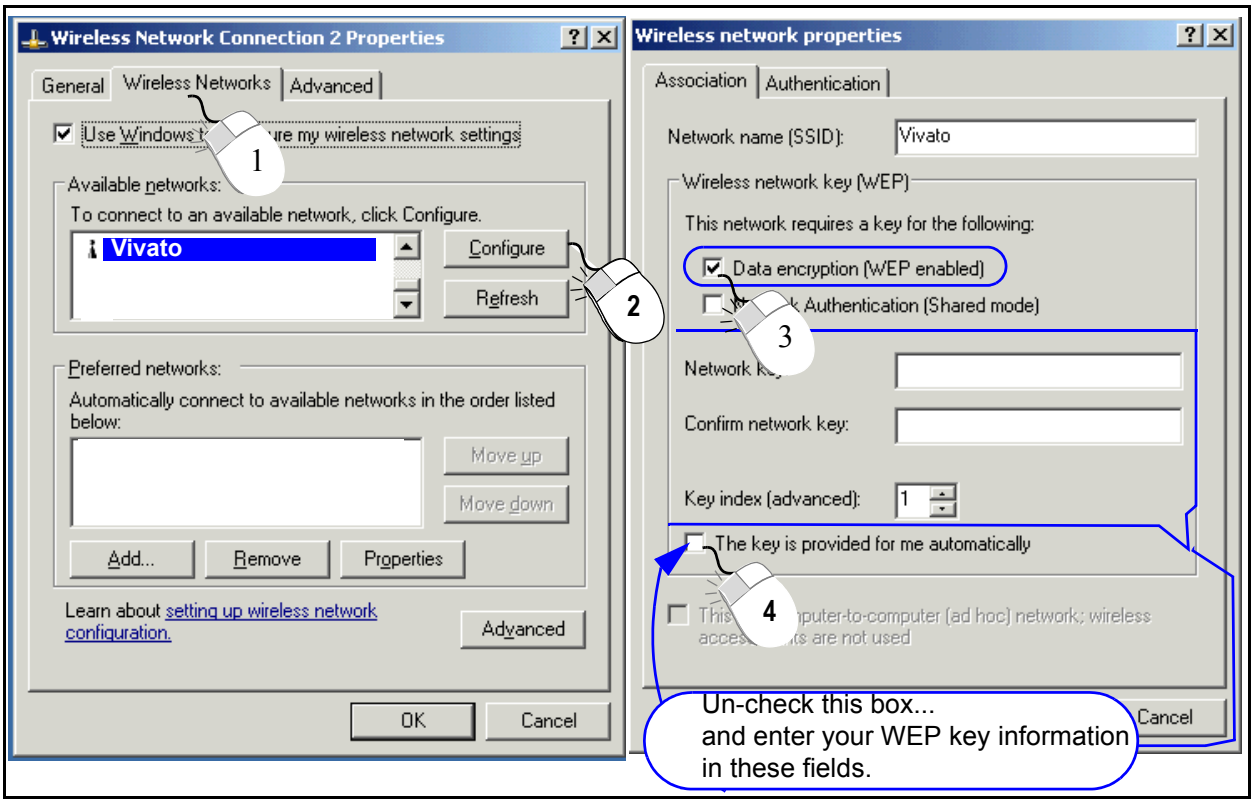


Figure 15—Configuring WEP in Your Client

Configuring 802.1x in Your Client

802.1x security should be enabled whenever a RADIUS server is used. Windows 2000 clients can use 802.1x/PEAP by downloading the free "Microsoft 802.1X Authentication Client" download.

