Vivato Wi-Fi Bridge/Router User Guide

Manual Part Number: 730-01362-02
Printed in U.S.A.

Copyright © 2003, Vivato, Inc.

Who Should Read This Book?

The Vivato Bridge/Router and Wi-Fi Switch System introduce 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 Bridge/Router.

Printing This Book

To print this book from the User Guide.PDF file on the Bridge/Router CD-ROM, 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. 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.**

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 Bridge/Router 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 Bridge/Router 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 Bridge/Router. Do not attempt to use a substitute power supply or modify this power supply.

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. Changes or modifications not expressly approved by Vivato could void the user's authority to operate the equipment. Refer any service or repair to authorized Vivato personnel or its certified agent.

FCC Declaration of Conformity

Responsible Party
Manufactured by Vivato, Inc.
139 Townsend Street, Suite 200
San Francisco, CA 94107, USA
Phone: (415) 495-1111, Fax (425) 495-6430

Product: Vivato, Inc. Wi-Fi Bridge/Router
This product is intended for home or office use.

The Vivato Wi-Fi Bridge/Router has been evaluated under FCC Bulletin OET 65C and found to be compliant to the requirements set forth in CFR 47 15.247 (b) (4) addressing RF Exposure from radio

frequency devices. The Wi-Fi Bridge/Router must be at least 20 cm (7.8 in.) from people when operating.

Interference and Equipment Limits
This equipment has been tested and found to comply with the limits pursuant to Part 15 of the FCC Rules. As such, operation of this equipment may not cause harmful interference and this equipment must accept any interference received including interference that may cause undesired performance.

This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. Contact Vivato personnel if interference is detected.

Note: Warning - This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the listed equipment. Vivato, Inc. is not responsible for any interference caused by unauthorized modification or configuration programming of this device or by the substitution or attachment of antennas or equipment other than that specified by Vivato, Inc. Violations of these conditions will void the user's authority to operate this device. This device must not be co-located with other transmitters and antennas.

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

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

Conventions Used in This Document

The following conventions are used in this document:

Table 1 — Document Conventions

Convention Format	What it Indicates
computer entry	Text that you enter on the Bridge/Router'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 Bridge/Router 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 Bridge/Router 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:

E-mail: support@vivato.net (use “manuals_feedback@vivato.net” for documentation feedback)

Mail:

Vivato, Inc.

139 Townsend St., Suite 200

San Francisco, CA 94107

To provide feedback on our documentation:

Feedback on the documentation shipped with the Vivato Wi-Fi Bridge/Router 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 support@vivato.net address for product support issues.)

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Introduction

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

The Wi-Fi Bridge/Router 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 Bridge/Router to provide high bit rate network coverage to larger spaces requiring Wi-Fi coverage.

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

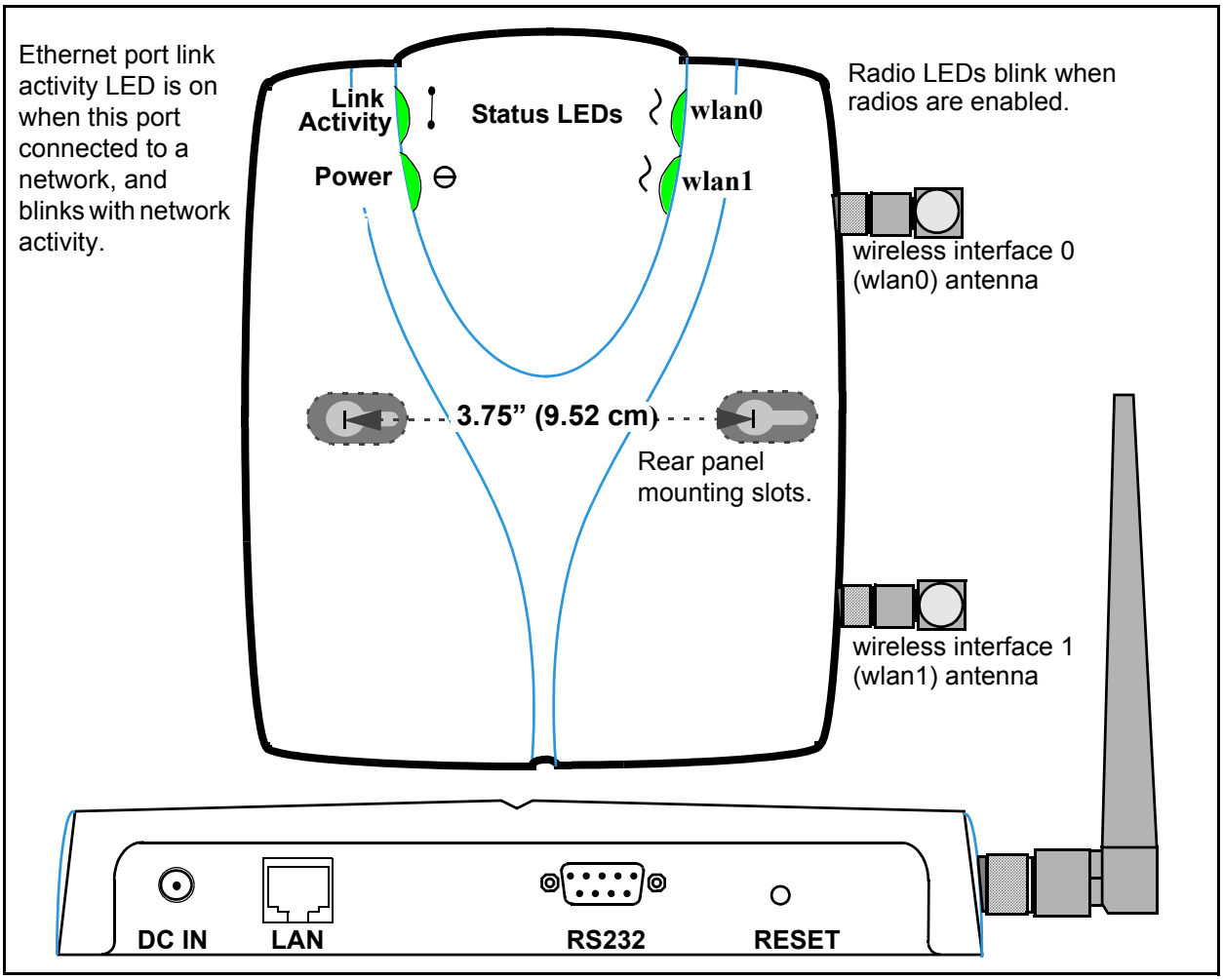


Figure 1—Connectors and Indicators

Omni-directional Antennas

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

Ethernet and Serial Ports

The **LAN** (Ethernet) port accepts an RJ-45 connector, linking the Bridge/Router to a 10/100 Ethernet LAN. The **RS232** (serial) port provides console access to the management system in the Bridge/Router 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 Bridge/Router to use the factory default settings, and deletes the previous configuration file.

Metal Enclosure

The Bridge/Router 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 Bridge/Router 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 Bridge/Router can be configured to communicate with clients and with a Vivato Wi-Fi Switch (using a Wireless Distribution System (WDS) connection) .

Multi-Bridge/Router Operation for Extended Coverage

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

Basic Service Set Operation

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

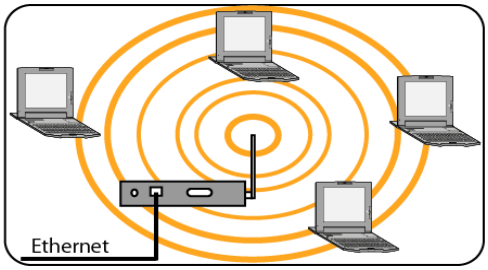
Web Page or Command Line Interface Configuration

The Vivato Vision© web interface Quick Setup pages are used for the initial configuration to get the Bridge/Router 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.

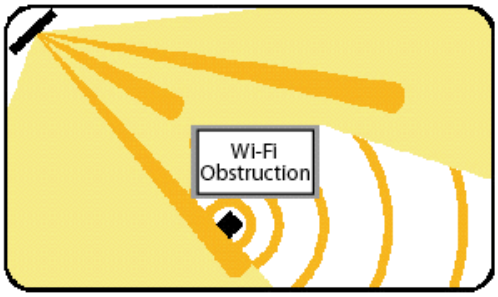
Network Configuration Examples

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

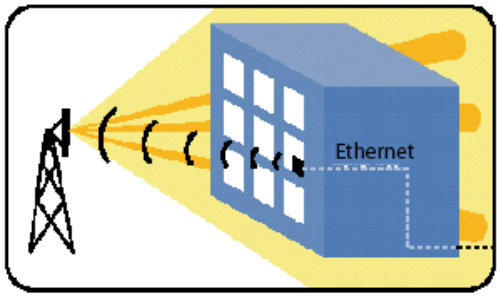
- **Access Point** (AP). As an access point (AP) connected directly to a wired LAN, the Bridge/Router provides a connection point for wireless users and, if more than one AP is connected, users can roam from one area to another without losing their connection to the network. See **"Access Point Location"** on page 8.

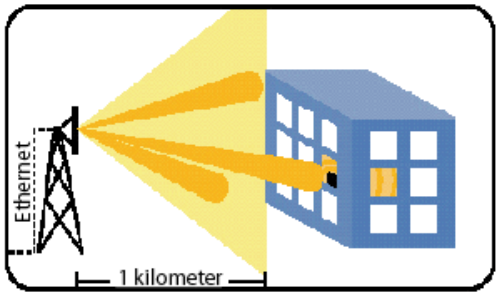


- **Coverage Filler** for a Vivato 2.4 GHz Wi-Fi Switch using WDS. With radio frequency (RF) systems, there can be coverage gaps or voids due to physical barriers or radio interference. Combining the 2.4 GHz Indoor Wi-Fi Switch with the Vivato Wi-Fi Bridge/Router can provide effective coverage in an area with poor quality or inadequate coverage. By placing the Wi-Fi Bridge/Router within the line of sight of the Vivato Switch, the Vivato Wi-Fi Bridge/Router can propagate Wi-Fi to areas with weak or blocked coverage. See **"Hole Filler Location Example"** on page 9.



- **Wireless Backhaul** to a Wi-Fi Switch. With a Vivato 2.4 GHz Outdoor Wi-FI Switch, 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 Bridge/Router can connect to Ethernet inside a building to provide wireless backhaul for the outdoor switch using one Wi-Fi channel, leaving another channel free for client connections through the outdoor switch. See **"Wireless Backhaul Example"** on page 9.





•**Repeater** to provide range extension. The Wi-Fi Bridge/Router can extend the range of a switch when acting as a repeater, either in conjunction with a Vivato Wi-Fi Switch or with other Vivato Bridge/Routers. One radio is used to establish a long-range connection with the Wi-Fi Switch or Bridge/Router, 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 10.

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 122F (0 to 50C)
- 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 Bridge/Router 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).
- Two antennas
- DB-9 null modem cable
- RJ-45 Crossover Ethernet cable
- Power supply
- Bridge/Router stand - allows the Bridge/Router to be positioned on its side when desired.
- Vivato Wi-Fi Bridge/Router

Installation

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

Step 1. Verify the contents of the shipping container (see **"Shipping Contents"** on page 5).

Step 2. Register your Vivato Bridge/Router. 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.**

Important	
	Registering your Wi-Fi Bridge/Router automatically generates a user name and password to access the Customer Support area of the Vivato website. This website contains the most up to date firmware and release notes for your Bridge/Router, along with other helpful information. Be sure to register your Wi-Fi Switch immediately to benefit from this valuable service!

Step 3. Analyze your site to estimate the best place to deploy the Bridge/Router. See **"Where to Position The Bridge/Router"** on page 7.

Step 4. Attach the two antennas.

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

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

Step 7. Verify Bridge/Router operation using a Wi-Fi client. See **"Verifying Wi-Fi Operation"** on page 117.

Where to Position The Bridge/Router

Where you position the Bridge/Router depends on your intended application and the physical surroundings. The applications are described in **"Network Configuration Examples"** on page 3.

The following conditions must be considered regardless of your application:

- Availability of mains (AC) power and LAN connections.
- Wall construction materials and other 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 4).

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 Bridge/Router’s antennas can be adjusted 90 degrees to allow transmission and reception of signals that are vertically or horizontally polarized. The Vivato Wi-Fi Switch’s antenna is

horizontally polarized, however this orientation can be affected somewhat by its signals being reflected off of hard services. Whenever you are using the Bridge/Router, especially with a Wi-Fi Switch, you should always adjust the antennas on the Bridge/Router to obtain the strongest signal level at the receiving device(s).

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 Bridge/Router's signal. Whenever possible, you should eliminate or minimize the use of these devices within the Bridge/Router's operating area in order to maximize Wi-Fi data rates.

The Vivato Wi-Fi Bridge/Router also uses the same frequencies as conventional access points (APs). All 802.11b devices must use carrier sense multiple access (CSMA) operation, where only one device can be transmitting an a time. This prevents interference from each other in a Wi-Fi area, but requires multiple devices on the same channel to take turns, reducing the overall available throughput for each device. When using the Bridge/Router with Vivato Wi-Fi Switch, use the Wi-Fi Switch's rogue access point detector (RAPD) to determine which channel has the least traffic and the least interference, and set the Wi-Fi Switch to use that channel. Refer to the *Urban Deployment* document on the Vivato CD-ROM 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 Bridge/Router to provide the greatest line of site access to the most clients. Whenever possible, mount the Bridge/Router in a central location that is above cubicle walls or other obstacles.

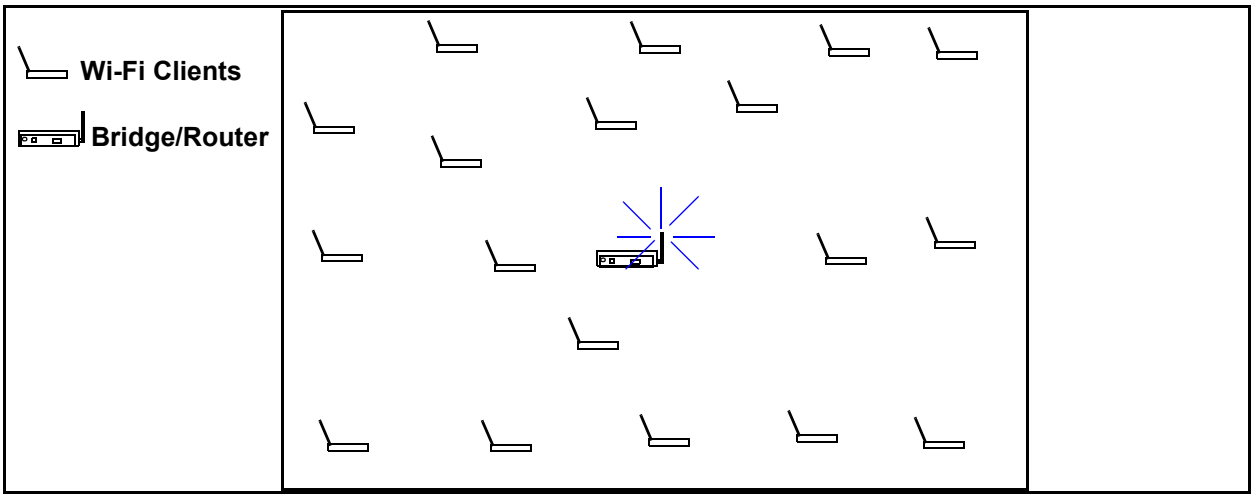


Figure 2—Access Point Location

Coverage Filler Positioning

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

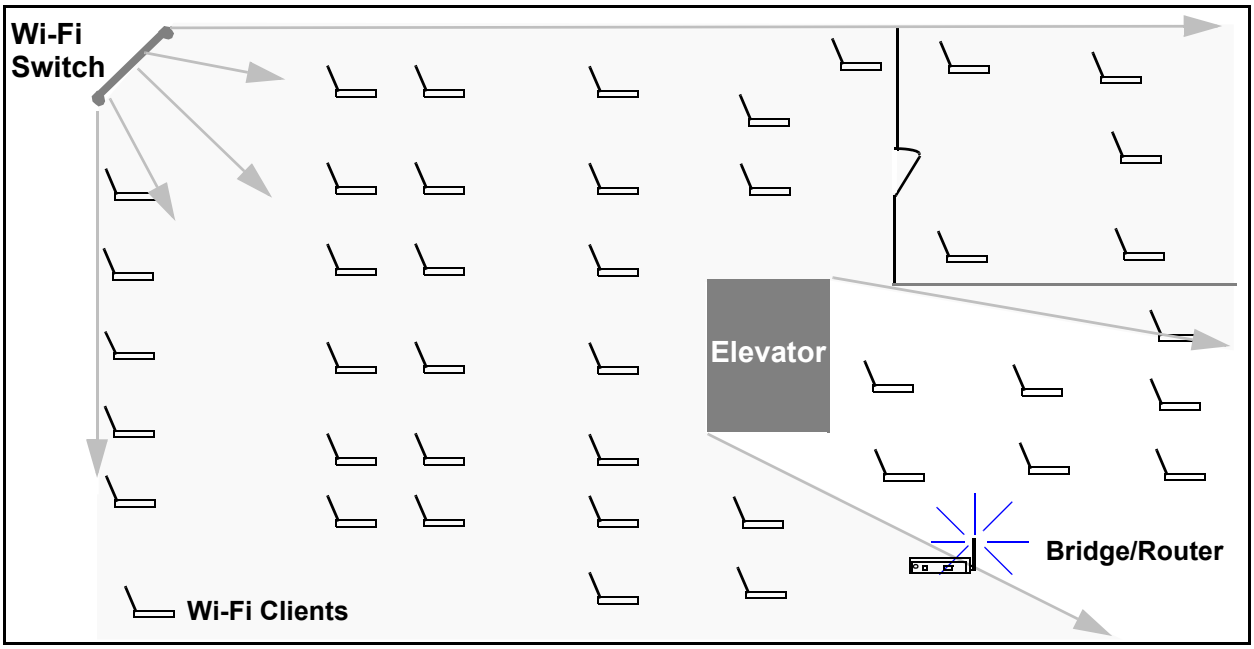


Figure 3—Hole Filler Location Example

Wireless Backhaul Positioning

When used to provide a wireless backhaul connection to a Vivato Wi-Fi Switch that only has a power connection, position the Bridge/Router as close as possible to the Wi-Fi Switch (clear line-of-sight path when possible). When used with an outdoor Wi-Fi Switch, this is often achieved by putting the Bridge/Router next to a window with a clear view of the Switch.

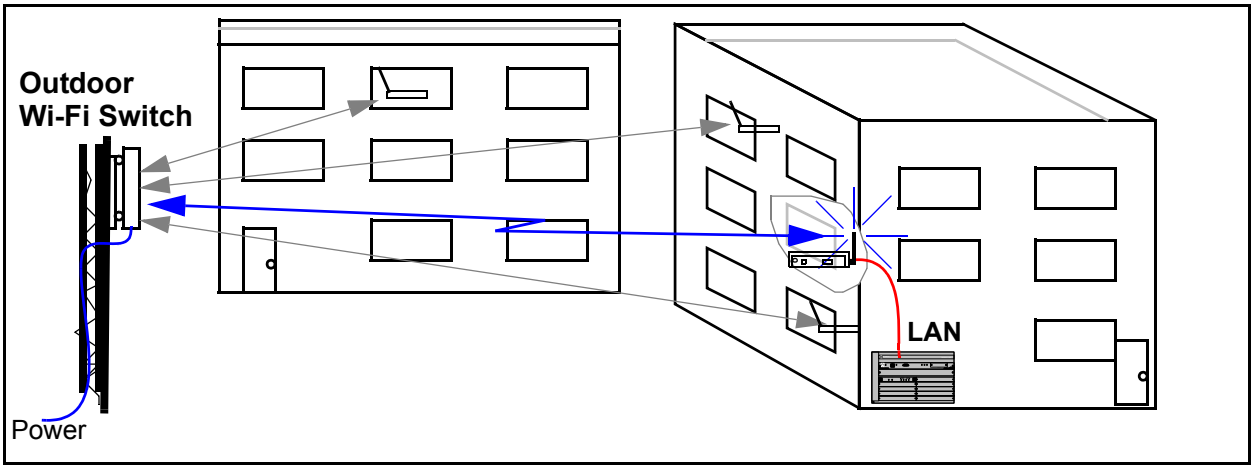


Figure 4—Wireless Backhaul Example

Range Extension Positioning

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

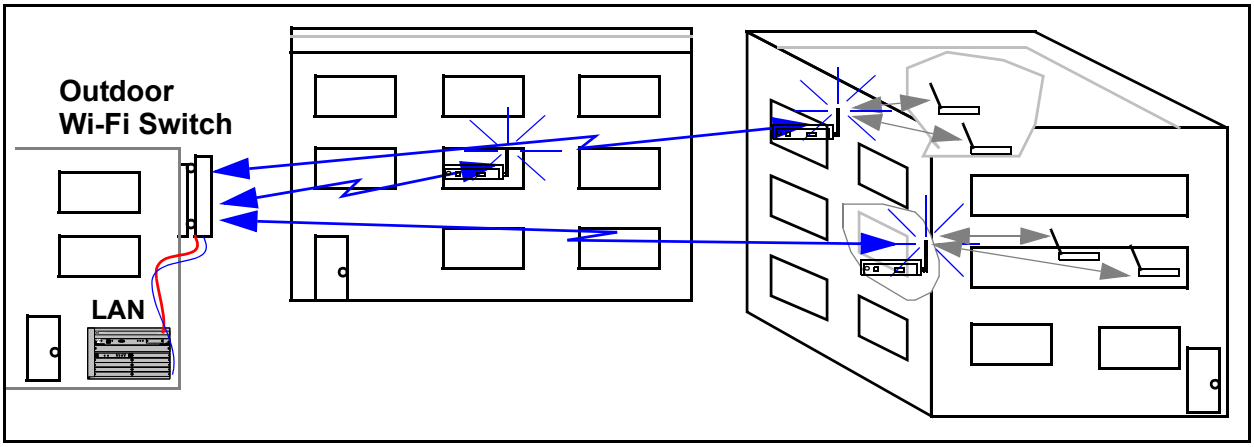


Figure 5—Wireless Backhaul Example

Preparing the Bridge/Router for Operation

To prepare the Bridge/Router 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 Bridge/Router, and insert the power supply terminal into its connector on the Wi-Fi Bridge/Router.

Step 3. Configure the Bridge/Router, using either the built-in Web interface or the command line interface. Refer to **"Initial Configuration Using the Built-In Web Pages"** on page 11 or **"Configuration Using The Command Line Interface"** on page 67.

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 Bridge/Router can be quickly configured using its built-in Vivato Vision© 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 Bridge/Router. To ensure Wi-Fi security before putting the Bridge/Router into service, make the necessary changes to the security settings during the initial configuration. See **"Security Configuration Web Pages"** on page 47.

Steps to Configuring the Vivato Wi-Fi Bridge/Router

Step 1. Connect a computer to the Wi-Fi Bridge/Router and access the Vivato Vision© web pages. See **"Configuration Connections"** on page 12.

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 19.

Step 3. Reboot the Wi-Fi Bridge/Router. The settings on the Quick Setup pages do not take effect until after the Wi-Fi Bridge/Router 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 47.

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 Bridge/Router'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 117 to see how you can make sure that everything is working as expected.

Default Configuration

The Wi-Fi Bridge/Router is delivered with the following settings pre-configured. Until you change *and save* the configuration, these settings are used anytime the Wi-Fi Bridge/Router 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 Bridge/Router 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 Bridge/Router 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 Bridge/Router, 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 42.
- **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 Bridge/Router using either a wired or a wireless connection. Once the connection has been established, the procedure to configure the Wi-Fi Bridge/Router is the same for either connection.

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

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

The default IP address of the Wi-Fi Bridge/Router is 169.254.20.1, which is within the range of 169.254.0.1 to 169.254.255.254. Your computer's network interface must be assigned an IP address within this range (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 network 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 98 support this feature.

Important	To ensure a quick connection to the Wi-Fi Bridge/Router 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 Bridge/Router 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 Bridge/Router, 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.

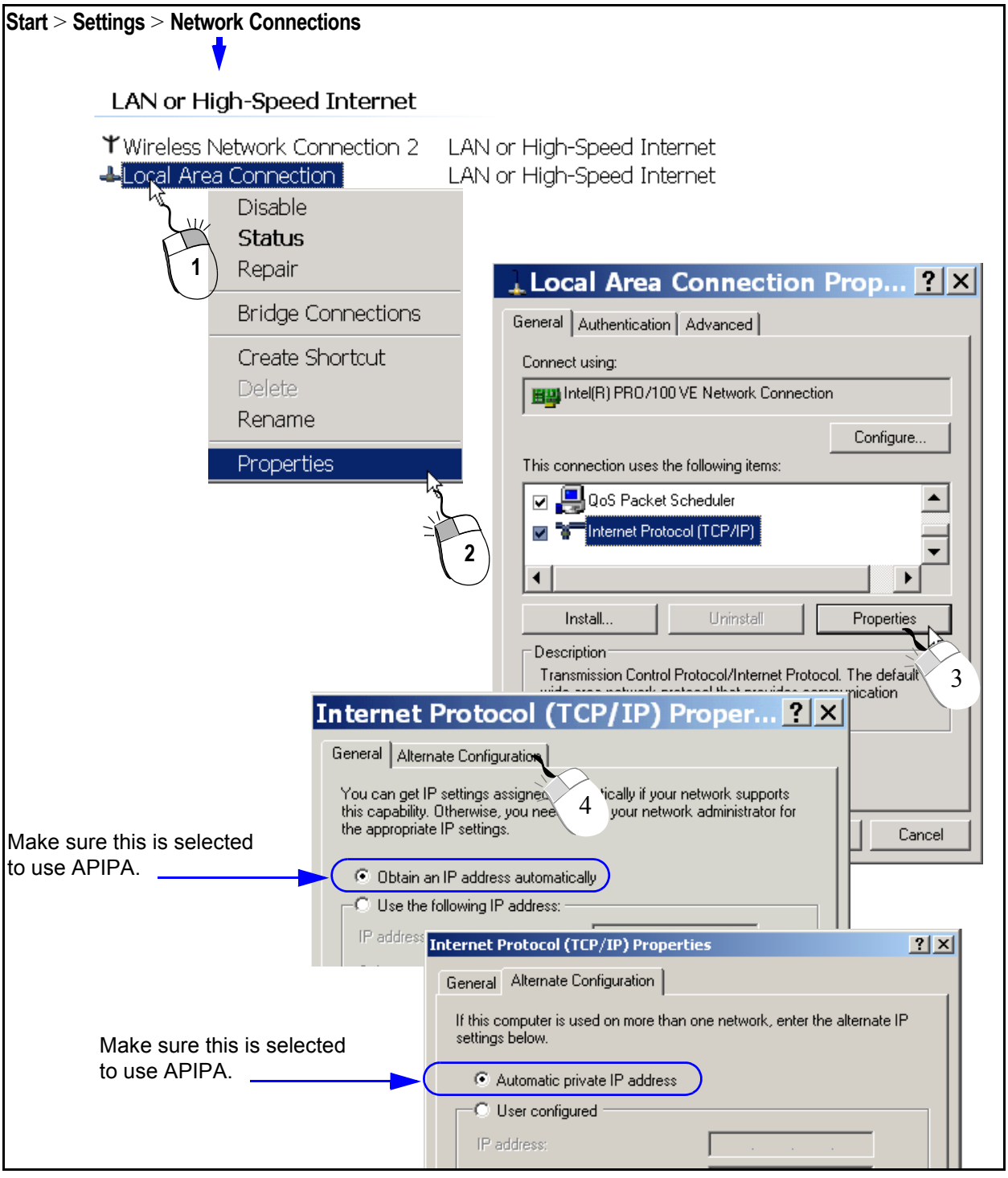


Figure 1—Enabling Automatic IP Address Assignment on Your Wireless Client

Step 5. Shut down your computer.

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

Wired Connection to Access the Configuration Web Page

After the Wi-Fi Bridge/Router 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 Bridge/Router's Ethernet port.

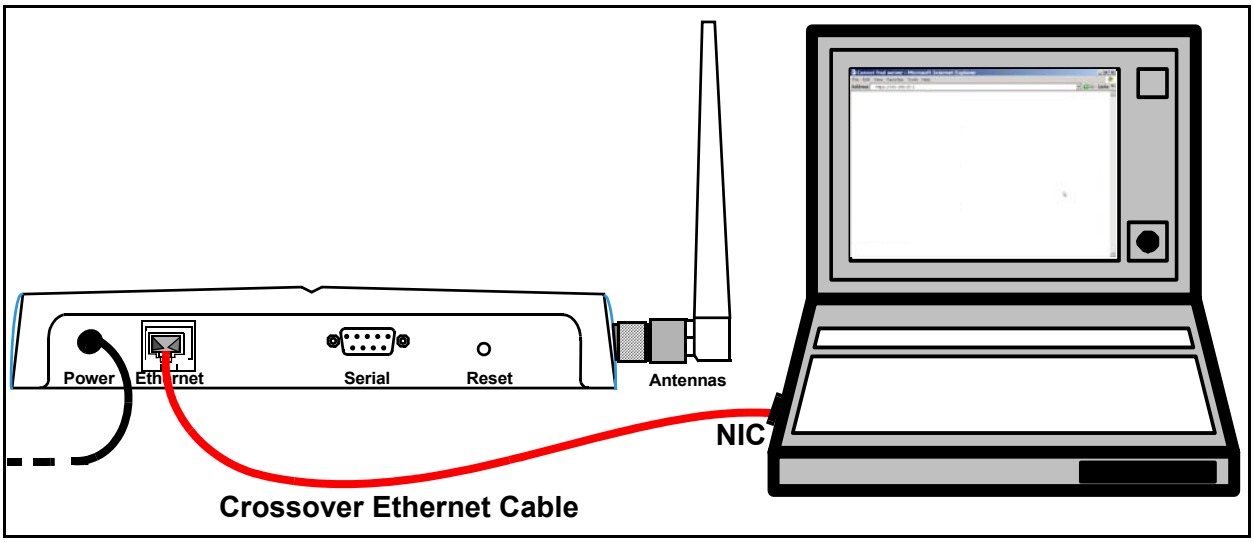


Figure 2—Wired Connection To Access The Configuration Web Page

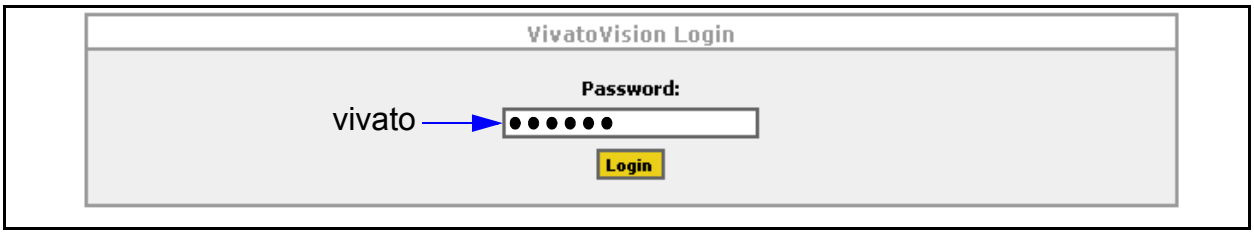
Step 1. Turn on your computer.

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 Bridge/Router 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 Bridge/Router. Select "Yes".

Step 5. The Wi-Fi Bridge/Router’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 Bridge/Router. 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 19.

Wireless Configuration Connection

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

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

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.

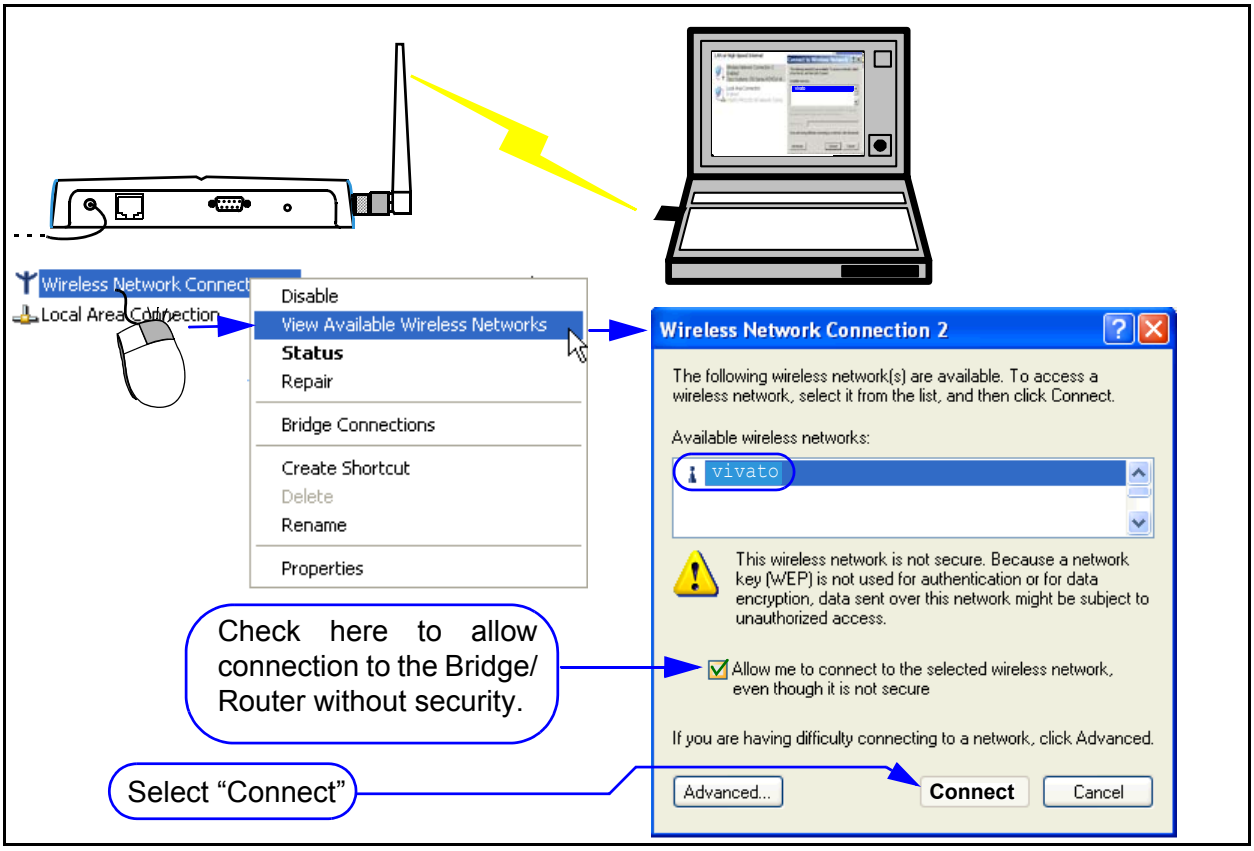


Figure 3—Wireless Connection to Access the Configuration Web Pages

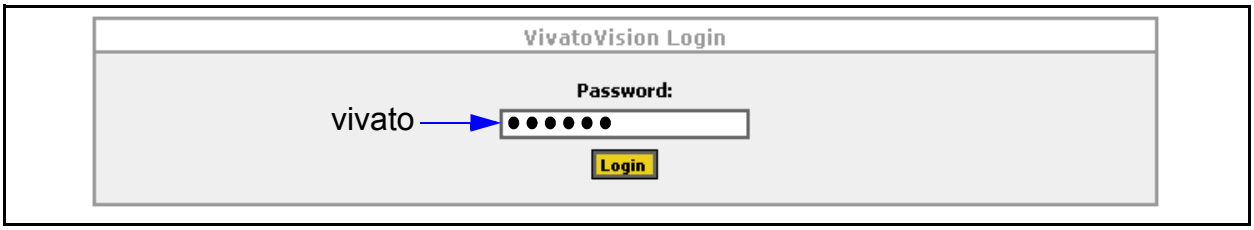
Because the Wi-Fi Bridge/Router is delivered with wireless security disabled to allow configuration through a wireless connection, you may need to confirm using an unsecured connection.

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

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

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 Bridge/Router IP address in the Address/Location field in your browser: **https://169.254.20.1**. The Wi-Fi Bridge/Router'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 Bridge/Router. 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.

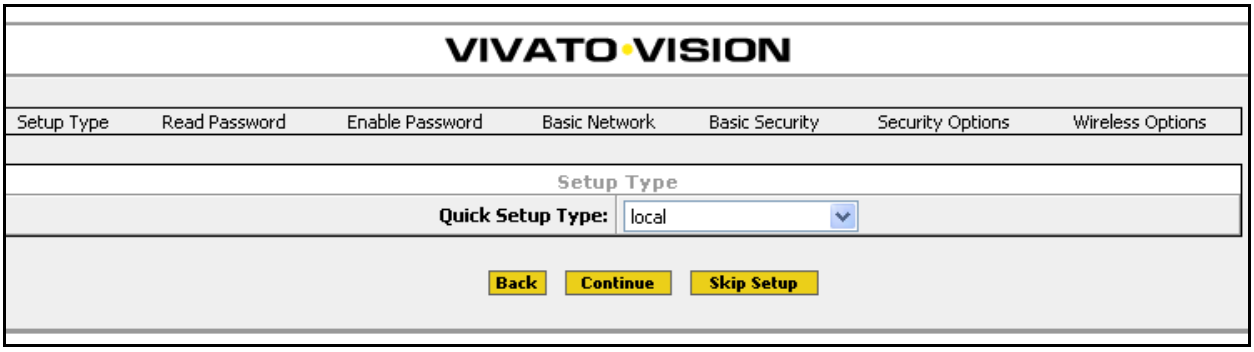
Entering the Initial Configuration Information in the Quick Setup Pages

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 Bridge/Router 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 Bridge/Router.

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

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 Bridge/Router's configuration. **The password is "vivato" when the Vivato Wi-Fi Bridge/Router 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.

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 Bridge/Router's configuration.
- **New "Enable" Password Verification**: Enter the new password again.

Basic Network Setup

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

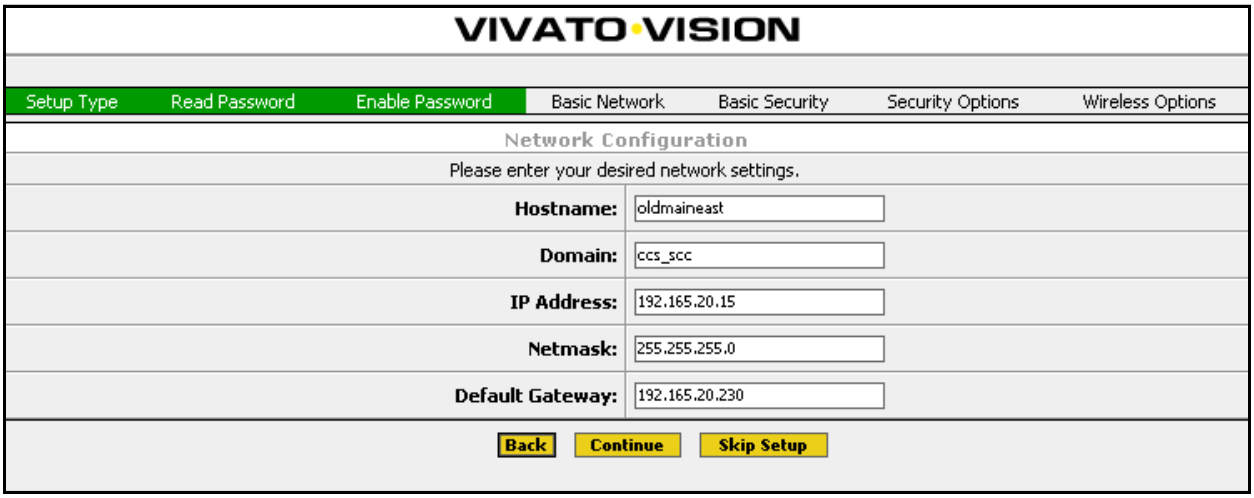


Figure 6—Basic Network Setup Page

- **Hostname**: Enter a name to be used to refer to the Wi-Fi Bridge/Router in your *wired* network. For your network to be able to identify the Wi-Fi Bridge/Router 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 Bridge/Router will be used.

- **IP Address**: Enter a static IP address for the Wi-Fi Bridge/Router. 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 Bridge/Router, 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 Bridge/Router.

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

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.

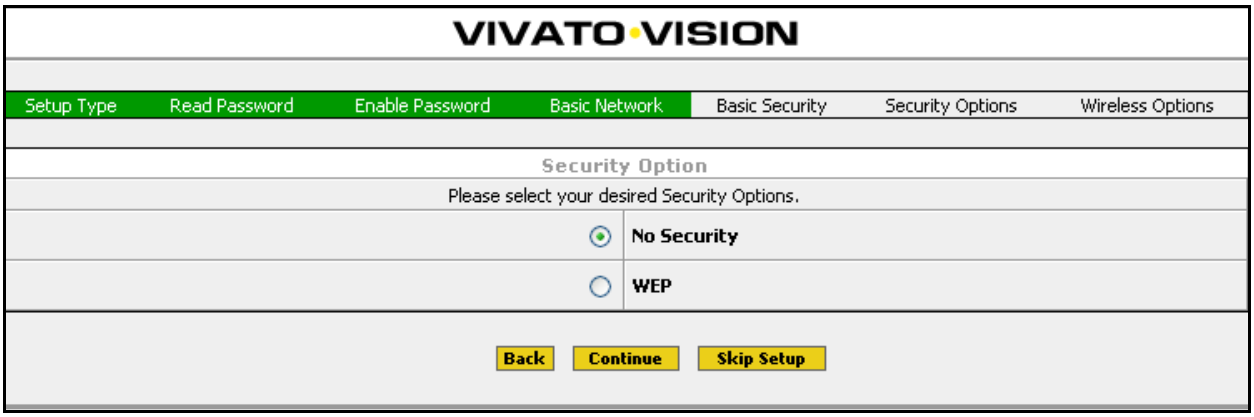
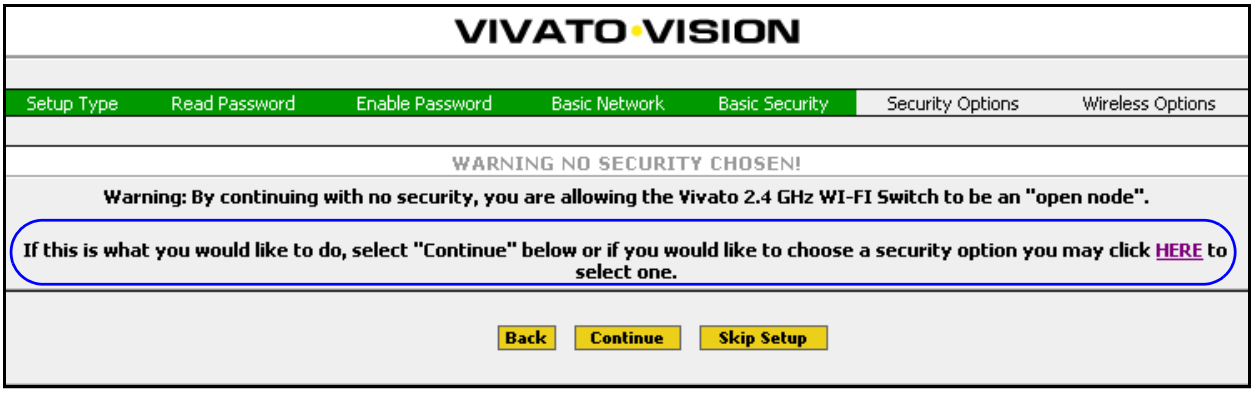


Figure 7—Basic Security Setup Page

- **No Security**: This setting allows any wireless client to associate with the Wi-Fi Bridge/Router 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).

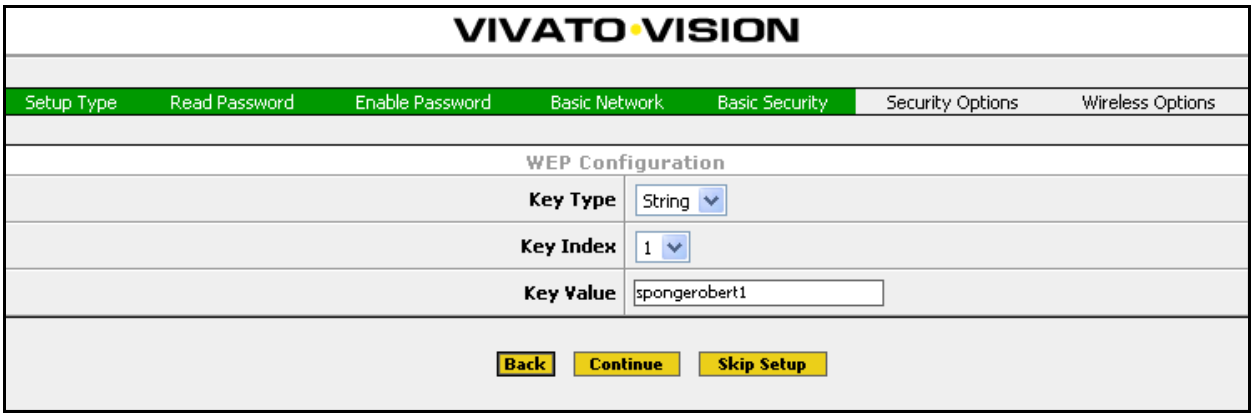
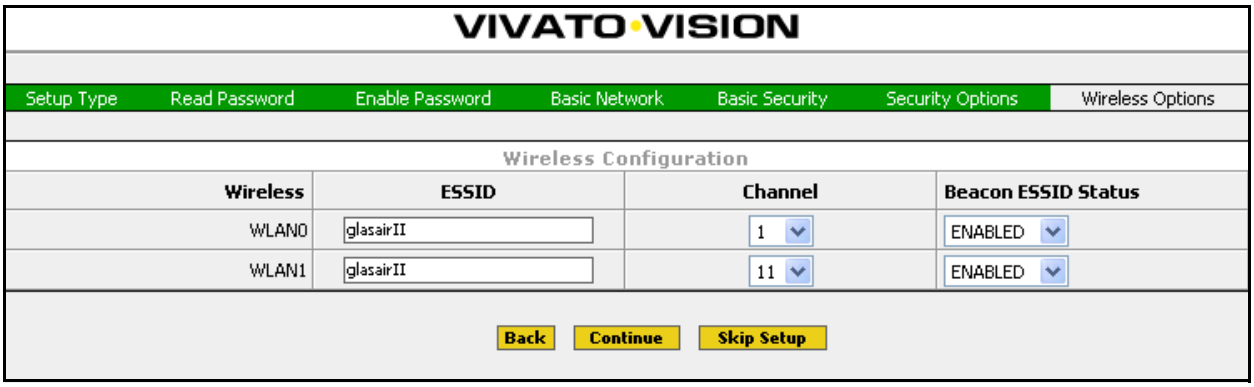


Figure 8—WEP Security Configuration During Quick Setup

Wireless Options Setup

Wireless options specify the extended service set identifier (ESSID) that the Wi-Fi Bridge/Router 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 Bridge/Router's signals.



- **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 Switch, 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 Bridge/Router'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 (channels 1 through 11 are supported). You should typically have one interface set to channel 1 and the other interface set to channel 11 (the default).

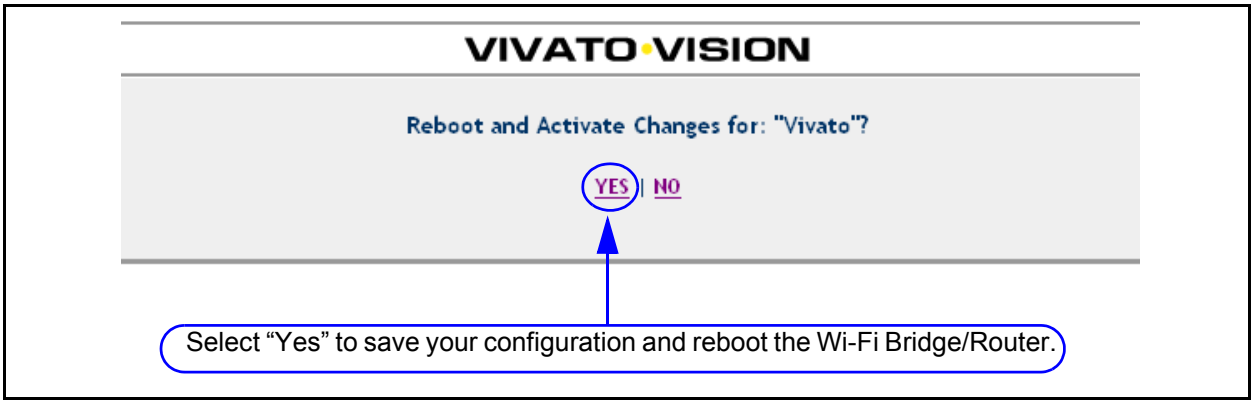
1. ESSID and SSID are essentially the same thing. The Vivato Wi-Fi Switch and Bridge/Router can broadcast on two or more wireless interfaces, so they create an "extended" service set.

- **Beacon ESSID Status**: When set to "DISABLED", the ESSID is not sent on the beacons from the Wi-Fi Bridge/Router to the clients. This prevents Wi-Fi clients from being able to see the Wi-Fi Bridge/Router's ESSID in its "Available Networks" list. When beacons are disabled, the only way a client can associate with the Wi-Fi Bridge/Router is if the ESSID is known and is manually entered into the client's list of preferred networks. This provides a level of security from undesired users who may attempt to associate with the Wi-Fi. This can also be used to help prevent undesired detection of a WDS link on that interface.

Rebooting the Wi-Fi Bridge/Router

After entering your configuration information on all of the Quick Setup screens, you are prompted to reboot the Wi-Fi Bridge/Router. 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 Bridge/Router to reboot using the new configuration, it should be ready to operate on your network. Connect your LAN cable to the Wi-Fi Bridge/Router's Ethernet port. Wi-Fi clients should be able to access your LAN through the Wi-Fi Bridge/Router at this time if their security settings have been properly configured.



Where Do I Go From Here?

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

- **Access Point operation**: If you are using the Bridge/Router 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 48 and follow the steps for configuring WEP in your client.
- **Coverage Filler, Repeater, and Wireless Backhaul operation:** To use the Bridge/Router with a Wi-Fi Switch, you need to configure one of the wireless interfaces in *both* devices to form a wireless distribution system (WDS) link between them. This involves setting the same channel number and enabling WDS on a wireless interface on both devices, 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 108. To use the Web configuration pages, see **"Network>WDS"** on page 44

To make additional changes to the Wi-Fi Bridge/Router'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 Bridge/Router 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 27.

Using the Main Configuration Web Pages

The Quick Setup screens are used to configure the Wi-Fi Bridge/Router 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 Bridge/Router. 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 Bridge/Router, select **Logout of Vivato Vision** to end your configuration session.