Use the following steps as a guideline to enable 802.1x. Your setup may be slightly different, depending on the version of Windows you are running:

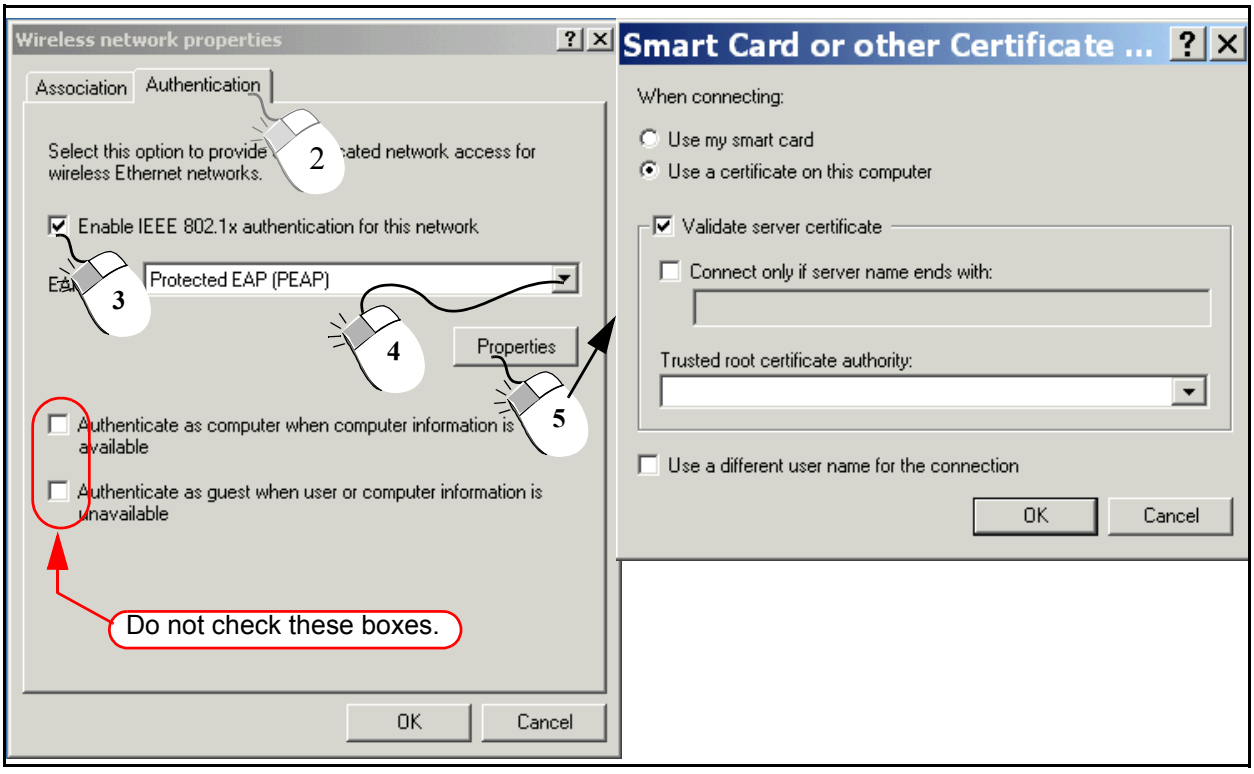
Step 1. Enable WEP, and check the box labeled "The key is provided for me automatically". See **Configuring WEP in Your Client**. WEP is used with 802.1x, but the key is provided automatically during the authentication process.

Step 2. Click on the Authentication tab in the Wireless Network Properties window (the window displayed while configuring WEP).

Step 3. Check the box next to "Enable network access control using IEEE 802.1X"

Step 4. Select "EAP type" and select either "Protected EAP (PEAP)" or "Smart card or other certificate".

Step 5. Select Properties to specify the method of obtaining authentication certificates that your network uses. If "EAP type" is set to "Smart card or other certificate", you must install the user certificate, computer certificate, and RADIUS server certificate on the client PC. If "Protected EAP (PEAP)" is selected, you only need to install the RADIUS server certificate.



 Copyright © 2004, Vivato, Inc.

Caution	When configuring Windows XP, Windows XP+SP1 or Win2000+SP3 client for 802.1x, *do not* select “Authenticate as computer when computer information is available.” or “Authenticate as guest when user or computer information is unavailable”. If these options are selected, a wireless interface on the Wi-Fi AP/Bridge may be left open when the user logs off. This presents the potential for unauthorized access to the Wi-Fi AP/Bridge.

 Copyright © 2004, Vivato, Inc.