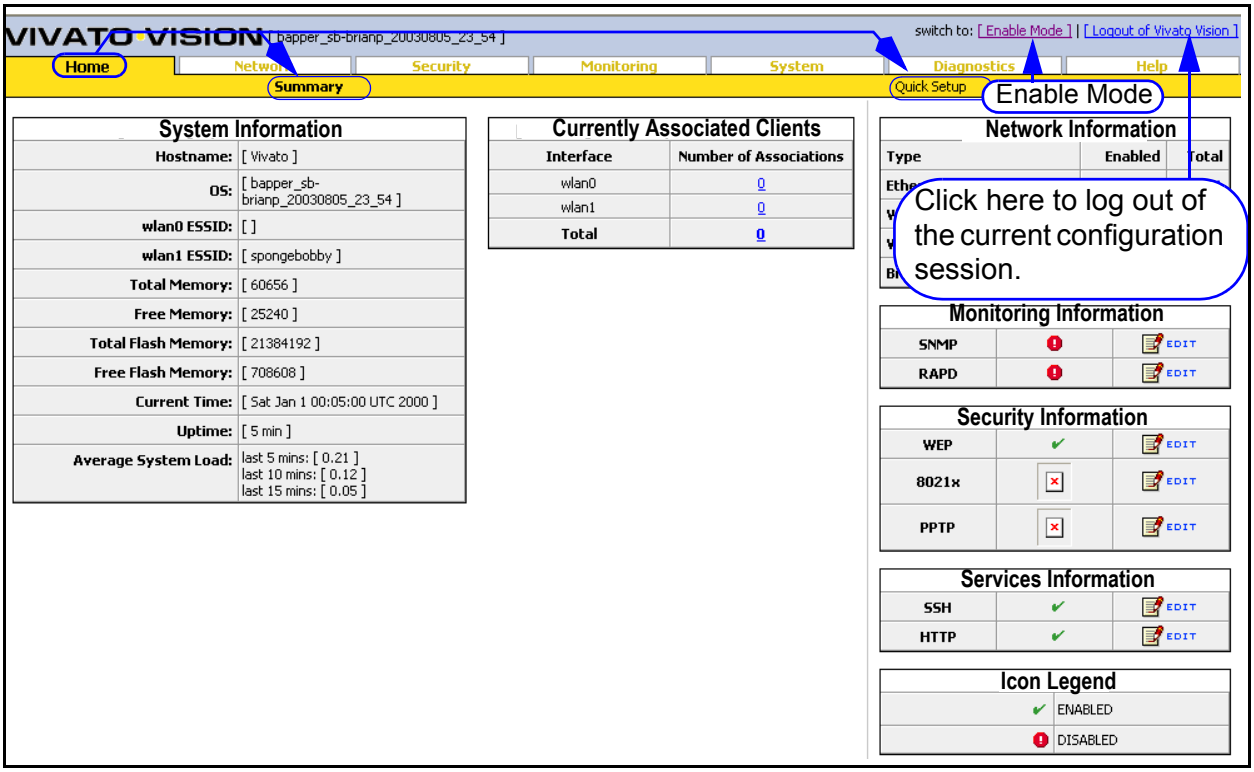


Figure 9—Accessing Settings From the Home Configuration Screen

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 Bridge/Router hardware and system configuration (see **"Accessing Settings From the Home Configuration Screen"** on page 27).

System Information

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

- **Hostname:** The Hostname that you assigned.
- **OS:** Version of the Wi-Fi Bridge/Router's software.
- **wlan ESSID**: The ESSID assigned to each wireless interface.
- **Total Memory**: Amount of memory in the Bridge/Router.
- **Free Memory**: Memory available for system use.
- **Total Flash Memory**: The total amount of flash memory used for storing the Wi-Fi Bridge/Router'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 Bridge/Router 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.

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 Bridge/Router. 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 Bridge/Router. 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.

Network Configuration Web Pages

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

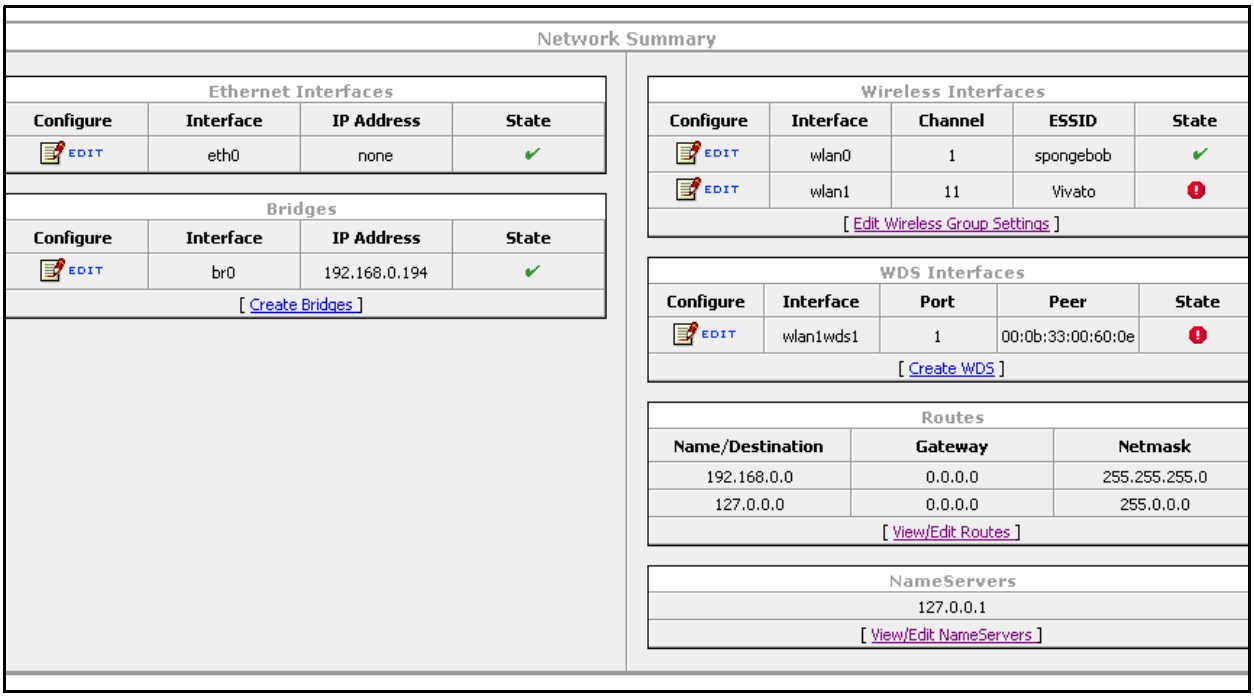
Network Settings

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 Switch.

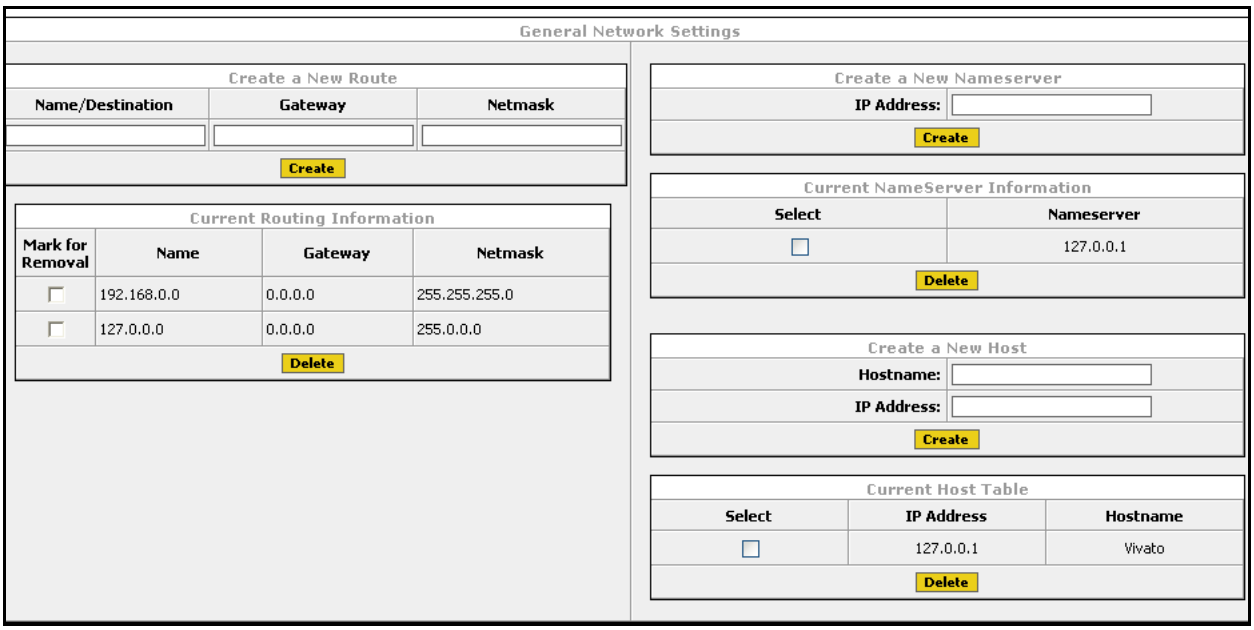
Network>Summary

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.



Network>General

The General Network Settings are used to specify other devices in your network that the Wi-Fi Bridge/Router must communicate and the routes used to get there. Settings are also provided to specify how the Wi-Fi Bridge/Router will handle packets from multiple clients to provide the greatest data rates.



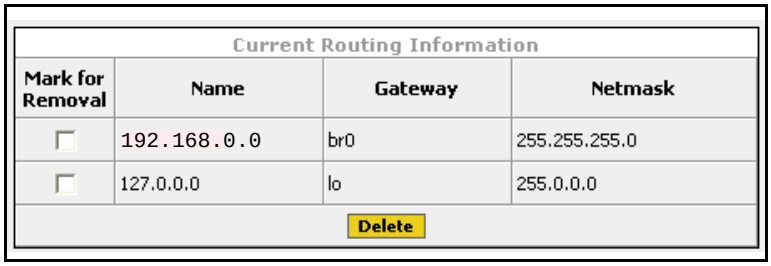
Create a New Route

Routes tell the Wi-Fi Bridge/Router 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

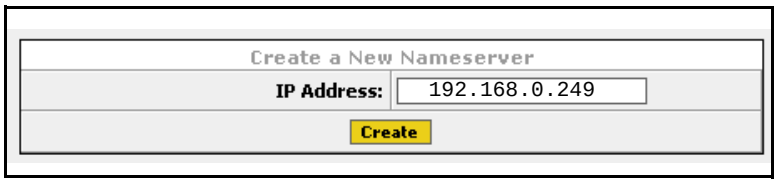
The Current Routing Information table indicates how packets within specified IP address ranges are directed (routed). In the example below, all packets addressed to the 192.165.0.0 base IP address that are within the Netmask of 255.255.255.0 are routed through the default bridge - br0. *The 127.0.0.0 route is a loopback path used by the Wi-Fi Bridge/Router'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 Bridge/Router uses to forward traffic to the destination address.
- **Netmask**: The subnet mask defining the range of IP addresses accessed through this route.

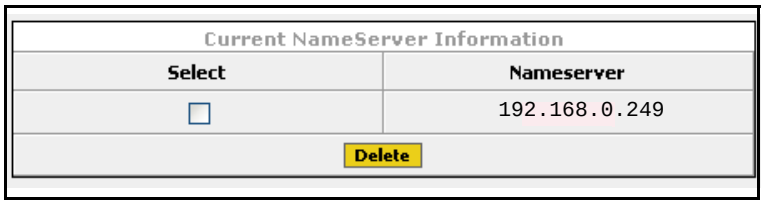
Create a New Nameserver

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.



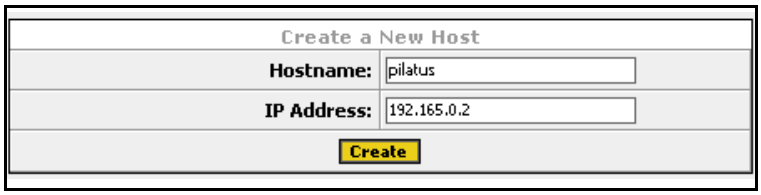
Current NameServer Information

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



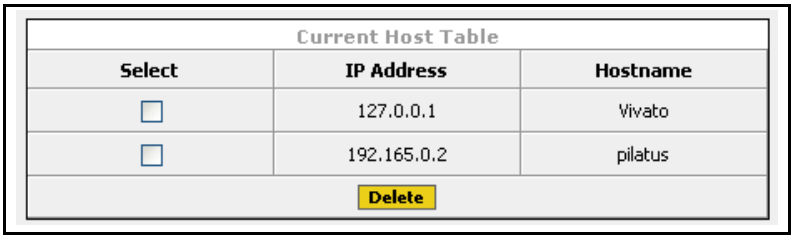
Create a New Host

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



Current Host Table

The Wi-Fi Bridge/Router'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**.



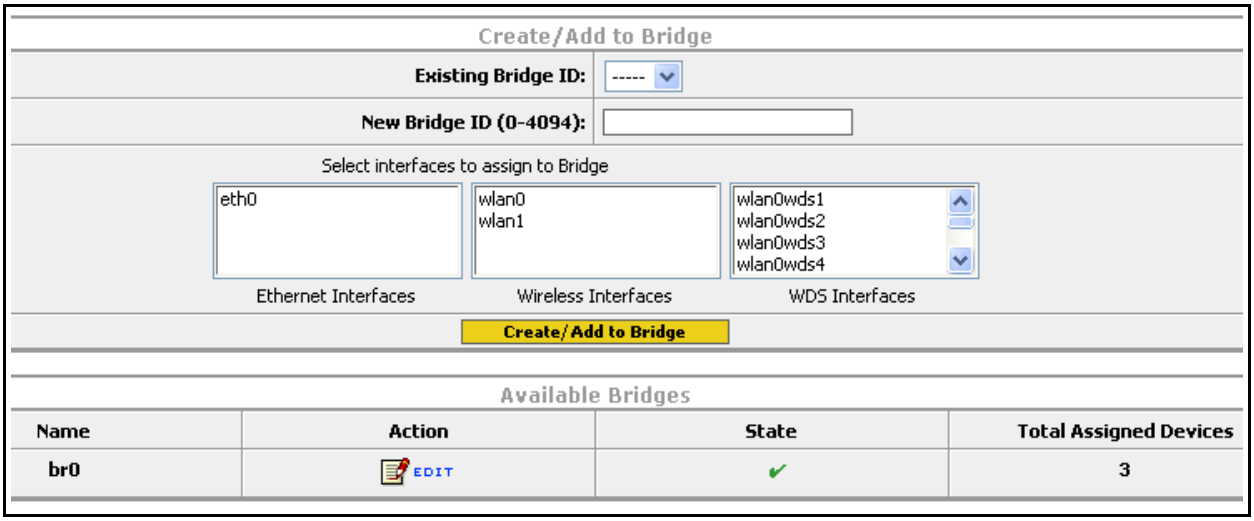
Network>Bridge

Bridges create pathways for data packets to travel freely between two or more interfaces within the Wi-Fi Bridge/Router. 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 Bridge/Router is applied to this bridge for immediate access to these interfaces.

Create/Add to Bridge

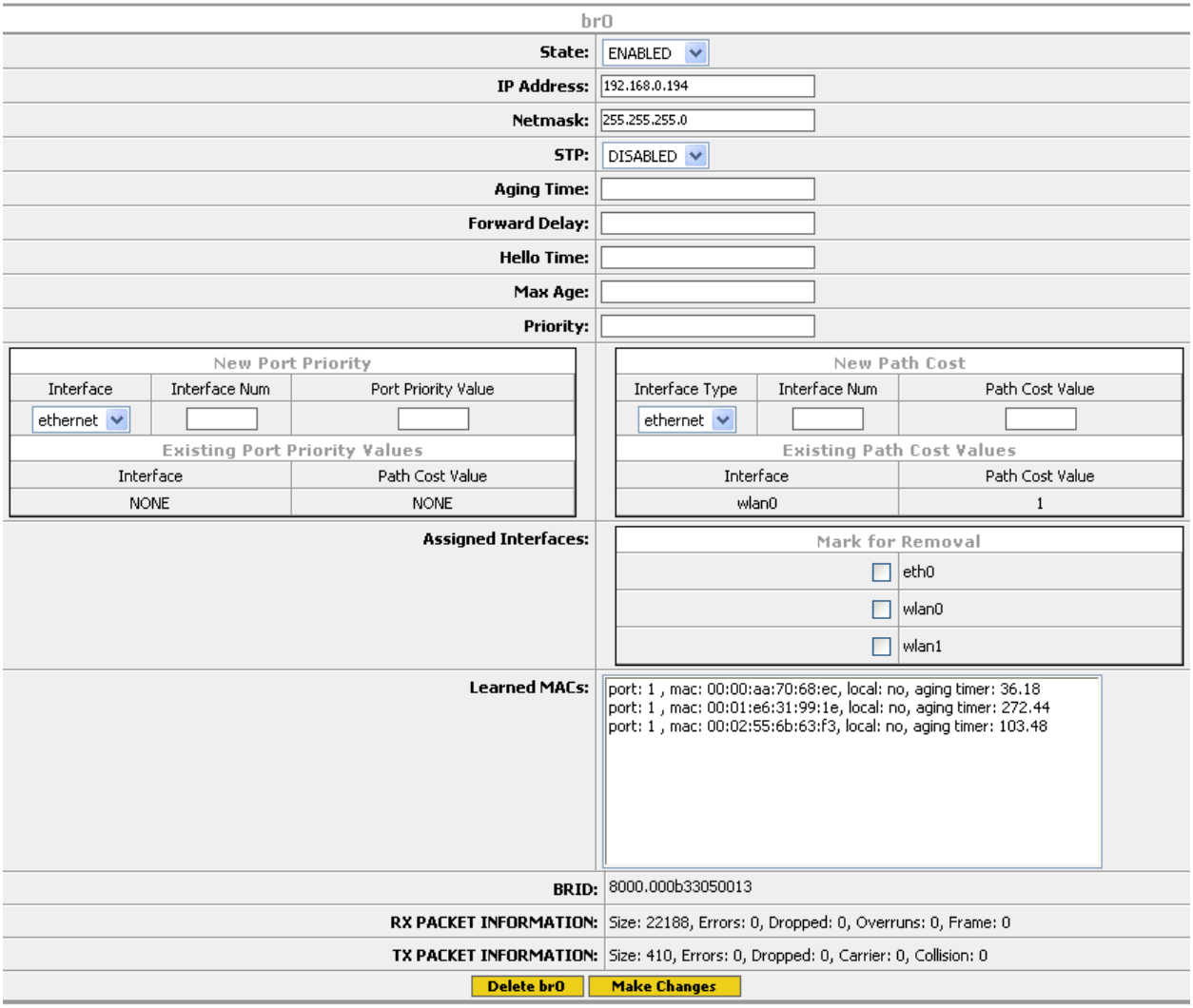
The following menu is used to add an interface to an existing bridge and to create a new bridge.



- **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.

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 Bridge/Router 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.

- **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 Bridge/Router 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 Bridge/Routers 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

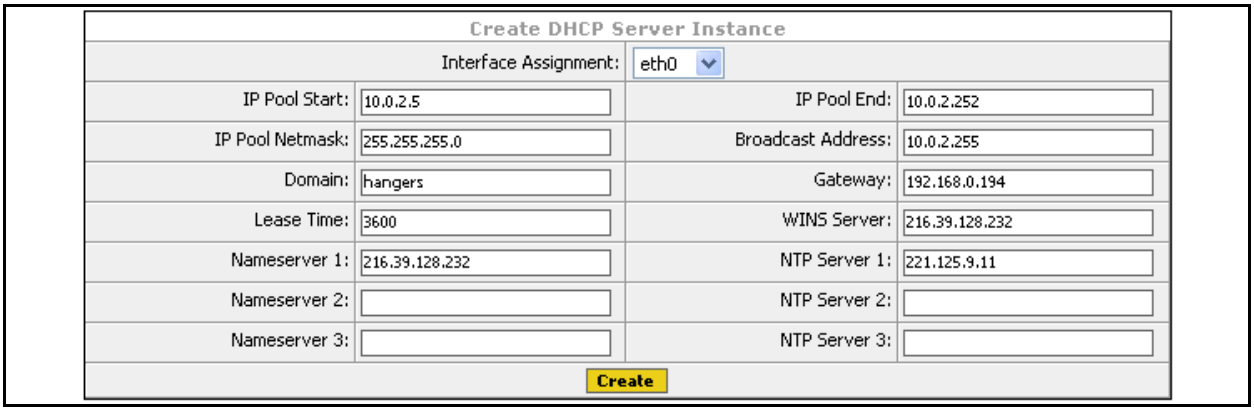
The IP address of the default bridge (br0) is used to access the Bridge/Router for initial configuration. If you delete this bridge before assigning an IP address to a different bridge, VLAN, or Ethernet interface, you will lose connection to the Bridge/Router when the bridge is deleted and you will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

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

Network>DHCP

The Wi-Fi Bridge/Router 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 Bridge/Router. See **"Dynamic Assignment of Client IP Addresses"** on page 123.

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 typically the Ethernet port connected to your wired network.
- **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.

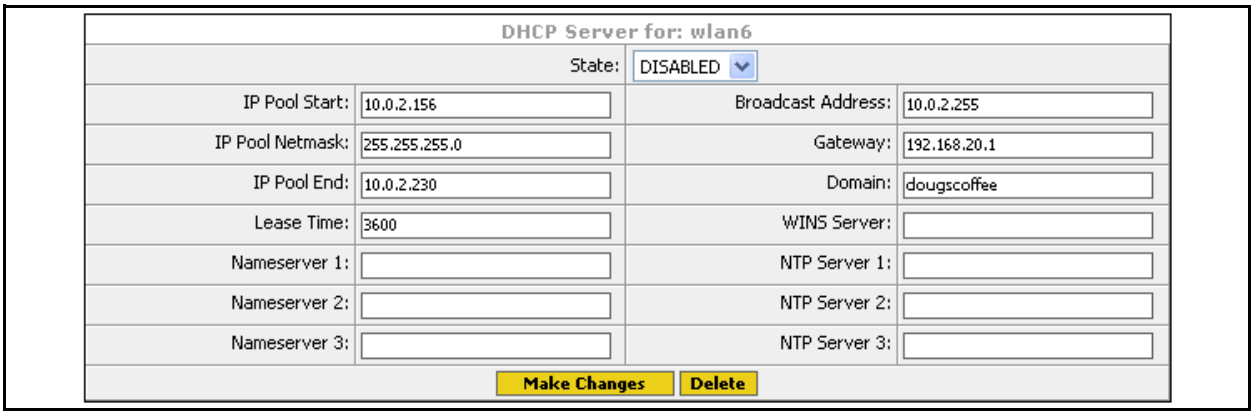


Figure 10—Editing or Deleting a Configured DHCP Server

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 Bridge/Router 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 80.

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

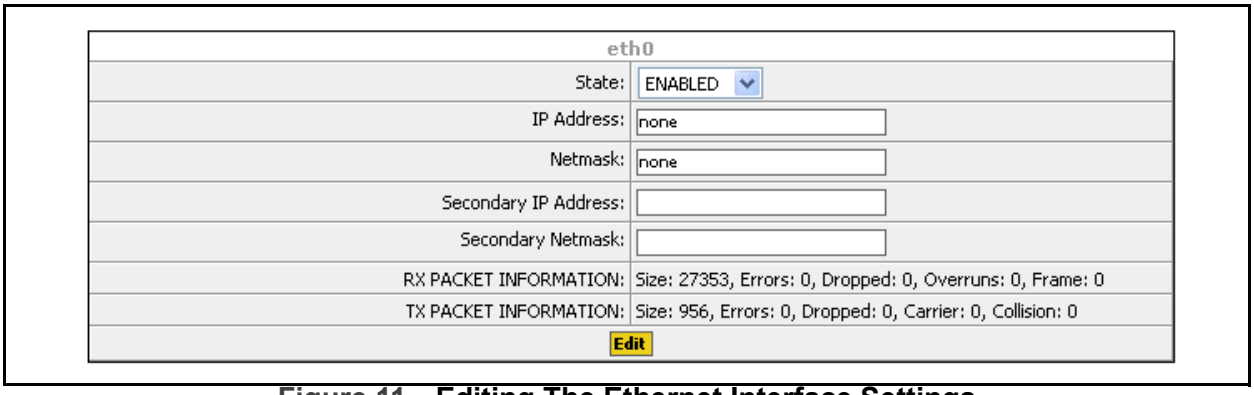
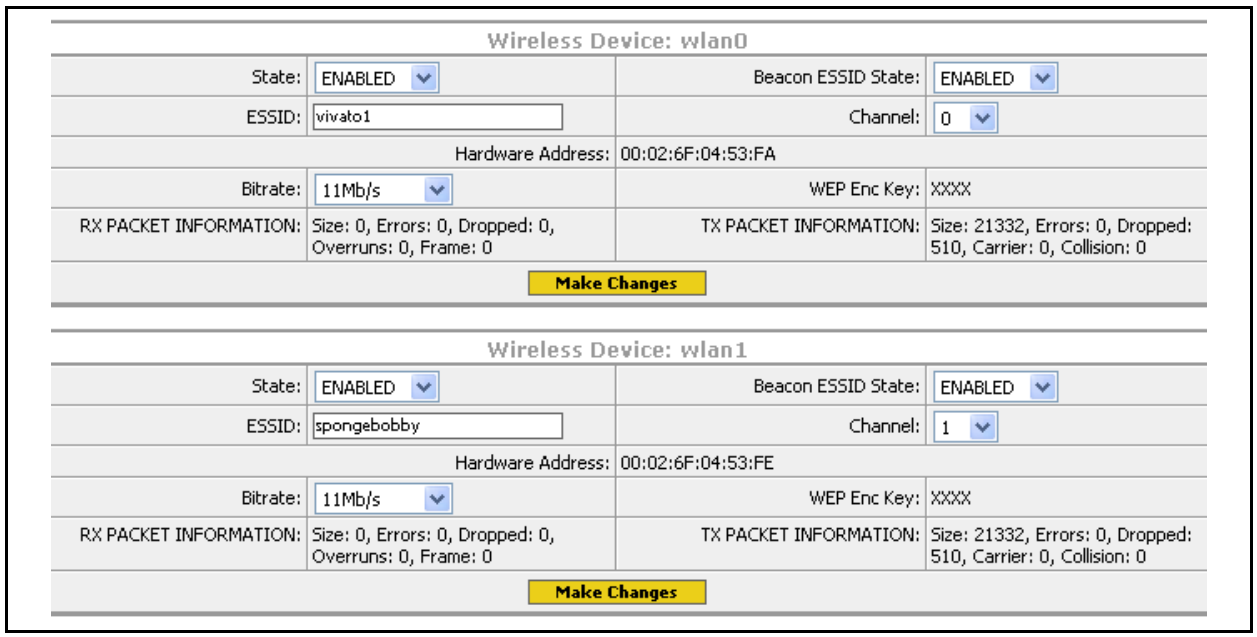


Figure 11—Editing The Ethernet Interface Settings

Network>Wireless Interfaces

The Wi-Fi Bridge/Router 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 80 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.

- **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 Bridge/Router. 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. Only channels 1 through 11 are available. 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).

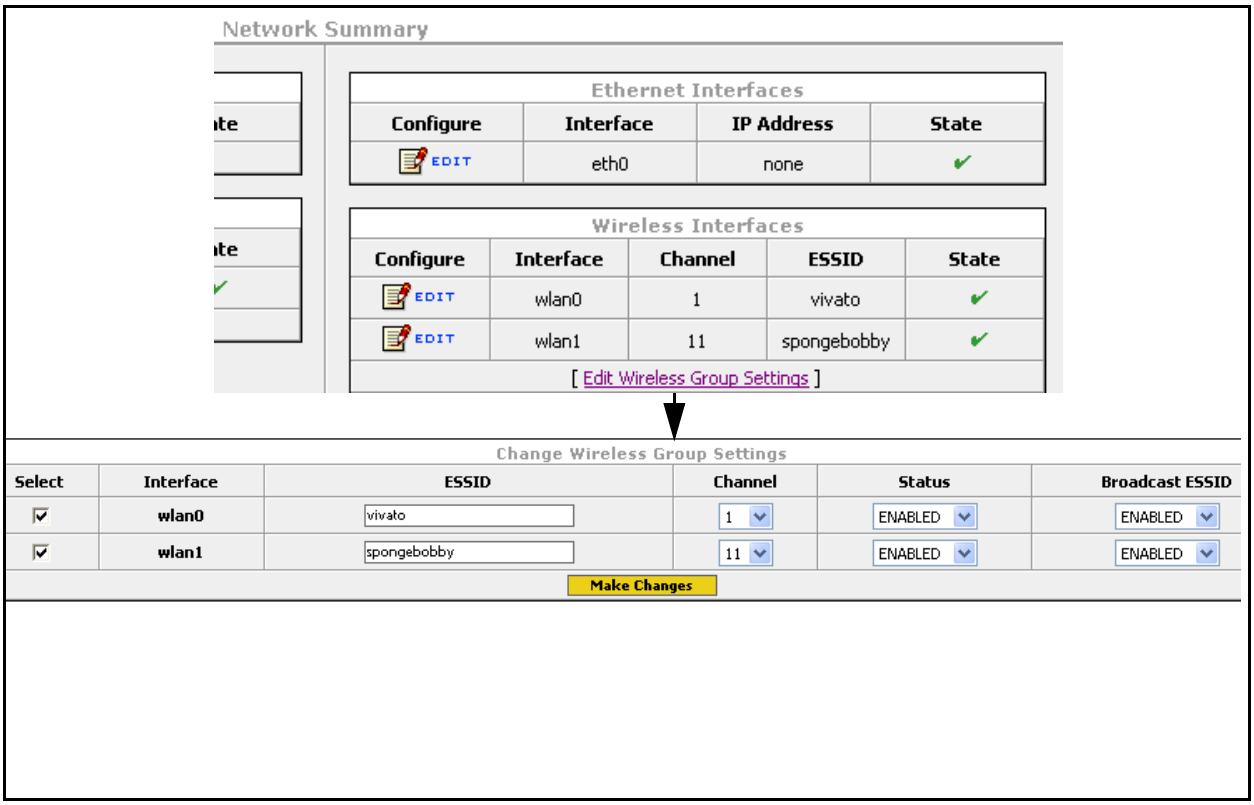


Figure 12—Editing Wireless Interface Settings As a Group

Configuring the Wireless Interfaces as a Group

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

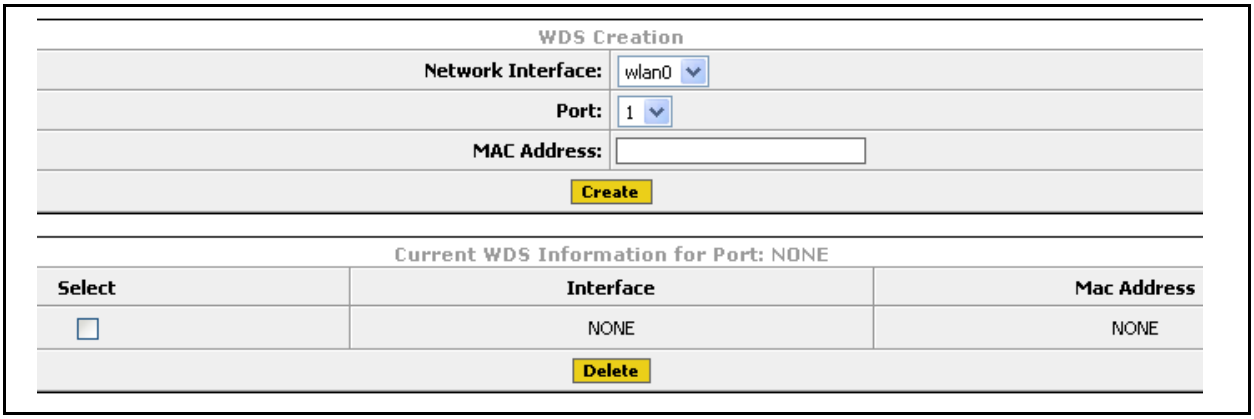
1. Enter the changes for the **ESSID**, **Channel**, **Status**, **Broadcast ESSID** for each interface. See **Configuring Wireless Interfaces Individually** for descriptions of each setting.
2. Click on the **Select** box for the interface(s) to configure using these changes.
3. Select **Make Changes**.

Network>WDS

Wireless distribution system (WDS) allows the Bridge/Router to connect to a Vivato Wi-Fi Switch through a wireless interface from each device. The WDS connection is used instead of a wired LAN connection when deploying the Bridge/Router as a coverage filler, range extender, or to provide a wireless backhaul to a Wi-Fi Switch. See **"Network Configuration Examples"** on page 3.

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 36.

For more information on WDS operation, see **"Configure WDS (Wireless Distribution System)"** on page 108.



WDS Creation

A WDS connection must be created on the Bridge/Router and on the Wi-Fi Switch 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 the Wi-Fi Switch (the “peer” address).

Current WDS Information

This area lists the WDS connections that have been configured on the Bridge/Router 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**.

Security Configuration Web Pages

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

Security settings determine who is allowed network access through the Vivato Wi-Fi Bridge/Router. Security is initially turned off in the Wi-Fi Bridge/Router 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.

Security Settings

Security settings are arranged on the following configuration pages:

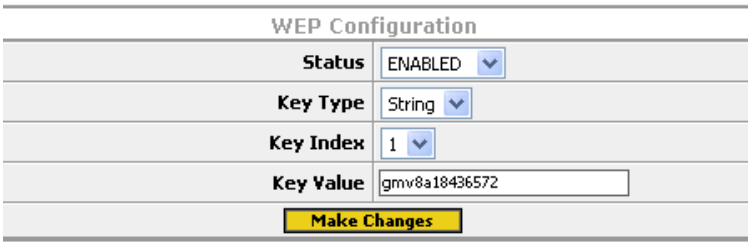
- **Security>WEP** - Wired Equivalent Privacy

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.

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 Bridge/Router and the wireless clients to try to provide a secure link between them. See **"Optimizing Your Wireless Client For Secure Communications"** on page 48 for information on configuring your 802.11b client to use WEP.



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.

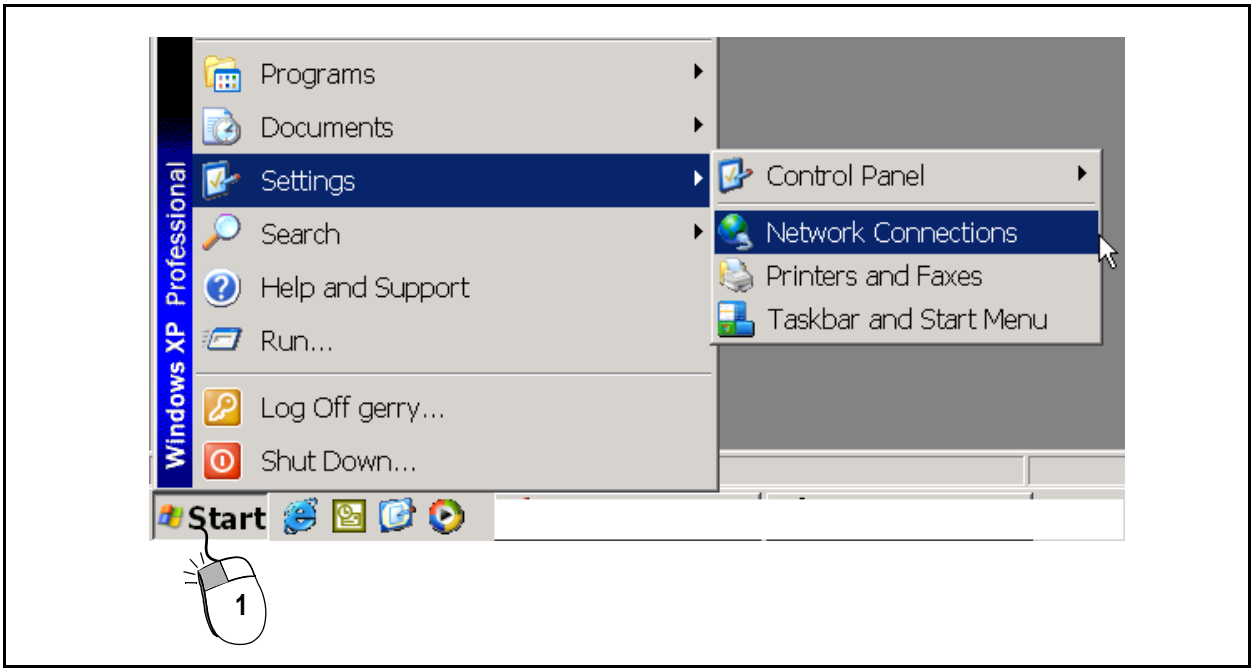
- **Key Index**: Up to four WEP keys can be configured. The key index represents which key value you are using. The key indexes and the key values for clients must match those of the Wi-Fi Bridge/Router. In most client's configuration settings, the WEP key index ranges from 1 to 4; just like the Wi-Fi Bridge/Router. 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 Bridge/Router 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 Bridge/Router's configuration to use the specified key value on the specified interface.

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 Bridge/Router'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**.

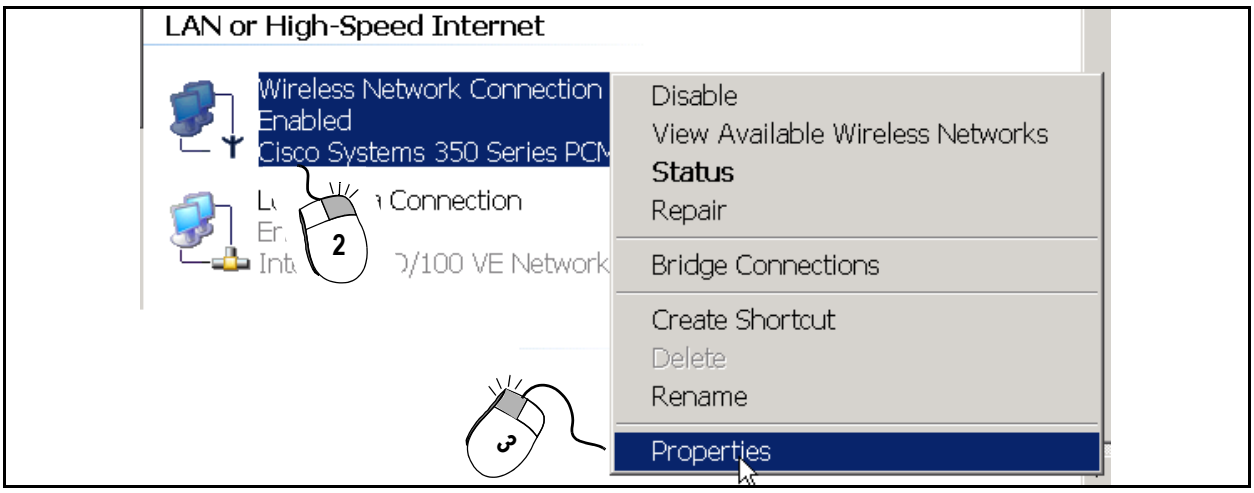


Figure 13—Accessing the Wireless Network Connections Configuration

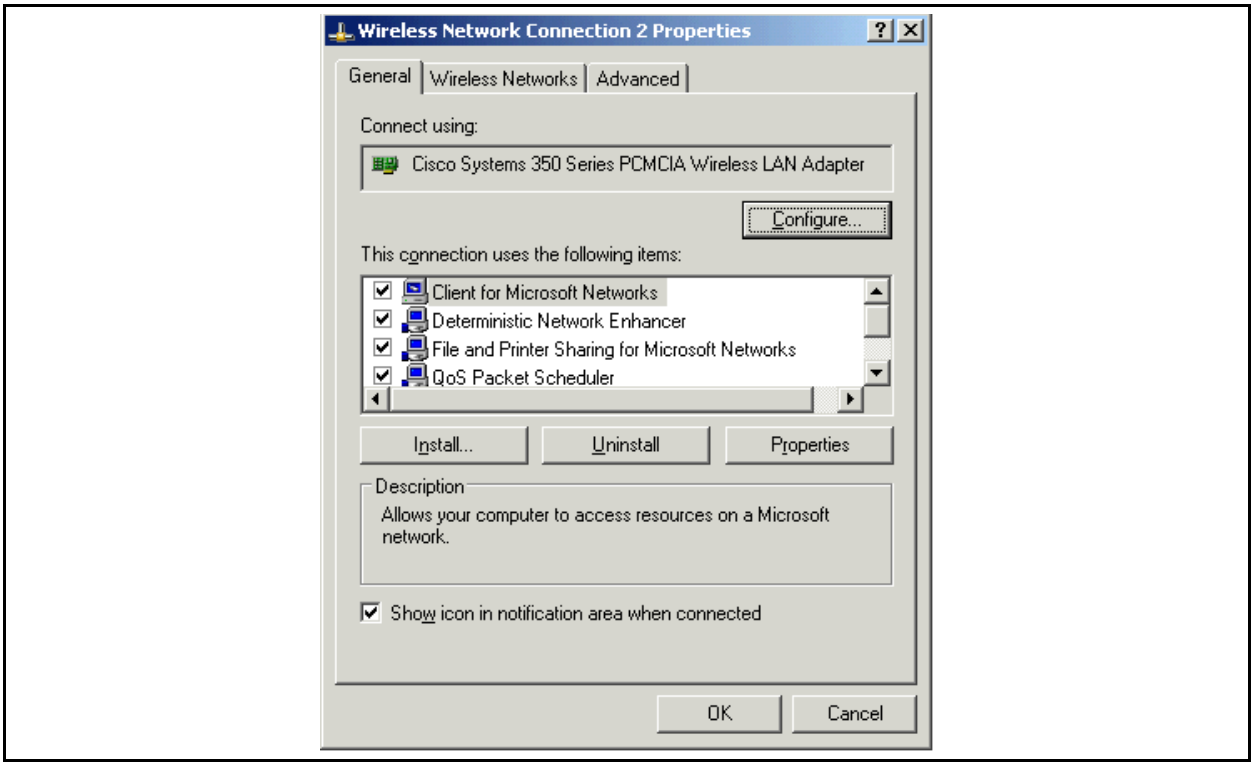


Figure 14—Windows XP Wireless Network Connections Screen (With the Client Enabled)

Configuring WEP in Your Client

See **"Security>WEP"** on page 47 for a description of WEP.

With the *client enabled* and close enough to the Wi-Fi Bridge/Router 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 Bridge/Router is not close*

enough to the client to receive its signals, or the Bridge/Router 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 50**). If the ESSID for the Wi-Fi Bridge/Router's wireless interfaces has been changed, use that entry instead.

If you are not receiving the Wi-Fi Bridge/Router's signal (no ESSID is shown), verify that a wireless interface has been enabled on the Wi-Fi Bridge/Router. See **"Network>Wireless Interfaces"** on page 42.

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.

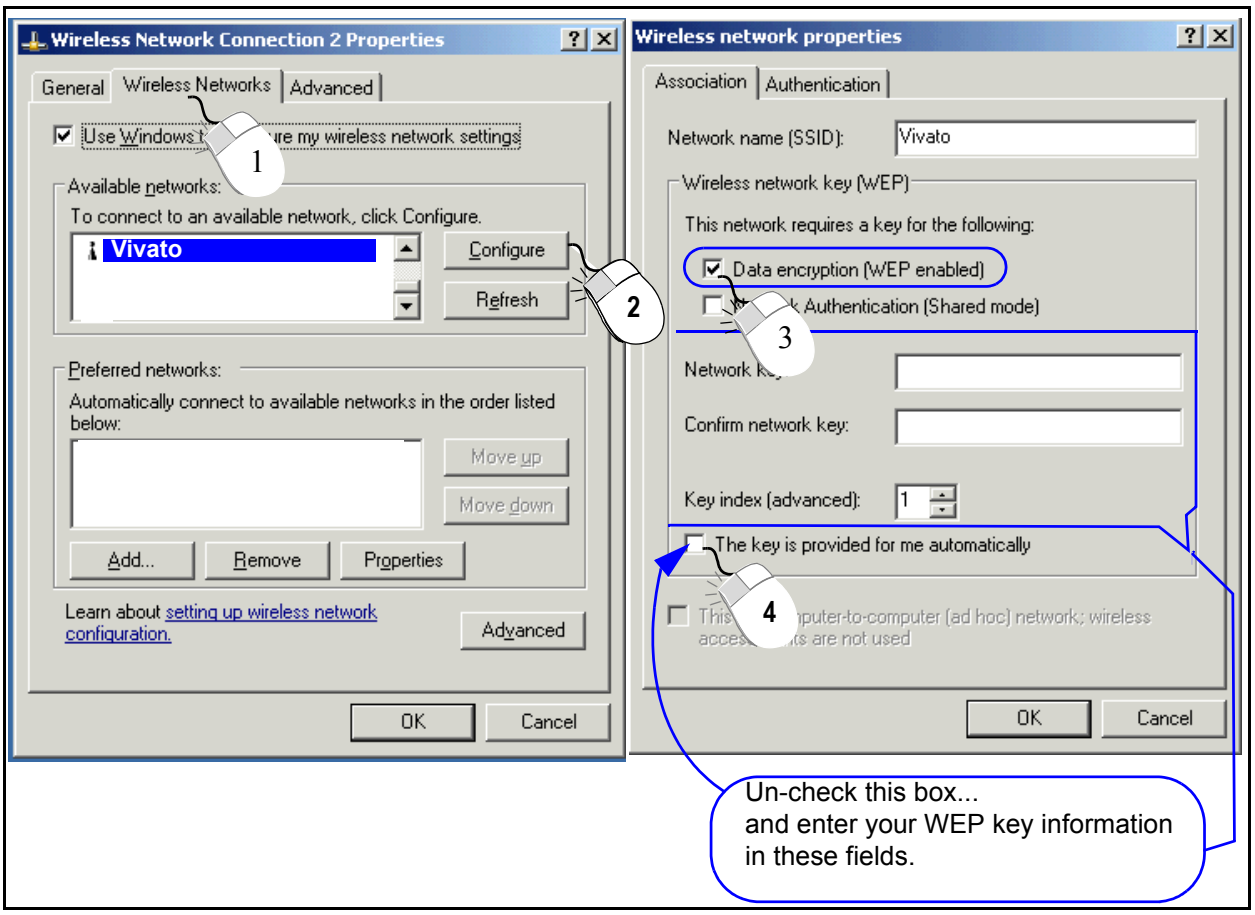


Figure 15—Configuring WEP in Your Client

Monitoring Clients and System Operations

The **Monitoring** web configuration screen accesses settings for displaying system messages and associated client information, and is also used for configuring simple network management protocols (SNMP).

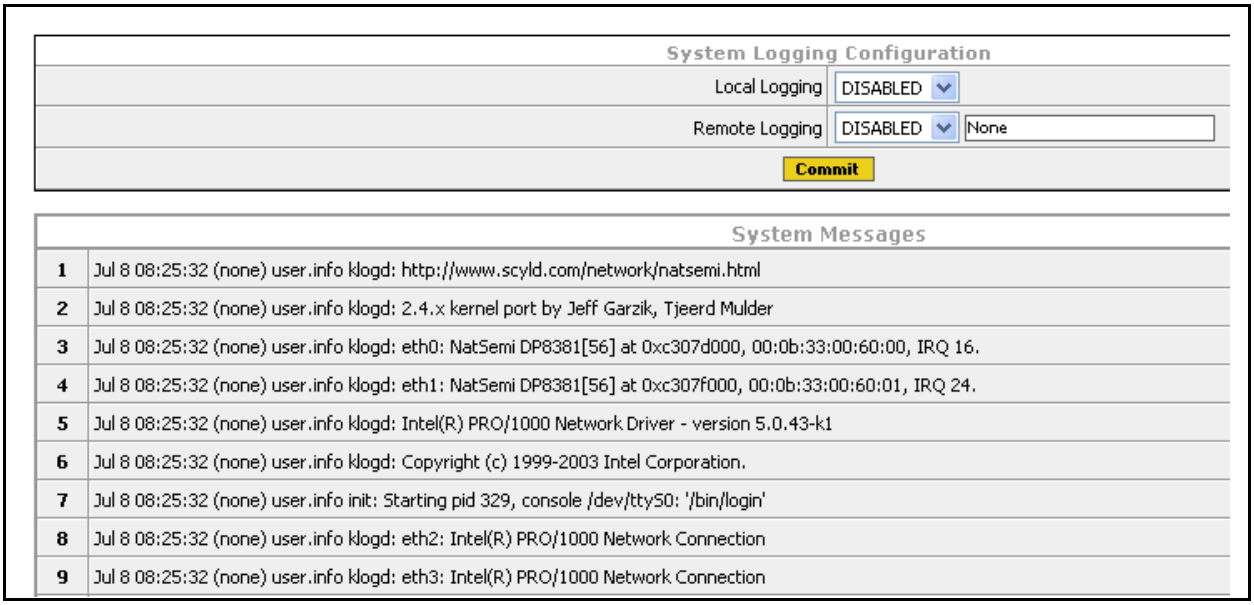
Monitoring Settings

Monitoring settings are arranged on the following configuration pages:

- **Monitoring>System Messages** - View system events and define where to store the system event log.
- **Monitoring>SNMP Monitoring** - Enable SNMP and configure communities, users, and traps.
- **Monitoring>Associated Clients** - View a dynamic listing of clients associating with each wireless interface.

Monitoring>System Messages

This page is used to view system event messages and define the remote log server.



System Logging Configuration

System messages can saved (logged) on the Wi-Fi Bridge/Router and on a remote device.

- **Local Logging**: Select ENABLED to save system messages in dynamic memory on the Wi-Fi Bridge/Router. The logged events can be viewed through the command line interface (CLI) using the **show logging** command. The log file is cleared any time the Wi-Fi Bridge/Router is rebooted. The default is DISABLED; displaying system messages on this web page but not saving them in the Wi-Fi Bridge/Router.
- **Remote Logging**: Select ENABLED to send system messages to a remote host located at the IP address entered in the box next to this field. The remote host must first be configured to accept remote logging (syslogd -r at a minimum).
- **Commit**: Select this field to put these settings into effect.

Monitoring>SNMP Monitoring

Simple network management protocols (SNMP) use pre-defined sets of data for the Wi-Fi Bridge/Router called a management information base (MIB) to monitor network operations. The MIBs are defined in a way that allows third-party developers of network monitoring software to use them with their products. The Vivato Wi-Fi Bridge/Router has its own MIB, and also supports several industry standard MIBs. Refer to **"Network Monitoring"** on page 113 for more operation on using SNMP with the Vivato Wi-Fi Bridge/Router.

The Vivato Wi-Fi Bridge/Router supports SNMP versions 1, 2c, and 3. Some configuration settings are only used by a specific SNMP version. These settings are separated on the configuration web pages.

Base SNMP Options

These settings do not take effect until **Make Base SNMP Changes** is selected after entering your information:

- **Status**: Select enable or disable to turn SNMP on or off, respectively.
- **System Name**: Enter the name of the system that you are monitoring.
- **System Location**: Enter the physical location of the Wi-Fi Bridge/Router you are monitoring, such as “Shilshoal Marina” or “Museum of Flight”
- **System Contact**: Enter the name of the person(s) supporting this Wi-Fi Bridge/Router.
- **Current SNMP Community Settings**: To remove a community that had previously been added, you can select that setting to be removed when Make Base SNMP Changes is selected. To de-select a community, hold the Ctrl key down and click on it again.
- **Current Trap Sinks**: To remove a trap sink that had previously been added, you can select that setting to be removed when Make Base SNMP Changes is selected. To de-select a trap, hold the **Ctrl** key down and click on it again.

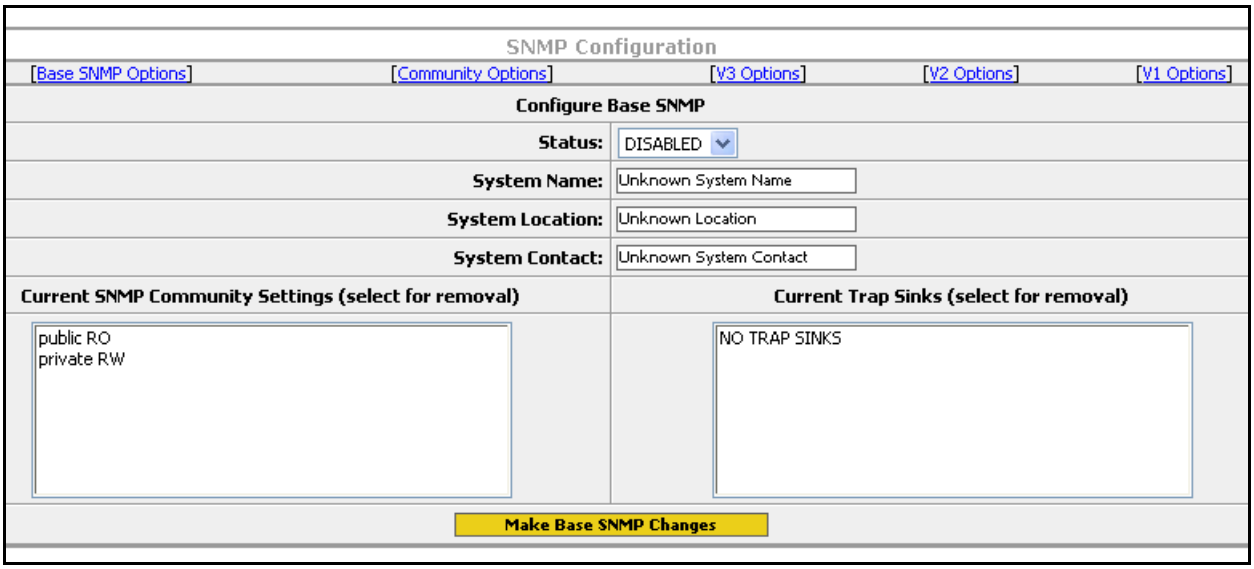


Figure 16—Base SNMP Options

Create an SNMP Community

Selecting Community Options accesses the following settings to create a new SNMP community. Settings are not configured until **Create New Community** is selected after entering your information.

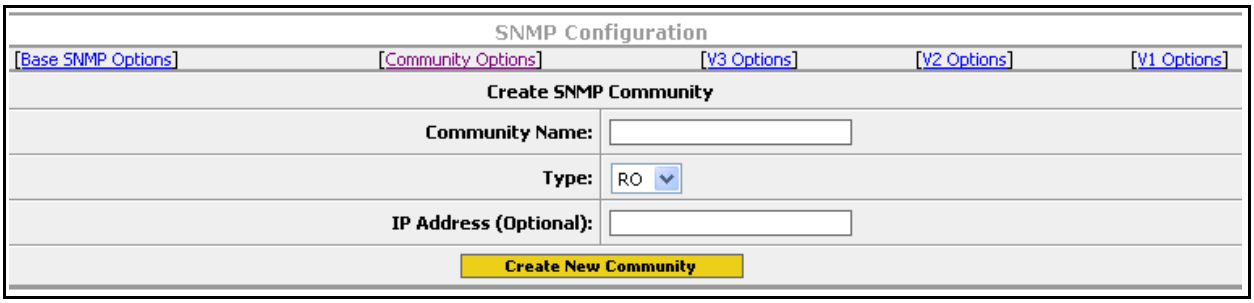


Figure 17—Create an SNMP Community

- **Community Name**: Enter the name of an SNMP community to create.
- **Type**: Specify whether to create a read only (RO) or a read/write (RW) community.
- **IP Address (Optional)**: Enter the IP address to use to access this community. If this option is used, only SNMP requests from the specified IP address are honored.

SNMP Version 3 Configuration Settings

The following settings are use to create an SNMPv3 trap sink and user.

Create an SNMP Version 3 Trap Sink

These settings are used to create an SNMPv3 trap sink. Settings do not take effect until **Create Trap Sink** is selected after entering your information.

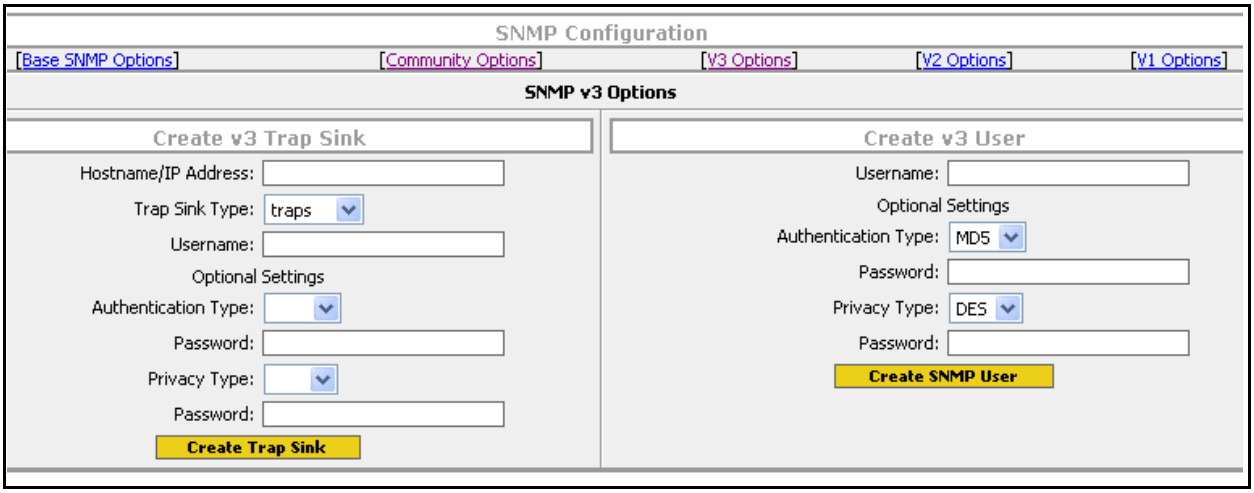


Figure 18—SNMP Version 3 Options

- **Hostname/IP Address**: Enter the host name or the IP address for creating the trap.
- **Trap Sink Type**: Specify whether to trap or to inform when a condition is detected.
- **Username**: Enter the user name.
- **Authentication Type**: Select the type of authentication: MD5 or SHA.
- **Password**: Enter the authentication password.
- **Privacy Type**: Select the encryption type to use (currently on DES is supported).
- **Password**: Enter the DES encryption password.

Create an SNMP Version 3 User

These settings create an SNMP version 3 user. Settings do not take effect until **Create SNMP User** is selected after entering your information.

- **Username**: Enter a user name.
- **Authentication Type**: Select the type of authentication to use with this user: MD5 or SHA.
- **Password**: Enter the password for this user.
- **Privacy Type**: Select the encryption type to use for this user (currently on DES is supported).

- **Password**: Enter the DES encryption password.

SNMP Version 2 Trap Sinks

The following settings are used to configure a trap or an inform for SNMP version 2. Changes do not take effect until **Create Trap Sink** is selected after entering your information.

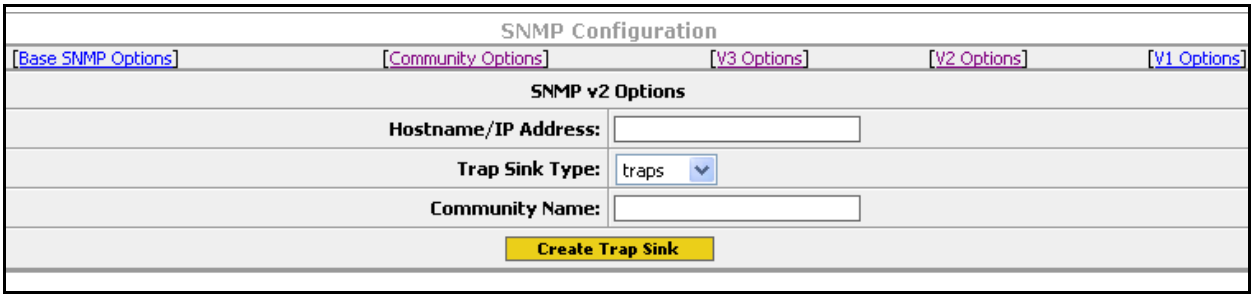
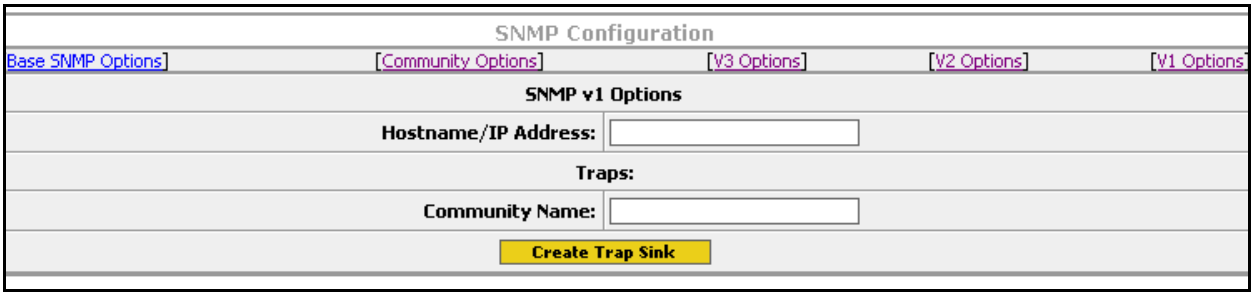


Figure 19—Creating an SNMP Version 2 Trap

- **Hostname/IP Address**: Enter the host name or the IP address for creating the trap.
- **Trap Sink Type**: Select the type of sink to create: **trap** or **inform**.
- **Community Name**: Enter the community name for the SNMP Trap to allow it to record traps from the Wi-Fi Bridge/Router.

SNMP Version 1 Traps

The following settings are used to configure a trap for SNMP version 1. Changes do not take effect until **Create Trap Sink** is selected after entering your information.



- **Hostname/IP Address**: Enter the host name or the IP address for creating the trap.
- **Community Name**: Enter the community name for the SNMP Trap to allow it to record traps from the Wi-Fi Bridge/Router.

Monitoring>Associated Clients

This table displays the number of clients that are currently associating with the Wi-Fi Bridge/Router on each wireless interface. Selecting the value displays a table of information for each client. This is helpful in understanding which clients are being serviced, the MAC address and IP address of each client, and the data rate of the connection to each client.

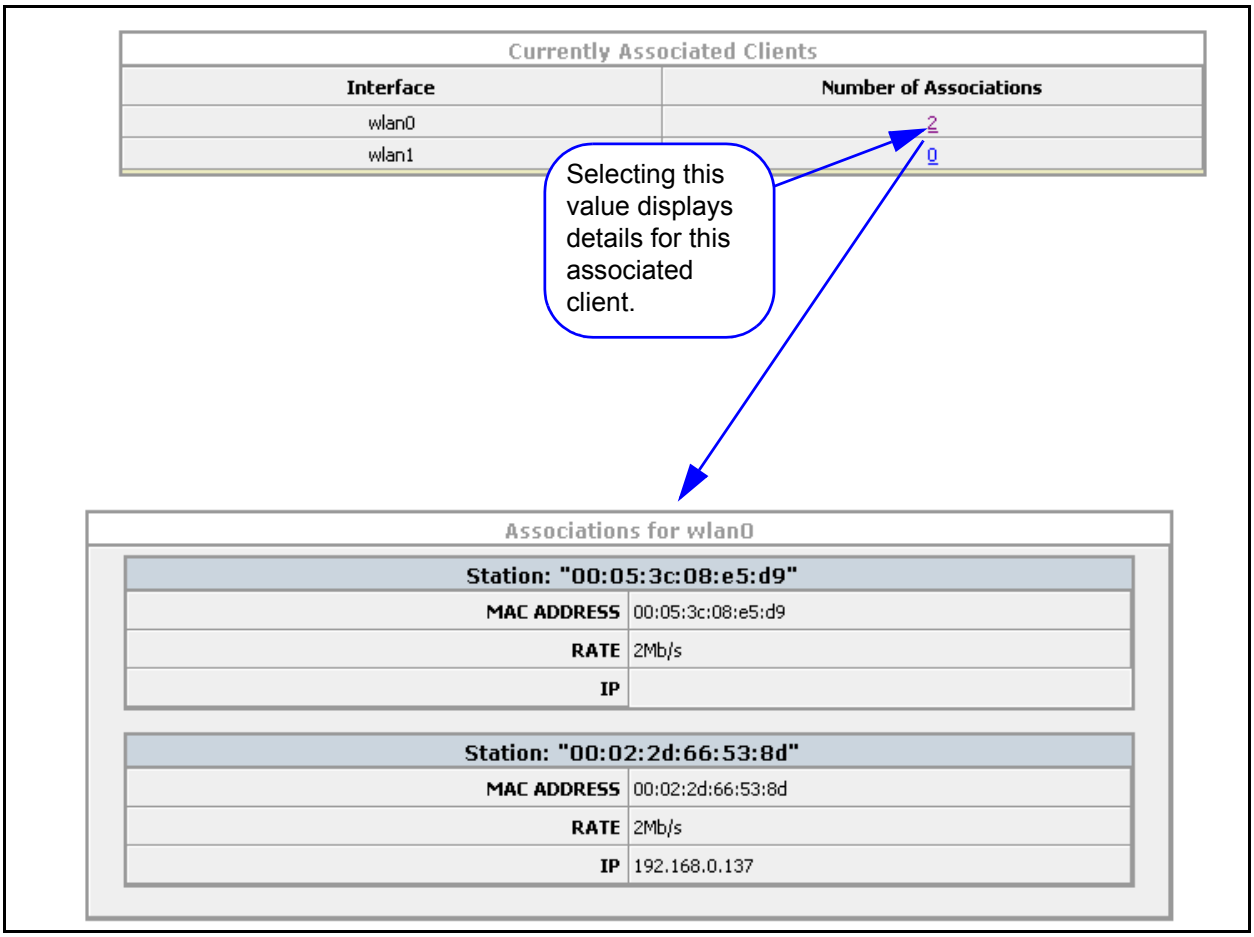


Figure 20—Example Associated Clients Information

Services, Password, Config, and Firmware Web Pages

The **System** web screens are used to view the current running configuration, enable and disable HTTP and SSH connections to the Wi-Fi Bridge/Router, change the system passwords, save and transfer configuration files, and install new firmware in the Wi-Fi Bridge/Router.

System Settings

System settings are arrange on the following configuration pages:

- **System>Summary**
- **System>Services**
- **System>Password**
- **System>Config**
- **System>Firmware**
- **System>Quick Setup**

System>Summary

This screen displays some current configuration information, such as the host name, the current firmware revision in the Wi-Fi Bridge/Router, and the web server software version. When in enable mode, the command line interface listing of the current (running) configuration is also displayed.

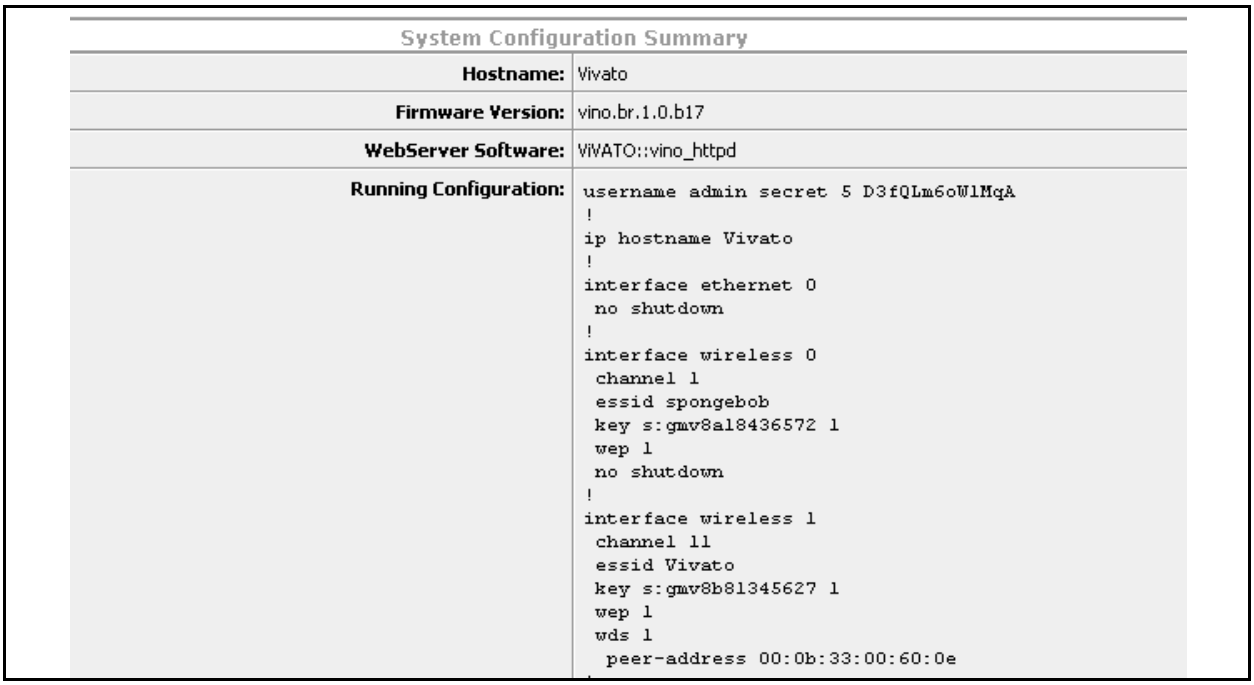
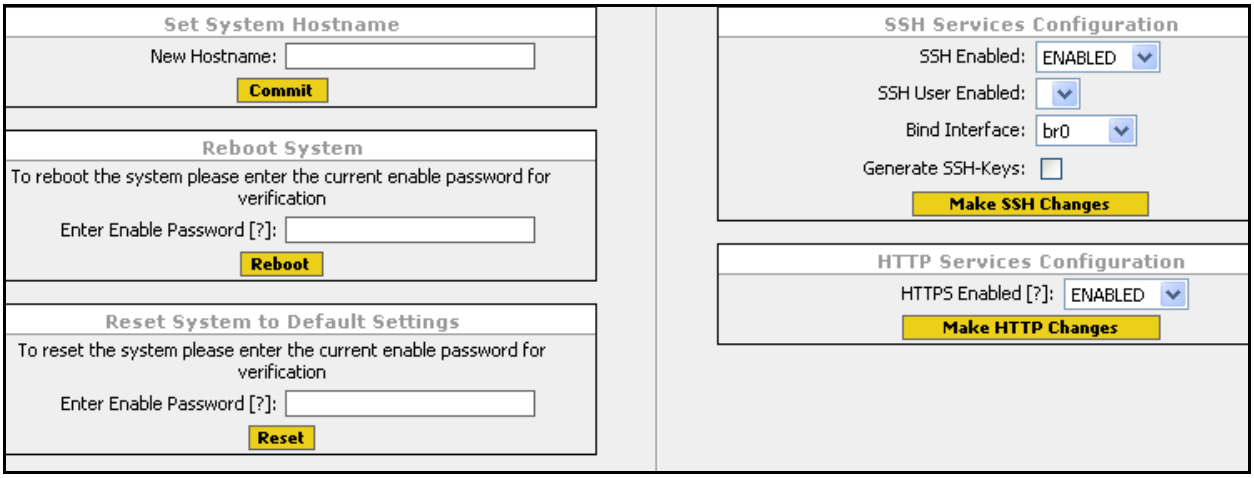


Figure 21—Example System Summary Screen

System>Services

Services lets you set or change the Wi-Fi Bridge/Router's host name, reboot the Wi-Fi Bridge/Router, return to the Bridge/Router to its default configuration, and enable or disable communications using secure shell or HTTPS protocols.



Set System Hostname

Enter a host name for the Wi-Fi Bridge/Router. The host name can also be set using the Quick Setup web pages. See **"Basic Network Setup"** on page 22.

Reboot System

Entering the enable password and selecting Reboot causes the Wi-Fi Bridge/Router to reboot using the last configuration saved as "startup-config".

Rebooting causes any unsaved configuration changes to be discarded. To preserve your current configuration, use Configuration File Options to save your configuration (see **"System>Config"** on page 60).

Reset System to Default Settings

Entering the enable password and selecting **Reset** causes the Wi-Fi Bridge/Router to reboot using the original factory configuration. This is used to clear the current settings and start with a "clean" configuration. After resetting, the default IP address (169.254.20.1) must be used to access the Bridge/Router.

This function renames the last saved configuration "startup-config.bak" and reboots the Bridge/Router. Since the Bridge/Router cannot find the "startup-config" file on reboot, it uses the initial product settings.

To use the "startup-config.bak" file to restore the last saved configuration, rename the file to "startup-config" and reboot.

Important	Reset sets the IP address of the Wi-Fi Bridge/Router to 169.254.20.1, and all other configurations are returned to their factory defaults, including disabling all security settings. See **"Steps to Configuring the Vivato Wi-Fi Bridge/Router"** on page 11to begin re-configuring the Wi-Fi Bridge/Router.

SSH Services Configuration

The secure shell (SSH) configuration effects access to the Wi-Fi Bridge/Router using a secure shell client. Changes do not take effect until **Make SSH Changes** is selected.

- **SSH Enabled**: Enable or disable the use of a secure shell to access the configuration settings.
- **SSH User Enabled**: Enable secure copy (SCP) file transfer to this Wi-Fi Bridge/Router. Users attempting to transfer files from another Wi-FI Bridge/Router to this Wi-Fi Bridge/Router must first enter “scpuser” as the user name and provide the enable password for this Bridge/Router to permit access.
- **Bind Interface**: Specify the interface on the Wi-Fi Bridge/Router to use for secure shell (SSH) access. When this feature is issued, only the IP address on that interface can be used to access the Bridge/Router through SSH. If an IP address has not been assigned to this interface, SSH access is not restricted.
- **Generate SSH-Keys**: Check this box to regenerate keys required for secure shell operation. These keys are generated whenever a new firmware image is booted for the first time, so your Wi-Fi Bridge/Router has the proper SSH keys when delivered.

HTTP Services Configuration

HTTP services configuration enables and disables the ability to access the Wi-Fi Bridge/Router’s built-in configuration web pages.Changes do not take effect until **Make HTTP Changes** is selected.

HTTPS Enabled: Enable or disable hyper-text transfer protocol secure (HTTPS) access to the configuration web pages.

System>Password

This page is used to change the passwords that let you read the current configuration and enable access to change the configuration. These are the same passwords that are configured on the Quick Setup pages. For both passwords, you need to enter the existing password once and then enter the new password twice. The new password(s) do not take effect until **Change Password** is selected for the associated password.

No enable password is set until you create it. If you did not create an enable password during the initial configuration using the Quick Setup pages, leave the "Current Password" field blank the first time you set the enable password.

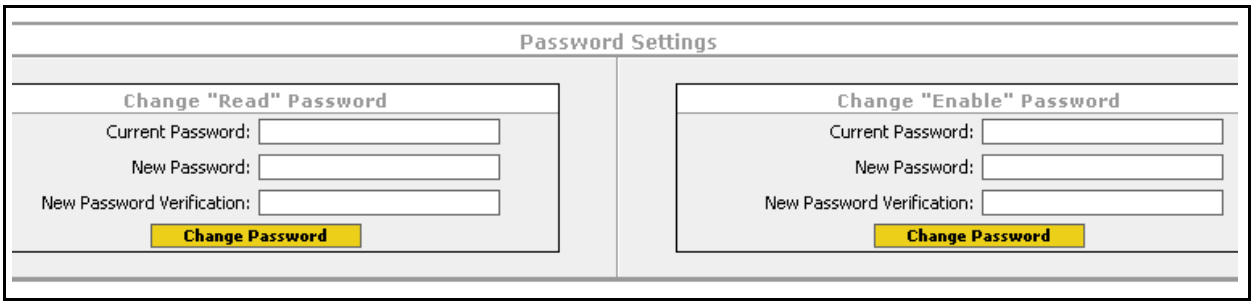
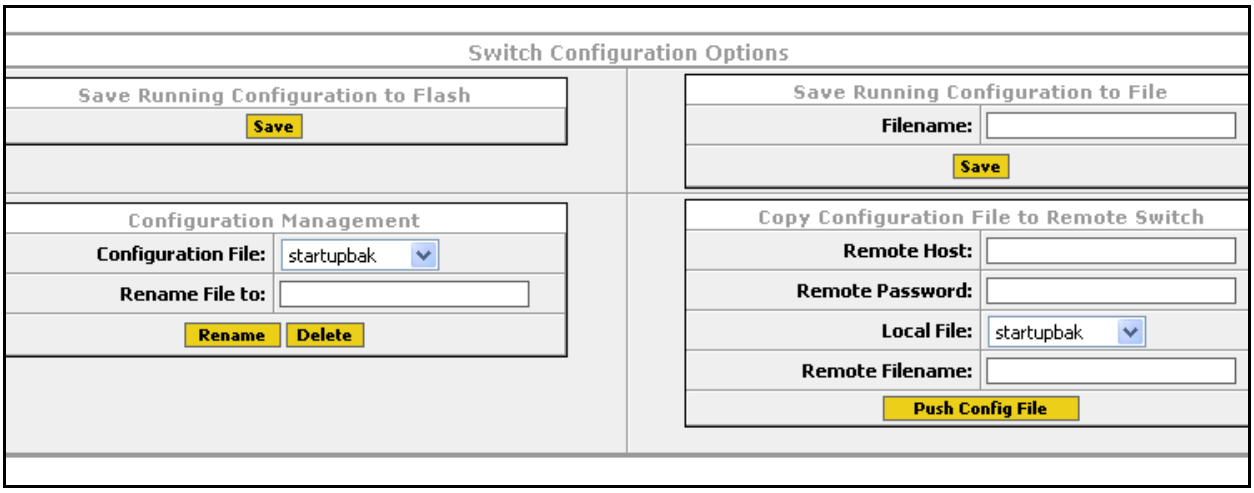


Figure 22—Changing the Read and Enable Passwords

System>Config

The Configuration page is used to save the current Wi-Fi Bridge/Router configuration for later use, rename or delete a configuration file, load a previously saved configuration, and send a configuration to a remote Wi-Fi Bridge/Router. Whenever you change configuration settings that you intend to use, you should always save those settings in your configuration file to prevent losing those changes if power to the Wi-Fi Bridge/Router is momentarily lost or if the Bridge/Router is rebooted.

The Wi-Fi Bridge/Router always uses the default configuration file entitled "startup-config" *whenever a reboot occurs*.



- **Save Running Configuration to Flash**: Save the current configuration settings as the default "startup-config" file. The next time you reboot the Wi-Fi Bridge/Router, these configuration settings are automatically used.
- **Configuration Management**: Rename or delete an existing configuration file. Multiple configuration files can be saved and retrieved for later use if desired.
  - ◊ **Configuration File**: Select the configuration file to rename or delete.
  - ◊ **Rename File To**: Enter the name to use for renaming the selected configuration file.
  - ◊ **Rename**: Select to rename the specified configuration file.
  - ◊ **Delete**: Select to delete the specified configuration file.
- **Save Running Configuration to File**: Enter a file name for saving the current configuration when **Save** is selected.
- **Copy Configuration File to Remote Switch**: These settings are used to send the configuration of this Wi-Fi Bridge/Router to another (remote) Wi-Fi Bridge/Router in order to configure it. **NOTE:** *The* **SSH User Enabled** *function of the* **SSH Services Configuration** *must be enabled on the remote Bridge/Router before it will accept the configuration file.*
  - ◊ **Remote Host**: Enter the host name or IP address of the remote Wi-Fi Bridge/Router.
  - ◊ **Remote Password**: Enter the read level password for the remote Bridge/Router.
  - ◊ **Local File**: Select the file to transfer to the remote Bridge/Router.
  - ◊ **Remote Filename**: Enter the name to use for storing the configuration file on the remote Bridge/Router.
  - ◊ **Push Config File**: Send the configuration file to the remote Bridge/Router.

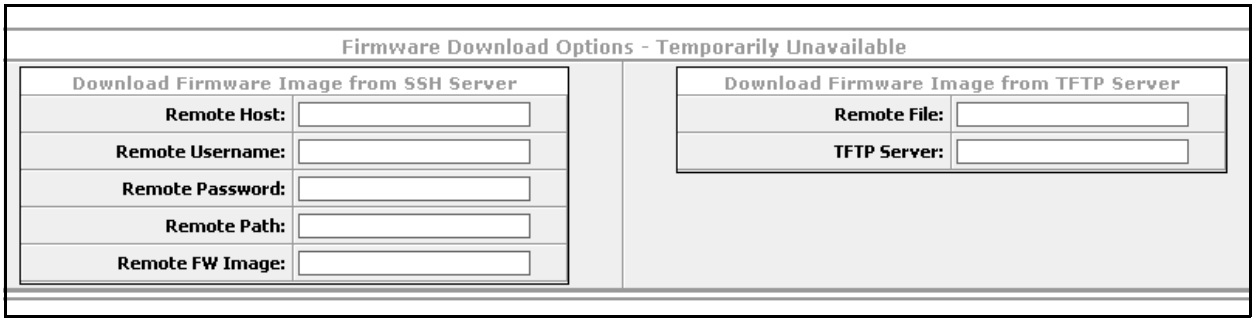
System>Firmware

(Firmware Updates Using the Web Interface Are Not Supported in This Firmware Release - Use the Command Line Interface for Updating Firmware. See "Commands for Managing Configuration Files" on page 85.)

The firmware in the Wi-Fi Bridge/Router determines which features are available and how they operate. As improvements to the firmware are developed by Vivato, the newer version can be loaded into your Wi-Fi Bridge/Router to provide new features and increase performance.

Images are saved as binary (.bin) files.

The following functions are used to manage the firmware in your Wi-Fi Bridge/Router.



Local Firmware Options

Local Firmware Options are used to load and manipulate firmware images for the Wi-Fi Bridge/Router to which you are connected.

Download Firmware Image From TFTP Server

This function is used to download a new firmware image from a TFTP server to the Wi-Fi Bridge/Router.

- **Remote File**: Enter the file name of the firmware image that you want to download.
- **Save File To Flash as**: Enter the name to use when saving the firmware image on the Wi-Fi Bridge/Router.
- **TFTP Server**: Enter the host name or IP address of the TFTP server where the firmware file resides.
- **Download**: Download the firmware file to the Wi-Fi Bridge/Router's flash memory.

Important	**DO NOT INTERRUPT THE COPYING PROCESS!**
	The Bridge/Router can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the Bridge/Router to operate.

Download Firmware Image From SSH Server

This function is used to download a new firmware image from a secure server to the Wi-Fi Bridge/Router.

- **Remote Host**: Enter the host name or IP address of the server where the firmware file resides.
- **Remote User Name**: Enter a user name configured on the remote server.
- **Remote Password**: Enter the password for the entered user name.
- **Remote Path**: Enter the directory path for the image to download, using the format in the following example: **//vivato/bridge_router/firmware_images**
- **Remote FW Image**: Enter the file name of the firmware image (.bin file) that you want to download.
- **Download**: Download the firmware file to the Wi-Fi Bridge/Router's flash memory.

Important	**DO NOT INTERRUPT THE COPYING PROCESS!** The Bridge/Router can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the Bridge/Router to operate.

System>Quick Setup

Displays the initial Quick Setup screen to access the quick setup pages and make any changes. See **"Steps to Configuring the Vivato Wi-Fi Bridge/Router"** on page 11.

Diagnostics and Help Web Screens

A **Diagnostics** web page is available to troubleshoot communications problems, and a **Help** link is provided to access the Vivato home page.

Diagnostics

Diagnostics settings are used to verify and troubleshoot packet transfer between the Wi-Fi Bridge/Router and connected networks.

Diagnostics>Tools

The Ping and Traceroute functions are used to verify access to selected hosts and to see the route used to access them.

Ping

Pinging tests to see if you can communicate with another device on the network. Packets are sent to the device, which in turn responds by sending return packets if communication is successful. If communication fails, an "unknown host" message is displayed or the command times out with no reply. An example successful ping result is shown below.

- **Host**: Enter the IP address or host name for the device you are trying to access. When specifying the host name, the name and IP address must first be entered into the Wi-Fi Bridge/Router's host table. See **"Create a New Host"** on page 35.
- **Ping Count**: Select the number of 64-byte packets to send during the pinging operation.
- Start Ping: Ping the specified host.

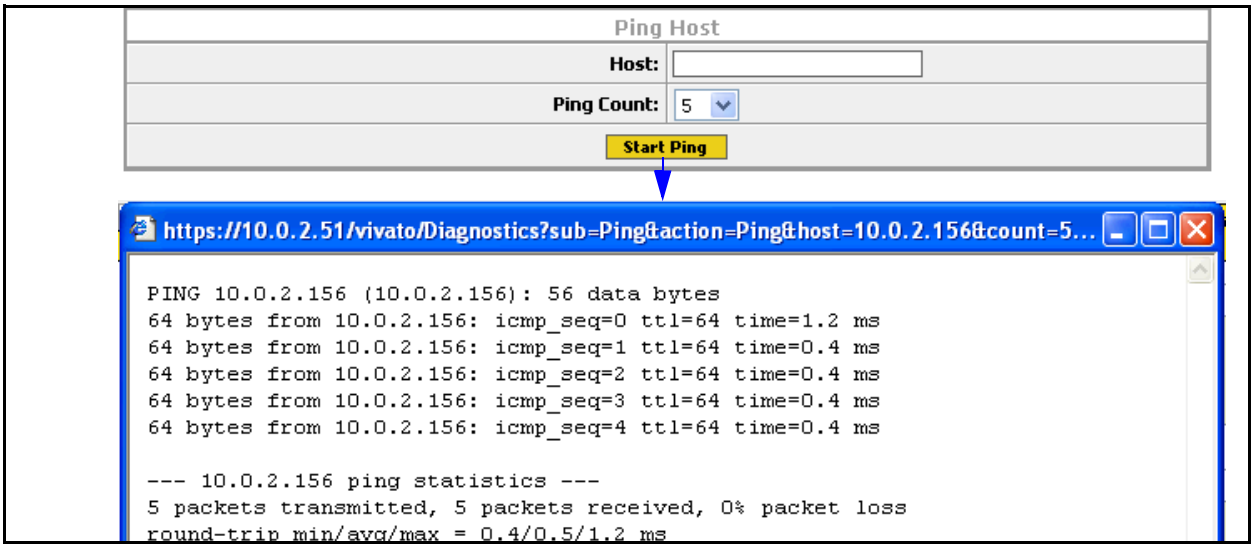
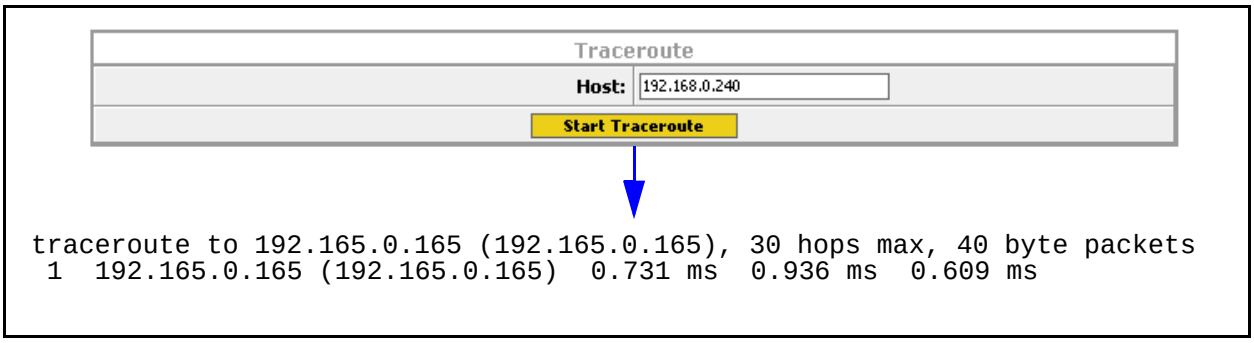


Figure 23—Example Results of Pinging a Host With Five Packets

Traceroute

Traceroute displays the IP addresses of devices used to access a device at a specified destination IP address or host name, the size of the packets transmitted, and the amount of time used for each "hop" between network devices.



Diagnostics>Arp

Address resolution protocol (ARP) associates a device's IP address with its unique hardware medium access control (MAC) address. When the Wi-Fi Bridge/Router sends an ARP request for a specific IP address, the MAC of the device with that address is returned and is entered into the ARP Information table (see below).

ARP Information

IP Address	Type	Flags	Hardware Address	Mask	Interface
192.165.20.4	ARPA	0x2	00:09:6B:10:5A:C6	*	br0
192.165.20.45	ARPA	0x2	00:50:70:52:0B:14	*	br0

Help

Selecting the **Help** tab causes the Wi-Fi Bridge/Router to access the Vivato Customer Support sign-in screen. After entering your Customer Support user name and password, you can access a variety of support information and firmware downloads for your Wi-Fi Bridge/Router.

Configuration Using The Command Line Interface

Refer to **"Default Configuration"** on page 12 before performing additional configuration using the CLI.

Refer to the *CLI Quick Reference.pdf* file on the Vivato CD-ROM for a concise listing of all CLI commands.

The command line interface (CLI) is used to change settings and query values in the Vivato Wi-Fi Bridge/Router; it is an alternative to using the web page interface. The CLI can be used to initially configure the Wi-Fi Bridge/Router for operation and to update the configuration after installation. Configuration files can be saved and retrieved to backup the configuration or to reconfigure the Bridge/Router. The CLI can also be used to monitor activity during Bridge/Router operation. Passwords are used to prevent unauthorized access to the CLI.

Caution 

To prevent unauthorized access to the Bridge/Router's configuration, the system administrator should use the **enable secret [<password type (0|5)>] <password text>** and **username admin secret [<password type (0|5)> <password text>** commands to set and save new passwords before putting the Bridge/Router into service.

Understanding How the CLI is Used

Command Descriptions

Command Levels

The commands are arranged in a hierarchical structure. The top level is the "**read"** level. Read level commands access system information and utilities used to monitor the overall status of the Bridge/Router and perform some troubleshooting operations.

The second command level is the "**enable"** level**.** Enable level commands are used to configure the Bridge/Router. Almost every function in the Vivato Wi-Fi Bridge/Router can be accessed using these commands. The enable level is accessed when you enter the **enable** command at the read level prompt. An additional password is required to access the enable level commands. Enable level commands are arranged in a number of sub-levels for configuring specific operations.

Important	Configuration changes are not saved until you issue the **write network flash:** or **write [memory]** command. Turning the Wi-Fi Bridge/Router off causes the last saved configuration to be used when power is restored. If power is interrupted before saving your changes, those changes are lost.

Connections and Terminal Settings

Commands can be entered on a computer using either of following methods:

- Running a Secure Shell (SSH) session configured for TCP/IP, and connected to the Wi-Fi Bridge/Router's Ethernet port (use the supplied crossover cable when connecting the Bridge/Router directly to your computer's network interface card). Use the Bridge/Router's IP address when configuring communications. The default IP address when shipped is 169.254.20.1, which is assigned to the default bridge: br0. The user name is "admin" and the password is "vivato". Your network interface's IP address must be set to be able to work with the Wi-FI Bridge/Router. See **"Enabling Your Computer's Network Adapter to Access the Wi-Fi Bridge/Router"** on page 13.
- Running a terminal emulator and connecting to the Bridge/Router's RS-232 serial (console) port with the supplied DB-9 null modem cable.

Emulating a VT100 terminal with the following settings typically works well:

- Baud: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Xon/Xoff

If the **vivato** prompt does not appear immediately after starting your terminal emulator, press the **Enter** key on your computer a few times to get a prompt. If no prompt appears, check your cable connections and terminal emulator settings.

Accessing the CLI

After connecting the Bridge/Router to your computer and initiating communications, a command prompt should be displayed on your computer. The following example illustrates how to access the read level using the SSH Secure Shell© client:

1. Using the Quick Connect feature of the secure shell client, enter the IP address of the Wi-Fi Bridge/Router and enter "**admin**" for the user name, and select **Connect** to begin the session.
2. Enter the read level password . The password is not displayed as you enter it.

   Note: Until you change it, the password is **vivato**.
3. If you enter a question mark at the prompt, a list of the available read level commands is displayed (as shown in the example below).

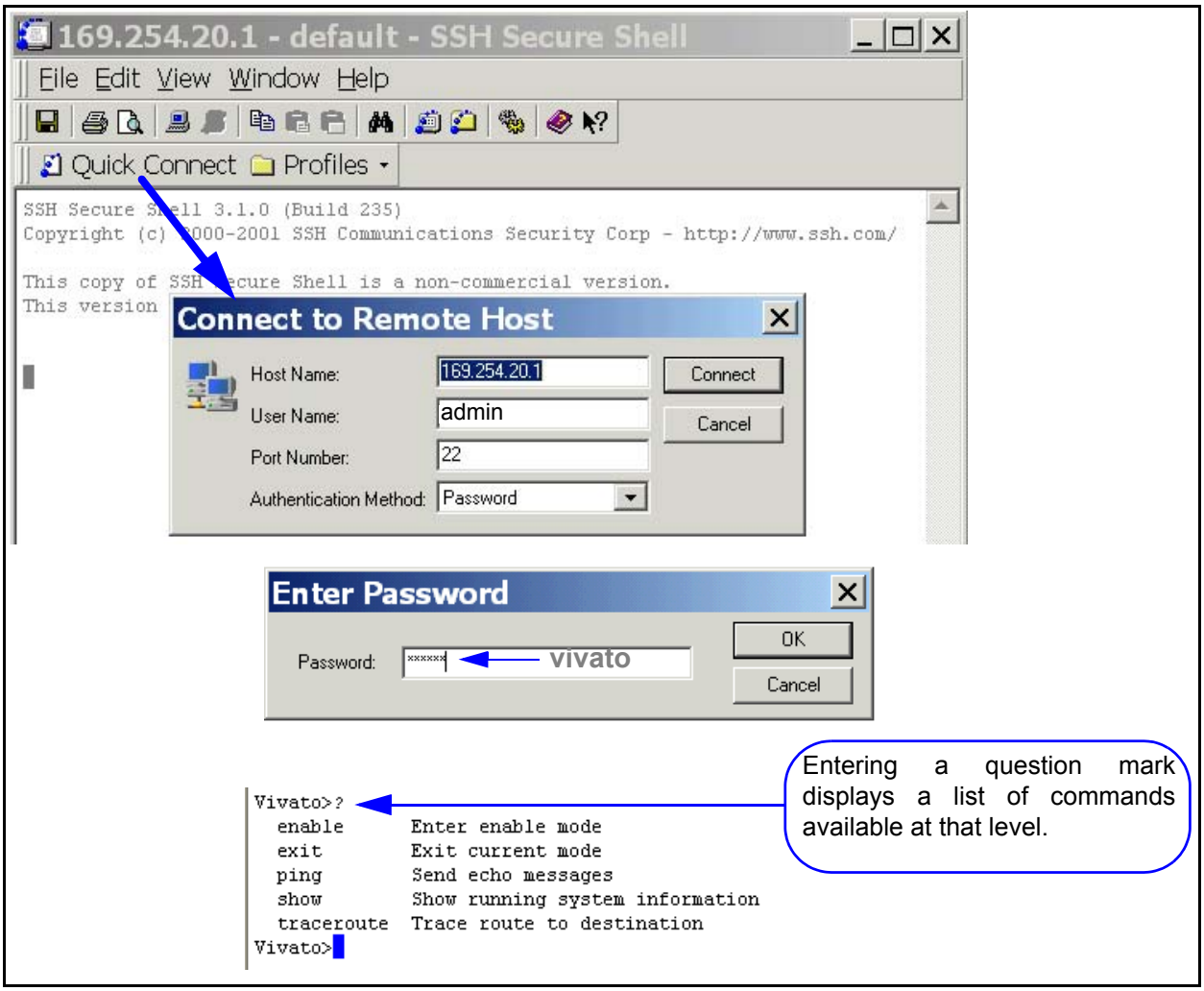


Figure 24—Using Secure Shell to Access the CLI and Display Read Level Commands

Accessing the Configuration Level

Use the following steps to access the enable level from the read level, and then access the global level of the configuration settings:

1. At the **vivato>** prompt, enter **enable**.
2. The Wi-Fi Bridge/Router is shipped without an enable password. If you have created an enable password (when using the Quick Setup web pages or by using the CLI), enter that password when prompted.
3. Enter **configure terminal** to access the global configuration level. The prompt changes to **vivato (config)#**. At this point you can start configuring the Wi-Fi Bridge/Router.

```
Vivato>
Vivato>enable
Password:
Vivato#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Vivato(config)#
```

Figure 25—Accessing the Global Configuration Level

Configuration Example

This example configures the Wi-Fi Bridge/Router as an access point using WEP security. Some settings are already provided in the default configuration, but are shown here to illustrate how they are set.

Change settings as needed for your desired configuration. The example begins at the initial command prompt:

login: **admin**	Enter the user name.
password: **vivato**	Enter the default read password.
vivato> **enable**	Enter the enable mode.
vivato# **configure terminal**	Enter the configuration mode.
vivato (config)# **interface wireless all**	Configure all wireless interfaces (wlans).
vivato (config-wlan-all)# **essid jims_java**	Set ESSID to “jims_java”.

Configure WEP security

vivato (config-wlan-all)# **key s:jimsgr8coffee 1**	Enter a 104-bit WEP key 1 as a string.
vivato (config-wlan-all)# **wep 1**	Enable WEP operation using key #1.
vivato (config-wlan-all)# **exit**	Stop configuring all wlans together.

Configure the wireless interfaces to provide one channel operation (default).

vivato (config)# **interface wireless 0**
vivato (config-wlan0)# **channel 1**
vivato (config-wlan0)# **exit**
vivato (config)# **interface wireless 1**
vivato (config-wlan1)# **shutdown**
vivato (config-wlan1)# **exit**

Create the default bridge (br0), and add each Ethernet and wireless interface to the bridge.

vivato (config)# **interface bridge br0**
vivato (config-br0)# **add interface ethernet 0**
vivato (config-br0)# **add interface wireless 0**
vivato (config-br0)# **add interface wireless 1**
vivato (config-br0)# **no shutdown**

Specify the IP address and netmask for bridge 0 (br0). This sets the IP address for the Wi-Fi Bridge/Router in your network.

vivato (config-br0)# **ip address 192.165.0.10 255.255.255.0**
vivato (config-br0)# **exit**

Generate the secure shell key and enable the secure shell daemon (default).

vivato (config)# **ip ssh genkey**
vivato (config)# **ip ssh server**

Enable the HTTP daemon for web access (default).

vivato (config)# **http-server**

Define the basic network settings

vivato (config)**# ip domain-name javaplanet** Set the domain name to “javaplanet”.
vivato (config)# **ip routing** Enable global IP routing.
vivato (config)# **ip name-server 192.165.0.99** Specify a name server on your LAN.
vivato (config)# **ip hostname french_roast** Set the host name to “french_roast”

Set the read and enable passwords. After an enable password has been specified, you will need to enter that password anytime you attempt to access the enable level.

french_roast (config) **username admin secret coffeem8** Set read level password.
french_roast (config) **enable secret sixty6flavors** Set enable level password.

Save the configuration inside the Wi-Fi Bridge/Router (as “startup-config”) and end the configuration session.

french_roast (config)# **exit**
french_roast# **write**
french_roast# **exit**

Navigating the CLI

Several keystroke sequences are available to move between levels on the CLI and move the cursor on the command line, and to get helpful information online.

Moving the Cursor Around on the Command LIne

You can use the following commands to move the cursor on the command line when making changes to settings:

Table 1—Command Line Shortcuts

Keystrokes	Function
Ctrl-B or left arrow key*	Moves the cursor back one character without erasing the character.
Ctrl-F or right arrow key*	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Ctrl-U	Removes all text on the command line.
* The arrow keys may not work with some terminal emulators.	

Using the “?” to Get Online Command Help

At any prompt on the command line you can enter a question mark (?) to get a list of the available commands at that level, along with a short description of each command. This can be helpful when you enter a command and get an “Invalid command due to syntax or parameter” error.

To get information on a specific command, such as the format of the command or additional specifiers used by that command, type the command, a single space, and then the question mark. For example: **enable**<space>**?** displays information on the enable commands.

Using the Tab Key to Complete a Command

Instead of individually keying-in every character of a command, you can enter the first few characters and press the **Tab** key to automatically fill in the remainder of that command. For example, to enter the "show running-configuration" command, you could enter "sh **Tab** ru **Tab"**. This feature increases the rate at which you can enter commands, and often reduces the number of keystroke errors.

Command Mode Access and Prompts

The following table lists the various commands and keystrokes used to access the main command levels:

Table 2—Command Mode Navigation

Command Level	How to Access	Resulting Command Line Prompt	To Go Back to the Previous Level
Read	Default state.	**vivato>**	
Enable	From the read level, enter **enable** and the enable password	**vivato#**	Type "disable".
Enable (Global Configuration)	From the Enable level, enter **configure terminal**	**vivato (config)#**	Type "exit".
Configure Specific Functions	At the global configuration prompt, enter the appropriate configuration command. For example, entering **interface ethernet 0** accesses the configuration settings for the ethernet 0 port.	Depends on the configuration function. For configuring the wireless interface, the prompt would be **vivato (config-eth0)#**	Type "exit" to return to the global configuration prompt. You also enter **Ctrl-z** to exit the global configuration mode are return to the initial enable prompt.

Command Conventions

Use the following conventions when entering commands and to understand the command listing used in this manual.

Entering Commands on the Command LIne

Most commands are entered using lower case letters, such as **configure terminal**. Do not substitute upper case letters, such as CONFIGURE TERMINAL or Configure Terminal. When upper case letters are shown in the command listing, use the upper case letters where indicated.

Reading the Command LIsting

Command list headings with initial upper case letters identify a group of related commands that are listed under it. For example, **Configure Interface Commands** is the heading for the list of all of the commands that are used to configure the ethernet and wireless interfaces. The actual commands used to configure the interfaces are listed under this heading using all lower case letters (such as **interface wireless**).

Entering Variables

Some commands only perform an immediate action (such as the **enable** command) or always require text or a number to be entered (such as the **interface wireless** command). It is assumed that you press the **Enter** key after typing in these commands .

Some commands may use a default of just pressing **Enter** after issuing the command, but also provide the use of specifying a file name or other text. These commands are listed in both forms, such as **write** and **write file <filename>**.

Optional Entries

Some commands use optional specifiers or entries. These are indicated by using brackets, **[ ],** in the command listing. For example, the following command contains optional entries:
snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth MD5|SHA <password> [priv DES <password>]]

Read Level Command Descriptions

The following commands are available at the read level.

enable

Enter the enable mode. This command must be issued any time you are going to change any Bridge/Router configuration settings. The enable password is required before access to configuration settings is allowed.

exit

Exit the configuration session to stop using the command line interface.

Ping

Send an echo message to another device. Pinging a device is used to see if you can communicate with a device at a specified IP address or that has a local host name. A packet is sent to the device, which in turn responds by sending return packets if communication is successful. If communication fails, an “unknown host” message is displayed or the command times out with no reply.

Ping commands are available at both the read and enable levels.

ping <ipaddress|hostname>

Specify the IP address to ping using 5 packets.

ping flood <ipaddress|hostname>

Specify the IP address or host name of a device to ping without waiting for a response before sending each packet. Packets are sent continuously as fast as possible until you press **Ctrl-C** on your computer. *This command should be used with caution, since it causes a very high level of network traffic while executing.*

ping flood

Enter this command to ping a host computer named “flood”.

ping flood count <1-100000> <ipaddress|hostname>

Specify the IP address or host name of a device to ping, and the number of packets to send, without waiting for a response before sending each packet. Packets are sent as fast as possible until the count has elapsed or until you press **Ctrl-C** on your computer.

ping count <1-100000> <ipaddress|hostname>

Specify the number of packets to use, and the IP address or host name, to ping a device. The Wi-Fi Bridge/Router waits for a reply from the host after each packet is sent before another packet is sent.

ping count <1-100000> flood <ipaddress|hostname>

Specify the number of packets to send, and the IP address or host name of a device, to ping without waiting for a response before sending each packet. Packets are sent as fast as possible until the count has elapsed or until you press **Ctrl-C** on your computer.

Show Commands

Show commands display system information. Some Show commands are available at the read level, but all show commands are available at the enable level.

Some commands, such as “show interfaces”, may display more than one page of information on your screen. To view all of the contents, you may need to use the Shift+PageUp and Shift+PageDown keys.

Read Level Show Commands

The following Show commands are available at the read level:

show arp

Displays a list of the IP addresses and the corresponding medium access control (MAC) addresses for associated devices using address resolution protocol (ARP).

```
Vivato#show arp
IP address      HW type    Flags      HW address          Mask     Device
195.145.0.240    0x1        0x2        00:09:6B:8C:2D:F2    *        br0
195.145.0.99     0x1        0x2        00:50:70:52:0B:14    *        br0
195.145.0.107    0x1        0x2        00:09:6B:10:5A:C6    *        br0
195.145.0.57     0x1        0x2        00:02:2D:66:53:8D    *        br0
Vivato#
```

Figure 26—Example “show arp” Output

show cpu

Displays central processor unit information.

show dhcp-server interface bridge <0-4094>

Enter the bridge number to display the DHCP settings for that interface.

```
Vivato#show dhcp-server interface bridge 0
DHCP status for br0:
  ip-pool 192.163.0.20 192.163.0.100 255.255.255.0
  broadcast-address 192.163.0.255
  gateway 192.163.0.199
  name-server 192.163.0.198
  ntp-server 192.163.0.197
  lease 36000
  domain-name vivato
  status UP
Vivato#
```

Figure 27—Example “show dhcp-server interface bridge 0” Output

show dhcp-server interface ethernet <0>

Display the DHCP settings for the Ethernet interface.

show dhcp-server interface wireless <0-1>

Enter the wireless interface number to display the DHCP settings for that interface.

show http-server

Displays the state of the http daemon: enabled or disabled.

show interfaces

Displays information about bridge, ethernet, and wireless interfaces, including their MAC addresses, IP addresses, and packets transmitted and received through each interface.

show interfaces bridge [0-4094]

Displays the configuration of all or (optionally) a specific bridge, including the IP and MAC addresses for that bridge, the transmit and receive statistics, whether spanning tree protocol (STP) is enabled, and which interfaces are part of each bridge.

Also shown is the status of that interface. When the interface is enabled, "**UP** BROADCAST RUNNING MULTICAST" is displayed. If the interface is disabled, the "UP" part is removed ("BROADCAST RUNNING MULTICAST").

The Bridge ID consists of 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 Wi-Fi Bridge/Router 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 Bridge/Routers are used in a network. If the priority setting of all bridges is the same, the lowest MAC address is used to determine priority.

For information on RX and TX packet statistics, see **show interfaces wireless <0-1>**.

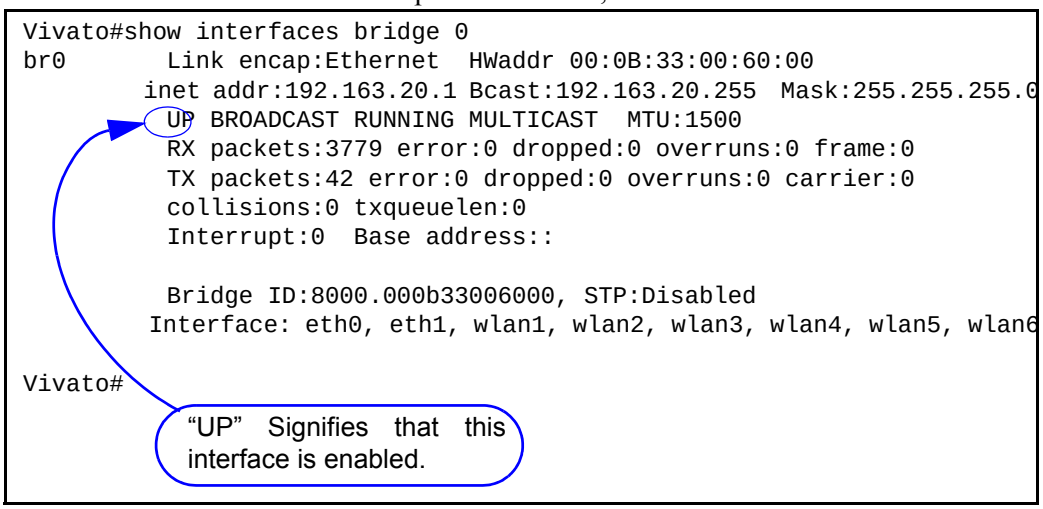


Figure 28—Example "show interfaces bridge" Output

show interfaces bridge <0-4094> fdb

Enter the number of a bridge to display the source MAC addresses of packets that have been forwarded through that bridge over any of its interfaces; also called the forwarding data base.

The length of time that the data is stored in that data base is determined by the **aging-time <10-1000000 seconds>** command. A "local" device indicates an interface that is part of this bridge.

```
Vivato#show interfaces bridge 0 fdb
br0:
port no mac addr                is local?       ageing timer
1     00:09:6b:e0:9e:bf       no                 7.59
1     00:09:7c:45:5b:8f       no                 0.27
1     00:0b:33:00:60:00       yes                0.00
2     00:0b:33:00:60:01       yes                0.00
3     00:0b:33:00:60:09       yes                0.00
```

Figure 29—Example "show interfaces bridge 0 fdb" Output

show interfaces bridge <0-4094> stp

Enter the number of a bridge to display the status of spanning tree protocol (STP) on that bridge: enabled or disabled.

show interfaces ethernet [0]

Displays the configuration for the ethernet interface, including the IP address (if assigned) and broadcast address, MAC address (HWaddr), bridges that this interface is part of, and transmit and receive packet statistics.

Also shown is the status of that interface. When the interface is enabled, "**UP** BROADCAST RUNNING MULTICAST" is displayed. If the interface is disabled, the "UP" part is removed ("BROADCAST RUNNING MULTICAST").

For information on RX and TX packet statistics, see **show interfaces wireless <0-1>**.

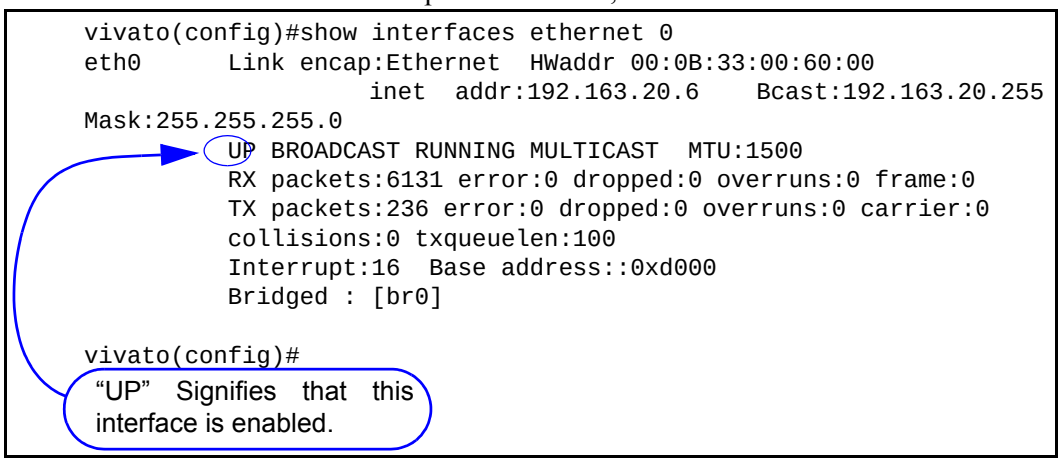


Figure 30—Example "show interfaces ethernet" Output

show interfaces wireless [associations]

Displays the configuration of all wireless interfaces or, optionally, information about clients associating through all wireless interfaces.

Configuration information includes the ESSID and WEP encryption key value (if used), channel assignment, association with any bridges, and bit rate for each wireless interface. See **Figure 31—Example "show interfaces wireless 1" Output**, for an example of what is displayed for each interface.

show interfaces wireless <0-1> associations

Displays information about clients associating through the specified wireless interface, including the MAC address, connection rate of the last packet received, and the IP address of the client.

```
Vivato#show interfaces wireless 0 associations
Associations on wlan0:
1    00:02:2d:66:53:8d  2Mb/s  192.168.0.118

Vivato#
```

WDS connection information is not included (see **show interfaces wireless < 0-1> wds <1-6>**.

show interfaces wireless <0-1>

Displays the configuration and operating statistics of a specified wireless interface.The following information is reported:

- Link encpap: Ethernet - Always indicates Ethernet packet encapsulation is used.
- HWaddr: The MAC address for this wireless interface.
- UP BROADCAST RUNNING MULTICAST - Displayed when this interface is up (not shut down).
- BROADCAST MULTICAST - Displayed when this interface is shut down.
- MTU 1500: The maximum transmission unit (MTU) is the maximum number of bytes sent per packet on this interface. This value is fixed at 1500.
- RX packets: The total number of frames received on this interface since the Wi-Fi Bridge/Router was last booted. The following received packet statistics are also displayed:
  - error: The number of frame check sequence (FCS) errors in received frames. This value includes errors detected in ALL packets received on that interface, whether they are from an intended client or broadcast from another source. In an environment with several clients or other Wi-Fi devices, this number can seem larger than expected, but it does not necessarily indicate a problem with this wireless interface or the intended clients.
  - dropped: The number of frames that were not buffered and were discarded, not counting WEP and WEP ICV errors.
  - overruns and frame: Not used at this time.
- TX packets: The total number of frames transmitted on this interface since the Wi-Fi Bridge/Router was last booted. The following transmitted packet statistics are also displayed:
  - error: The number of transmission retries that exceeded the retry limit.
  - dropped: The number of packets that have been discarded.
  - overruns and carrier: Not used at this time.
- Interrupt and Base address: Internal hardware interface settings.
- Bridged: Displays the bridge (if any) that this interface is part of.
- Essid: The extended service set identifier for this interface.
- Beacon Essid: Enabled or disabled. See **"disable beacon-essid"** on page 99.
- Channel: The channel that this interface is using to transmit and receive.
- Access Point: See HWaddr above.

- Bit Rate: This is the maximum bit rate supported on this interface. This value cannot be changed.
- Beacon Interval: See **"beacon-interval <0-8191>"** on page 98.
- Sensitivity: See **"sensitivity <1-3>"** on page 101.
- Encryption key: “Off” means that WEP is disabled. “XXXX” means that WEP is enabled and the “Encryption mode:” is set to restricted.
- RX invalid nwid, invalid crypt, RX invalid frag, Tx excessive retries, and Invalid misc, are not used at this time.

```
Vivato#show interfaces wireless 1
wlan1     Link encap:Ethernet  HWaddr 00:0B:33:00:60:09
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:23 error:553 dropped:0 overruns:0 frame:0
          TX packets:1228 error:54 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:21  Base address::0xd140
          Bridged : [br0]

          Essid:tripacer
          Beacon Essid: Enabled
          Channel:1  Access Point:00:0B:33:00:60:09
          Bit Rate:11Mb/s
          Beacon Interval: 0  Sensitivity:0
          Encryption key:XXXX   Encryption mode:restricted
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:0
Vivato#
```

Figure 31—Example “show interfaces wireless 1” Output

show interfaces wireless < 0-1> wds <1-6>

Enter the wireless interface number and wireless distribution system (WDS) port number to display that WDS configuration and operating statistics. The “HWaddr” shown is the MAC address that is automatically assigned for spanning tree protocol operation on that wireless interface and port. See **show interfaces wireless <0-1>** for a description of the other reported values.

The following example shows the WDS settings for wireless interface 1, port 2:

```
Vivato#show interfaces wireless 1 wds 2
wds1-2    Link encap:Ethernet  HWaddr 00:0B:33:31:80:09
          BROADCAST MULTICAST  MTU:1500
          RX packets:25 error:897 dropped:0 overruns:0 frame:0
          TX packets:1673 error:78 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:21  Base address::0xd140
          Bridged : [no]

Vivato#
```

show ip domainname

Displays the domain name for the Wi-Fi Bridge/Router.

show ip host

Displays the host table for the Wi-Fi Bridge/Router, containing host names and their IP addresses.

show ip hostname

Displays the host name for the Wi-Fi Bridge/Router.

show ip nameserver

Displays the IP address for any name servers that have been specified using the **ip name-server <ipaddress>** command.

show ip route

Displays IP routing information for the Wi-Fi Bridge/Router. Routes determine how packets with IP addresses within specified subnets are directed.

In the example below, host 145.88.47.9 can be accessed through gateway 195.145.3.150, by way of interface br0. All hosts on the 195.145.0.0 network can be accessed directly through interface br0. Destination 127.0.0.0 is the local host. The 127.0.0.0 route is the local host loop-back route. The flags “U” and “G” stand for “up” (status of the route) and “gateway ”, respectively.

Table 3—Example IP Routing Information

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
145.88.47.9	195.145.3.150	255.255.255.0	UG	0	0	0	br0
195.145.0.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo

show ip ssh

Displays the state of the secure shell (SSH) daemon: enabled or disabled. If SSH operation has been bound to a particular interface using the **ip ssh bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>)** command, that interface is also listed.

show logging

Displays a list of locally logged system events if logging has been enabled.

show memory

Displays information about installed memory and memory usage in the Bridge/Router.

show serial

Displays the product serial number.

show snmp-server

Displays simple network management protocol (SNMP) server status and configuration, such as the name, location, contact name, public and private community names, and host IP addresses.

```
harvey(config)#show snmp-server
snmp-server contact george
snmp-server location upstairs closet
snmp-server name clydesdale
snmp-server community public RO
snmp-server community private RW
snmp-server community icehouse RW 192.163.20.1
snmp-server engineID A52D
snmp-server
!
harvey(config)#
```

Figure 32—Example "show snmp-server" Output

show uptime

Displays the of day, how long the Bridge/Router has been up since it was last rebooted (days, hours, minutes), the number of users that have accessed the Bridge/Router, and the average load through the Bridge/Router**.**

show version

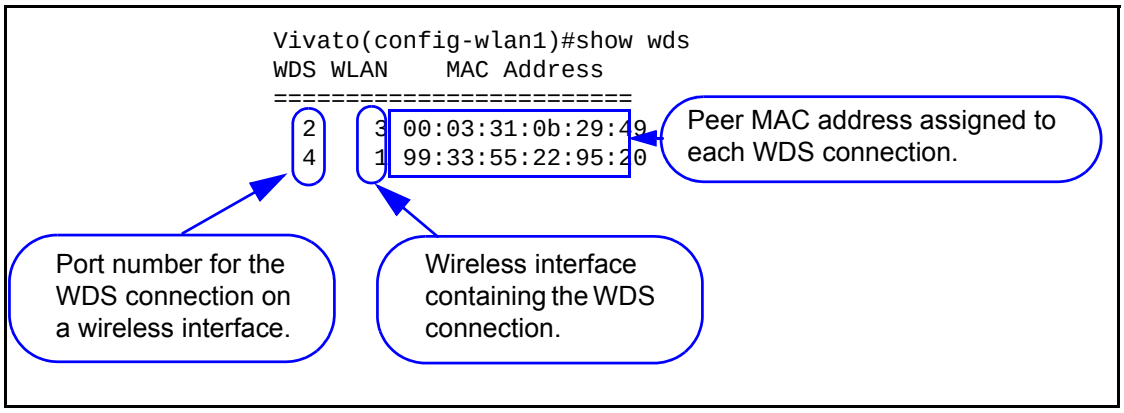
Displays the product serial number, base MAC address for the Wi-FI Bridge/Router, and the versions of software ("Vino Version").

Enable Level Show Commands

The following Show commands are only available at the enable level:

show wds

Display the wireless distribution system (WDS) connections that have been created and the peer MAC addresses that have been assigned to them.



show flash:

Displays the names of configuration files that have been saved in the Wi-Fi Bridge/Router. Configuration files are saved using the **write network flash:**.

show running-config

Displays the current running configuration of the Wi-Fi Bridge/Router, including any dynamic settings that are in effect.

traceroute <ipaddress|hostname>

Displays information about the network route used to access the specified destination address or host name. If the specified address or host is not found, the Wi-Fi Bridge/Router continues to try to locate it until you press the **Ctrl**-**C** keys.

Enable Level Command Descriptions

Refer to these sections for descriptions of commands that are available at the “enable” level (see **"enable"** on page 74).

Table 4—Enable Level Commands

configure [terminal]	**Configure No Interface Commands**
Commands for Managing Configuration Files	**Configure Crypto (Generate Keys) Commands**
Configure IP Commands	**Configure Log Commands**
Configure Enable Secret Commands	**Configure HTTP-Server Commands**
Configure Interface Commands **interface bridge <0-4094>** **interface ethernet 0** **interface wireless < 0-1|all>**	**Configure SNMP-Server Commands**
Configure No SNMP-Server Commands	**Configure Username Admin (Read Level) Secret**
Configure WDS (Wireless Distribution System)	**disable**
edit flash:	**edit flash:**
exit	**reboot**
support	

configure [terminal]

This command tells the CLI to use your terminal to configure the Bridge/Router after accessing the enable level (see **"enable"** on page 74). After entering this command, the command prompt changes to vivato (config)# to indicate that you can now enter the following configuration commands.

Commands for Managing Configuration Files

The following commands are used to copy, write (save), delete, and retrieve firmware and configuration files on the Wi-Fi Bridge/Router. All of these commands are available at the enable level prompt, **Vivato#**, but are not available at the configuration prompt, **Vivato(conf)#**.

configure network flash:

This command is used to configure the Bridge/Router using a saved configuration file. To view the currently saved configuration files, use the **show flash:**command. After entering this command, you are prompted to enter the name of the configuration file to use. The default is “startup-config”.

Important	The default configuration file name is “startup-config”, and is created the first time you use the Quick Setup web pages for the initial configuration or when you save a configuration using that default file name. Once startup-config is created, the Wi-Fi Bridge/Router is *always* configured using that file whenever a reboot occurs by cycling power or by issuing the “reboot” command. To use a different configuration file as the default reboot configuration, use the **copy flash: flash:** command to rename that file “startup-config”. When you reboot the Wi-Fi Bridge/Router, the settings in the new startup-config file are used. The **copy flash: flash:** command can be used to save a copy of the current startup-config file before replacing it. See also **"Reset System to Default Settings"** on page 58.

copy flash: flash:

This command is used to make a copy of an existing configuration file on the Wi-Fi Bridge/Router using a different name. After entering this command, you are prompted to enter the name of the existing configuration file and the file name to use for the copy (as shown below):

Vivato#**copy flash: flash:**

Source file: **startup-config**

Destination file: **old-config**

Vivato>

copy flash: scp:

This command is used to copy a configuration file from the Wi-Fi Bridge/Router to another Wi-FI Bridge/Router or other system. After entering this command, you are prompted to enter the name of the configuration file on the Wi-Fi Bridge/Router, the user name and password for the remote device, the host name (or IP address) of the remote device, and the full directory path and file name for storing the file.

When transferring a file (such as a configuration file) to another Wi-Fi Bridge/Router, the other Wi-Fi Bridge/Router must first be enabled to allow SCP transfer into it. This is done using the **username scpuser (Not Supported in This Firmware Release)** command. When you issue the copy flash: scp: command, you must enter “scpuser” as the user name and enter the enable password of the other Wi-Fi Bridge/Router to gain access to it and copy the file into its flash memory (see below):

Vivato#**copy flash: scp:**

Source file: **startup-config** (The name of the file on this Bridge/Router that you are copying.)

Username: **scpuser**

Password: (Enter the enable password for the other Wi-Fi Bridge/Router.)

Hostname: **172.220.0.35** (Enter an IP address, or enter a host name if a DNS server is present.)

Directory [/]: (When copying to a Wi-Fi Bridge/Router, leave this blank.)

Destination file [startup-config]: **north_bridge_router_config**

copy flash: tftp:

This command is used to copy a file on the Bridge/Router to a connected host computer that is running a TFTP server program. After entering this command, you are prompted to enter the name of the file to copy, the host name (or IP address) of the computer that the file is being sent to, and the name to use when saving the file to that computer.

For example, when using the **support** command to send in a copy of your configuration when requesting customer support for your Bridge/Router, you would use the following commands:

Vivato# **copy flash: tftp:**

Source file: **VSupport_Vivato_08062003.tar**

Hostname: **192.165.20.2**

Destination file [VSupport_Vivato_08062003.tar]: <enter>

!! (appears during file transfer)

copy scp: firmware:

This command copies a Wi-Fi Bridge/Router firmware image stored on a secured external host to the Bridge/Router's flash memory. This is done to upgrade the firmware. After the image has been copied, reboot the Bridge/Router to use this image.

Important	**DO NOT INTERRUPT THE COPYING PROCESS!** The Bridge/Router can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the Bridge/Router to operate.

After entering this command, you are prompted to enter the user name and password on the remote host, the hostname (or IP address) where the file is stored, the full directory path and file name of the file to copy, and the file name to use for storing the copy of the configuration file to the Bridge/Router (as shown below):

Vivato#**copy scp: firmware:**

Username: **gerry**

Password:

Hostname: **192.165.20.68**

Directory [/]: **vivatoimages**

Source file: **vino_1_3_0.bin**

Destination file [vino_1_3_0.bin]:

copy scp: flash:

This command is used to copy a configuration file from another device to the Wi-Fi Bridge/Router. After entering this command, you are prompted to enter the user name and password on the remote device, the hostname (or IP address) where the file is stored, the full directory path and file name of the file to copy, and the file name to use for storing the copy of the configuration file to the Wi-Fi Bridge/Router (as shown below):

Vivato#**copy scp: flash:**

Username: **gerry**

Password:

Hostname: **gardenhose**

Directory [/]: **wifibackups**

Source file: **north_bridge_router_config**

Destination file [north_bridge_router_config]: **renew_config**

copy tftp: firmware:

This command copies a Bridge/Router firmware image stored on an external host running a TFTP server program to flash memory. This is done to upgrade the firmware in the Bridge/Router. After the image has been copied, reboot the Bridge/Router to use this image.

Important	**DO NOT INTERRUPT THE COPYING PROCESS!** The Bridge/Router can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the Bridge/Router to operate.

After entering this command, you are prompted to enter the hostname (or IP address) where the file is stored, the name of the image file, and the file name to use for storing the copy of the configuration file to the Bridge/Router (as shown below):

Vivato#**copy scp: firmware:**

Username: **gerry**

Password:

Hostname: **192.165.20.68**

Directory [/]: **vivatoimages**

Source file: **vino_1_3_0.bin**

Destination file [vino_1_3_0.bin]:

copy tftp: flash:

This command is used to copy a file from another device to the Wi-Fi Bridge/Router using trivial file transfer protocol (TFTP). After entering this command, you are prompted to enter the

hostname of the other device, the source file name to download, and the destination file name to use when saving it to the Wi-Fi Bridge/Router. A TFTP server must be running on the source device to enable the file transfer.

delete flash: <filename>

Enter the name of a configuration file to remove from the Wi-Fi Bridge/Router's memory. Use the **show flash:** command to see what configuration files have been saved.

dir

List the contents of the Wi-Fi Bridge/Router's flash memory (duplicate function of the **show flash:**command).

rename flash:<filename> flash:<new filename>

Enter the name of an existing file and a new name to rename it. For example; **rename flash:startup-config flash:old-config**

write [memory]

Use this command to save the current configuration as "startup-config (the default configuration file name). If this file already exists, the file is overwritten with the new settings.

write network flash:

This command saves the current configuration to the Wi-Fi Bridge/Router's flash memory. After entering this command, you are prompted to specify a file name to save the current configuration. The default configuration file is "startup-config".

write network scp:

This command saves the current configuration to a remote device. After entering this command, you are prompted to specify the user name and password for the device, the host name (or IP address), the full directory path, and the filename to use for storing the configuration (as shown below):

RV-7#**write network scp:**

Username: **gerry**

Password:

Hostname: **gardenhose**

Directory [/]: **bridge_router/backups**

Destination file [startup-config]: **north_bridge_router_config**

write terminal

This command causes the current configuration settings to be displayed on your terminal (just like the **show running-config** command).

Configure Crypto (Generate Keys) Commands

Use the following commands to configure the Wi-Fi Bridge/Router to allow remote access using a secure connection.

crypto key generate <dsa|rsa|rsa1>

Select the type of encryption key to re-generate. These keys are used when accessing the Wi-Fi Bridge/Router through its configuration web pages or when connecting using a secure shell. These keys are automatically generated whenever the Wi-Fi Bridge/Router is rebooted, but you can regenerate these keys using this command.

See **"ip ssh genkey"** on page 103 to enable secure shell operation on the Wi-Fi Bridge/Router. This command also provides regeneration of the encryption keys.

Configure Enable Secret Commands

The enable password must be entered before the configuration of the Wi-Fi Bridge/Router can be changed.

This is the only password requested when using a terminal program and an RS-232 connection to the Wi-Fi Bridge/Router.

When using a secure shell to access the Wi-Fi Bridge/Router, you must first enter the user name (default is “admin”) and the read password (default is “vivato”) to access the read level. To begin configuring the Wi-Fi Bridge/Router, you must then enter the “enable” command and the enable password.

See **username admin secret [<password type (0|5)> <password text>** for information on setting the read level password.

enable secret [<password type (0|5)>] <password text>

This command sets the enable level password. When the “<password type (0|5)>” option is not used, it is assumed that the password you enter is unencrypted (clear text). The password type options allow you to specify that the password being entered is unencrypted, by specifying “0” for the password type, or is encrypted, by specifying “5” for the password type.

Configure HTTP-Server Commands

When enabled, the HTTP daemon provides access to the Wi-Fi Bridge/Router’s configuration web pages.

http-server

Enable the httpd daemon. By default, the http daemon is enabled to allow access to the web user interface configuration pages.

no http-server

Disable the http daemon.

Configure Interface Commands

The following commands are used to configure the ethernet and wireless interfaces in the Bridge/Router.

DHCP Server Operation

Dynamic host configuration protocol (DHCP) is used to automatically assign IP addresses to clients associating through the Wi-Fi Bridge/Router. The bridge, Ethernet, and Wireless interfaces all support DHCP operation using the same command set. Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface.

For more information on configuring DHCP, see **"Dynamic Assignment of Client IP Addresses"** on page 123.

interface bridge <0-4094>

Enter the number of the bridge to create. Issuing this command changes the prompt to indicate which bridge you are configuring, such as **vivato (config -br1)#** if you entered 1 for the value. This prompt must be displayed when issuing any of the following bridge configuration commands.

Note: A default bridge (br0) exists between the Ethernet 0 interface (eth0) and the wireless interfaces (wlan1-wlan13) for wireless clients to communicate with the wired network.

An Ethernet or a wireless interface can only be assigned to one bridge. Therefore, you must first remove any Ethernet or wireless interfaces from the default bridge (br0) before they can be assigned to a new bridge. An interface can only be added to a bridge if that interface does not have its own assigned IP address.

add interface ethernet <0>

Add the Ethernet interface to this bridge.

no add interface ethernet <0>

Remove the Ethernet interface from this bridge.

add interface wireless < 0-1>

Enter the number of the wireless interface to add to the bridge.

no add interface wireless < 0-1>

Remove the specified wireless interface from this bridge.

add interface wireless < 0-1> wds <1-6>

Enter the number of the wireless interface and the port number of a wireless distribution system (WDS) connection on that interface to add that WDS connection to the bridge. This adds the WDS connection residing on that wireless interface to the bridge, but does not add the wireless interface itself to the bridge. See **"Configure WDS (Wireless Distribution System)"** on page 108.

aging-time <10-1000000 seconds>

Enter the number of seconds that network addresses of devices using the bridge are stored in the bridge table after receiving a packet. The default value is 300 seconds.

dhcp-server

Enable dynamic host configuration protocol (DHCP) for automatic assignment of IP addresses to clients associating through this interface. This default state is disabled.

dhcp-server broadcast-address <ip 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.

no dhcp-server broadcast-address <ip address>

Remove the specified DHCP broadcast address.

dhcp-server domain-name <domain name>

Enter a domain name to represent the range of IP addresses served by this DHCP server.

no dhcp-server domain-name <domain name>

Remove the specified name of the domain containing the DHCP server.

dhcp-server gateway <ip address>

Enter the IP address of the interface used as the gateway for DHCP clients to connect to your wired network. This is typically the Ethernet port connected to your wired network.

no dhcp-server gateway <ip address>

Remove the default gateway at the specified IP address.

dhcp-server ip-pool <start ip address> <end ip address> <netmask>

Enter the starting and ending IP address range and net mask for assigning IP addresses on this interface using DHCP.

no dhcp-server ip-pool <start ip address> <end ip address> <netmask>

Remove the specified starting and ending IP address range and net mask from being assigned to clients associating through this interface using DHCP.

dhcp-server lease <1-4294967295>

Enter the number of seconds that an assigned IP address can be leased by a client before it must be renewed. The default is 10 days (864,000 seconds).

no dhcp-server lease <1-4294967295>

Delete the previously set DHCP lease time.

dhcp-server name-server <ip address>

Enter the IP address of a name server. Up to three name servers can be specified by issuing this command for each entry.

no dhcp-server name-server <ip address>

Enter the IP address of a name server to remove from the list of name servers.

dhcp-server ntp-server <ip address>

Enter the IP address of a network time protocol (NTP) server. Up to three time servers can be specified by issuing this command for each entry.

no dhcp-server ntp-server <ip address>

Enter the IP address of a network time server to remove from the list of time servers.

dhcp-server wins <ip address>

Enter the IP address of a Windows internet naming service (WINS) server.

no dhcp-server wins <ip address>

Enter the IP address of a Windows internet naming service (WINS) server to remove it from DHCP configuration.

exit

Issue this command to stop configuring the specified bridge interface and return the command line prompt to the previous level.

forward-time <4-200 seconds>

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 reconfigures the topology. Setting the value too high can cause delays until the spanning tree protocol reconfigures the topology. The default setting is 15 seconds.

no forward-time

Reset the forward time to the default setting of 15 seconds.

hello-time <1-10 seconds>

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 default setting is 2 seconds.

no hello-time

Reset the hello time to the default setting of 2 seconds.

ip address <ipaddress> <netmask> [secondary]

Enter an IP address and a subnet mask for the bridge. In the default configuration, an IP address is assigned to the default bridge (br0), which is the IP address that is used to access the Wi-Fi Bridge/Router. The optional “secondary” entry is used to create a secondary IP address for this bridge.

Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from the bridge. The optional “secondary” entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this bridge, it must be removed before the primary IP address can be removed.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address (client DHCP). If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server. The default state is disabled.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface and allow it to be reassigned.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip broadcast-address <ipaddress> [secondary]

Enter an IP address to use when sending broadcast messages over the bridge interface, and use the optional “secondary” entry to make this a secondary broadcast IP address for this interface.

ip routing

Enter this command to enable IP routing on this interface.

no ip routing

Disable IP routing on this interface.

max-age <6-200 seconds>

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 default value is 20 seconds.

no max-age

Resets the max age to the default value of 20 seconds.

path-cost interface <ethernet 0|wireless 0-1> <0-65535>

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 the LAN 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.

path-cost interface <wireless 0-1> wds <1-6> <0-65535>

Specify the wireless interface and its wireless distribution system (WDS) connection, and enter the path cost for the WDS connection on this bridge. Although the wireless interface for the WDS connection is used in this command, the path cost of the wireless interface itself is not affected; only the path cost of the WDS connection is affected. 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 connection.

Larger path cost values can result the LAN 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.

priority <0-65535>

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 the bridge priority number results in the bridge being selected as the root bridge or a designated bridge.

shutdown

Disable the bridge interface.

no shutdown

Re-enable the bridge interface.

stp

Enable spanning tree protocol (STP) on this bridge.

no stp

Disable spanning tree protocol on this bridge.

show <text>

See **"show interfaces bridge [0-4094]"** on page 77.

shutdown

Disable the bridge.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless < 0-1>|wireless <0-1> wds <1-6>>

Enter the type and number of an interface to use its IP address as the source IP address for network address translation (NAT). The IP address of this bridge, and the IP address of the desired source interface, must be configured before address translation can occur.

interface ethernet 0

Configure the ethernet interface. Issuing this command changes the prompt to **vivato (config -eth0)#.** This prompt must be displayed when issuing any of the following ethernet interface commands:

DHCP Server Operation

Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface. See **"dhcp-server"** on page 92.

exit

Issue this command to stop configuring the specified ethernet interface and return the command line prompt to the previous level.

ip address <ipaddress> <netmask>

Specify the IP address and the subnet mask used to access this ethernet interface. Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

Note: The IP address of the default bridge that bridges the Ethernet and wireless interfaces (bro) is initially used provide access to the Wi-Fi Bridge/Router. See **"interface bridge <0-4094>"** on page 91.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from this interface. The optional "secondary" entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this interface, it must be removed before the primary IP address can be removed.

ip broadcast-address <ipaddress> [secondary]

Enter the IP address to use for broadcast messages, and use the optional "secondary" entry to make this a secondary broadcast IP address for this interface.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address (client DHCP). If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server. The default state is disabled.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface.

ip routing

Enter this command to enable IP routing on this interface. If you are at the Vivato(config)# prompt, IP routing is enabled globally.

no ip routing

Disable IP routing on this interface (or globally at the Vivato(config)# prompt).

show <text>

See **"show interfaces ethernet [0]"** on page 78.

shutdown

Disables the ethernet interface indicated in the command prompt.

no shutdown

Re-enables the interface after using the **shutdown** command to disable it.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless < 0-1>>

Enter the type and number of an interface to use its IP address as the source IP for network address translation (NAT). The IP address of this Ethernet interface, and the IP address of the desired source interface, must be configured before address translation can occur. The default state is disabled.

interface wireless < 0-1|all>

This command selects the wireless interface for configuration. The Wi-Fi Bridge/Router contains 2 fully configurable wireless interfaces. Each interface can be configured individually, or all interfaces can be configured as a group.

Issuing this command changes the prompt to **vivato (config -wlanN)#**, where N is the specified interface number, or **vivato (config -wlan-all)#** when all interfaces are being configured together. One of these prompts must be displayed when issuing any of the following wireless interface commands.

By default, wireless interfaces are bridged to the Ethernet 0 (eth0) interface for wireless clients to be able to access the wired network. See **"interface bridge <0-4094>"** on page 91.

beacon-interval <0-8191>

Specify the amount of time, in milliseconds, between beacons. The default is 100, and should not be changed in most circumstances. This command can be used with an individual wireless interface, and can also be used to change all wireless interfaces at once when

"**interface wireless all**" is specified. Entering either 0 or 8191 results in the maximum period between beacons.

Decreasing the interval generally has an adverse effect on performance, since beacons become a larger percentage of the traffic. Also, the "power-save" function on clients is alerted to a beacon more often, reducing power save benefits.

Increasing the interval may cause an excessive amount of data to be buffered before the beacon is sent, resulting in lost data. Also, some protocols may time out if packets are not delivered before the increased interval period has elapsed.

bitrate <1|2|5.5|11|auto>

Specify 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 802.1lb 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.

channel <1-11>

Enter a channel number for the wireless interface. The value must be in the range of 1 to 11. Whenever possible, you should use the default channels: 1 and 11.

DHCP Server Operation

Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface. See **"dhcp-server"** on page 92.

disable beacon-essid

This command prevents the ESSID from being 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. Therefore, only clients that have had the ESSID manually entered into their preferred wireless network list can associate with the Wi-Fi Bridge/Router. The default state is to send the ESSID in beacons until this command is issued.

no disable beacon-essid

Issuing this command allows the ESSID to be transmitted in beacon messages from this interface, allowing all clients to see the ESSID in their list of available networks.

essid <text>

Enter an identifying name for the extended service set for this wireless interface. The name must be in the range of 1 to 32 characters long.

exit

Enter this command when you are done configuring this wireless interface.

ip address <ipaddress> <netmask>

Assign an IP address and subnet mask to an individual wireless interface. This command is not used when all wireless interfaces are being configured at once by issuing the **interface wireless all** command.

ip address <ipaddress> <netmask> secondary

Enter an IP address and a subnet mask to create a secondary IP address for this interface. Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from this interface. The optional "secondary" entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this interface, it must be removed before the primary IP address can be removed.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address. If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface.

ip broadcast <ipaddress> [secondary]

Enter an IP address to use when sending broadcast messages over this interface, and use the optional "secondary" entry to make this a secondary broadcast IP address for this interface.

no ip broadcast-address [secondary]

Remove the broadcast IP address or, optionally, the secondary broadcast IP address, for this interface.

ip routing

Enter this command to enable IP routing on this interface. If you are at the Vivato(config)# prompt, IP routing is enabled globally.

no ip routing

Disable IP routing on this interface (or globally at the Vivato(config)# prompt).

key <value> <1-4>

This command specifies the wired equivalent privacy (WEP) encryption key value for the specified key assignment. The key value consists of 10 or 26 hex digits (0-9, a-f), or 5 or 13 alphanumeric ascii values (0-9, a-z), depending on the key length (40-bit or 128-bit). When using ascii values, enter **s:** at the start of the value to identify it as an ascii value. The key assignment value must be in the range of 1 to 4.

For example, 104-bit (13 digit ascii) WEP key assigned to key index 1 could be set up for all wireless interfaces by issuing the following command at the **vivato (config -wlans)#** prompt: **key s:gmv8a18436572 1**

sensitivity <1-3>

Change the receiver sensitivity for this wireless interface: 1 = most sensitive (default), 3 = least sensitive. Under most conditions this value should be left at "1" to receive signals from far away clients.

This command can be used with an individual wireless interface, and can also be used to change all wireless interfaces at once when "**interface wireless all**" is specified.

shutdown

Issuing this command disables the wireless interface.

show <text>

See **"show interfaces wireless <0-1>"** on page 80.

shutdown

Disables the ethernet interface indicated in the command prompt.

no shutdown

Issuing this command re-enables the wireless interface if it has been shut down.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless < 0-1>>

Enter the type and number of an interface to use its IP address as the source IP for network address translation (NAT). The IP address of this wireless interface, and the IP address of the desired source interface, must be configured before address translation can occur.

wds <port (1-6)>

Enter a port number (1-6) to enable wireless distribution system (WDS) operation on this wireless interface and port. Each wireless interface can support up to six WDS connections.

When this command is issued, the Wi-Fi Bridge/Router automatically creates a unique MAC address for spanning tree protocol operation on this wireless interface and port. The command prompt is also changed to indicate that you are now configuring a WDS connection that represents a logical interface used only for WDS operation (see below). This new interface has its own set of configuration commands. See **"Configure WDS (Wireless Distribution System)"** on page 108.

```
Vivato(config-wlan1)#wds 1
Vivato(config-wlan1wds1)#
```

Although the WDS interface shares the same physical layer properties as the wireless interface it resides on (such as channel number, receiver sensitivity, and transmit power), it is regarded as a totally separate logical interface. Therefore, to use a WDS connection in a bridge it must be added to the bridge just like any other interface.

The default state has no WDS connections enabled. Use the **no shutdown** command to enable the WDS connection after it is created.

wep <1-4>

This command selects the wired equivalent privacy (WEP) encryption key to use and enables WEP for the wireless interface. The value must be in the range of 1 to 4. Issuing this command restricts access through the wireless interface to clients using the correct WEP key and key assignment values. The default state is disabled.

no wep

This command disables using wired equivalent privacy (WEP) encryption for the wireless interface.

Configure No Interface Commands

The following commands disable interfaces in the Bridge/Router.

no interface bridge <0-4094>

Specify the number of the bridge interface to disable.

Configure IP Commands

Use these commands to specify internet protocol (IP) addressing.

ip domainname <text>

Enter a name to refer to the domain that includes the IP addresses that you assigned to the interfaces within the Bridge/Router. No default domain name is configured.

ip host <hostname> <ipaddress>

Enter a host name and IP address to enter into the host table. Use the **"show ip host"** on page 82 to view the contents of the host IP table.

ip hostname <hostname>

Enter a host name for the Bridge/Router to use with a domain name service (DNS) server; the default host name is “Vivato. The host name is also displayed at the command line prompt.

```
Vivato(config)#ip hostname Mirabeau
Mirabeau(config)#
```

ip name-server <ipaddress>

Enter the IP address of the domain name service (DNS) server to use when looking for the IP address of a specified domain.

ip route <destination prefix> <destination mask> <forwarding router address>

Enter the IP address prefix and net mask of the destination network, and the IP address of the router used to access that network.

For example, entering **ip route 135.220.6.0 255.255.255.0 134.228.4.203** tells the Bridge/Router to route all IP datagrams destined for the 135.228.6.0/24 network through a gateway who’s IP address is 135.228.4.203.

To create a default gateway, enter 0.0.0.0 for the destination prefix and mask, and the IP address of the gateway. For example, if the default gateway is at 192.163.20.240, enter ip route 0.0.0.0 0.0.0.0 192.163.20.240.

ip routing

Enter this command to enable IP routing globally (on all interfaces). The default state is disabled.

ip ssh genkey

Generate encryption keys for a secure shell connection to the Bridge/Router. This command re-generates the same cryptographic keys created by the **crypto key generate <dsa|rsa|rsa1>** command.

ip ssh server

Start the SSH daemon to enable secure shell access.

ip ssh bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>)

Specify the interface on the Bridge/Router to use for SSH access. When this command is issued, only the IP address on that interface can be used to access the Bridge/Router through SSH. If an IP address has not been assigned to this interface, SSH access is not restricted.

no ip ssh bind [interface (wireless <0-1>|ethernet 0|bridge <0-4094>]

Do not restrict SSH access to any interface or, optionally, to a previously bound interface.

Configure Log Commands

The following commands are used to specify where to send system message log information.

logging local

Enable logging and log system messages to the Wi-Fi Bridge/Router's memory. Use the **"show logging"** on page 82 to view the log. The default state is disabled.

logging remote <ipaddress|hostname>

To enable logging and display system information on a remote host, enter the IP address or host name of the remote host. The remote host must first be configured to accept remote logging (syslogd -r at a minimum). The default state is disabled.

no logging local

Disable local logging.

no logging remote

Disable remote logging.

Configure SNMP-Server Commands

The following commands are used to configure simple network management protocol (SNMP) operation.

snmp-server

Enables the SNMP daemon. The default state is disabled.

snmp-server bind interface (wireless < 0-1>|ethernet 0|bridge <0-4094>)

Specify the interface on the Wi-Fi Bridge/Router to use for SNMP access. When this command is issued, only the IP address on that interface can be used to access the Bridge/Router by and

SNMP client. If an IP address has not been assigned to this interface, SNMP access is not restricted.

snmp-server community <community name> RO|RW [<source ip address>]

Enter the name of an SNMP community to create and whether it allows read only (RO) or read-write (RW) operation. If the [<source ipddress>] option is used, only SNMP requests from the source IP address are honored.

snmp-server contact <text>

Enter text for system contact information, such as a person's name.

snmp-server engineID <engine identifier>

Enter an SNMP engine identifier (ID). An engine ID can only be created if there are no SNMPv3 users. Use the 'no snmp-server user' command to remove all users if you have any defined. Only hex characters (0-9 and a-f) can be used to define an SNMPv3 engineID.

snmp-server host <hostname|ipaddress> traps version 1 <community name>

Use this command to create a trap sink for SNMP version 1. Enter the host name or IP address and the community name. See **Table 5—Examples for Creating Traps/Informs Sinks on page 106**.

snmp-server host <hostname|ipaddress> traps|informs version 2c <community name>

Use this command to create a trap sink or an inform sink for SNMP version 2c. Enter the host name or IP address, whether to create a trap or an inform, and the community name. See **Table 5—Examples for Creating Traps/Informs Sinks on page 106**.

snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth MD5|SHA <password> [priv DES <password>]]

Use this command to create a trap sink or an inform sink for SNMP version 3. Specify the host name or IP address, whether to create a trap or an inform, and enter the user name. Optionally, you can specify the authentication type, password, and the DES56 encryption password. The authentication password is used if the optional DES password is not entered. See **Table 5—Examples for Creating Traps/Informs Sinks on page 106**.

Table 5—Examples for Creating Traps/Informs Sinks

Setting	Command
Creates an SNMPv1 trap sink.	snmp-server host 10.0.0.1 traps version 1 private
Creates an SNMPv2c trap sink.	snmp-server host 10.0.0.1 traps version 2c private
Creates an SNMPv2c inform sink.	snmp-server host 10.0.0.1 informs version 2c private
Creates an SNMPv3 trap sink with user "lrs".	snmp-server host 10.0.0.1 traps version 3 user lrs
Creates an SNMPv3 inform sink with user "lrs".	snmp-server host 10.0.0.1 informs version 3 user lrs
Creates an SNMPv3 inform with user "lrs" using authentication and encryption.	snmp-server host 10.0.0.1 informs version 3 user lrs auth MD5 12345678 priv DES 23456789

snmp-server location <text>

Enter the SNMP system location, such as "inside the krell lab".

snmp-server name <text>

Enter the SNMP system name, such as "WISP 1".

snmp-server user <username> [auth MD5|SHA <password> [priv DES [<password>]]]

To create an SNMPv3 user, enter the user name, authentication method and password, and DES56 encryption password to enable authentication and encryption for SNMP. The privacy password is optional. If it is not entered, the authentication password is also used for the privacy password.

The following examples illustrate how this command is used:

Table 6—Examples for Configuring an SNMPv3 User

Setting	Command
Create a user named "lrs" with no authentication and no privacy.	snmp-server user lrs
Create a user named "lrs" that only uses authentication.	snmp-server user lrs auth MD5 12345678
Create a user named "lrs" with authentication and encryption using the authentication password.	snmp-server user lrs auth MD5 12345678 priv DES
Create a user named "lrs" with authentication and with encryption that uses it's own password	snmp-server user lrs auth MD5 12345678 priv DES 23456789

Configure No SNMP-Server Commands

The following commands disable various aspects of simple network management protocol (SNMP) operation. See also **Configure SNMP-Server Commands**.

no snmp-server

Disables the SNMP daemon.

no snmp-server community <community name>

Enter the name of the SNMP community to be deleted. See also **snmp-server community <community name> RO|RW [<source ip address>]**.

no snmp-server contact

Deletes the SNMP contact information.

no snmp-server engineID

Removes the SNMP engine identifier. An engine ID can only be removed if there are no SNMPv3 users. Use the 'no snmp-server user' command to remove all users if you have any defined.

no snmp-server host <hostname|ipaddress> traps|informs version <1|2c|3>

Enter this command to disable the corresponding trap or inform. See **snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth MD5|SHA <password> [priv DES <password>]]**).

no snmp-server location

Deletes the SNMP location information.

no snmp-server name

Deletes the SNMP name information

no snmp-server user <username> [auth MD5|SHA <password> [priv DES <password>]]

Enter this command to remove the specified SNMPv3 user (see **snmp-server user <username> [auth MD5|SHA <password> [priv DES [<password>]]]**).

Configure Username Admin (Read Level) Secret

The read level secret is used to access the Wi-Fi Bridge/Router through a secure shell or the configuration webpages; it is not used when a terminal program and an RS-232 connection are used. By default, the user name is “admin” and the password is “vivato”.

username admin secret [<password type (0|5)> <password text>

This command sets the read level password. When the "<password type (0|5)>" option is not used, it is assumed that the password you enter is unencrypted (clear text). The password type options allow you to specify that the password being entered is unencrypted, by specifying "0" for the password type, or is encrypted, by specifying "5" for the password type.

Use the **enable secret [<password type (0|5)>] <password text>** command to change the enable level secrete.

username scpuser (Not Supported in This Firmware Release)

Enter this command to enable secure copy (SCP) file transfer to this Wi-Fi Bridge/Router. Users attempting to transfer files from another Wi-FI Bridge/Router to this Wi-Fi Bridge/Router must first enter "scpuser" as the user name and provide the enable password for this Bridge/Router to permit access. See **"copy flash: scp:"** on page 86.

Configure WDS (Wireless Distribution System)

A wireless distribution system uses a Vivato Bridge/Router and Vivato Wi-Fi Switch to provide a wireless data link that can span large distances to provide a network connection to a remote Wi-Fi Switch or to connect two network segments together. The remote Switch can use the WDS link to a local Bridge/Router as a substitute for its own wired backhaul connection, requiring only mains power to provide 802.11b service to clients.

The link is created by first enabling WDS operation on a wireless interface on the Wi-Fi Switch and on the Bridge/Router, and then specifying the MAC address of the WDS-enabled wireless interface on the opposing device as the "peer address".

A WDS connection is created at the wireless interface configuration level using the **wds <port (1-6)>** command. The command prompt then changes to indicate that you are configuring that WDS connection (as shown below).

The WDS connection acts as a separate logical interface, even though it configured on a wireless interface. Functioning as an interface, an IP address can be assigned to the WDS interface using a static address or by DHCP client operation.

Important 	The WDS connection must be added to the default bridge before it can pass traffic to other interfaces on the Bridge/Router. Use the **add interface wireless < 0-1> wds <1-6>** command to add the WDS connection to the bridge.

Important 	To help secure the WDS traffic, enable WEP on the wireless interfaces at both ends of the WDS link.

Use the **show wds** command to view a WDS configuration on a wireless interface.

The following WDS commands are available to configure the specific WDS connection indicated at the command prompt. See **"WDS Configuration Example"** on page 111 to see how some of these commands are used.

exit

Exit the WDS configuration and return to the configuration prompt level. To return to the WDS command prompt after exiting, you need to first prefix to the specific wireless interface (using the **interface wireless < 0-1|all>** command), and then enter the **wds <port (1-6)>** command for the specific WDS connection.

ip address <ip address> <subnet mask> [secondary]

Specify an IP address and subnet mask for this WDS connection. The IP address and netmask bits can also be entered using the format in this example: 10.0.3.34/24. The optional "secondary" entry is used to create a secondary IP address for this WDS connection.

When a WDS connection is removed, any primary and secondary IP addresses assigned to that connection are also removed.

no ip address <ip address> <subnet mask> [secondary]

Enter the previously assigned IP address to remove it from this WDS interface. Use the "secondary" option to remove a secondary IP address.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface to assign it an IP address*. If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface and allow it to be reassigned.

ip broadcast-address <ip address> [secondary]

Enter the broadcast IP address for this WDS connection. The optional "secondary" entry is used to create a secondary broadcast IP address for this WDS connection.

no ip broadcast-address <ip address> [secondary]

Enter the previously assigned broadcast IP address to remove it from this WDS interface. Use the “secondary” option to remove a secondary broadcast IP address.

peer-address <mac address>

Enter the MAC address of the wireless interface on the Wi-Fi Switch that is being used for a WDS link to the Bridge/Router (in the format 00:0B:33:31:85:A3).

A peer MAC address can only be used with one WDS connection on any wireless interface.

shutdown

Enter this command to disable this WDS connection.

no shutdown

Enable this WDS connection.

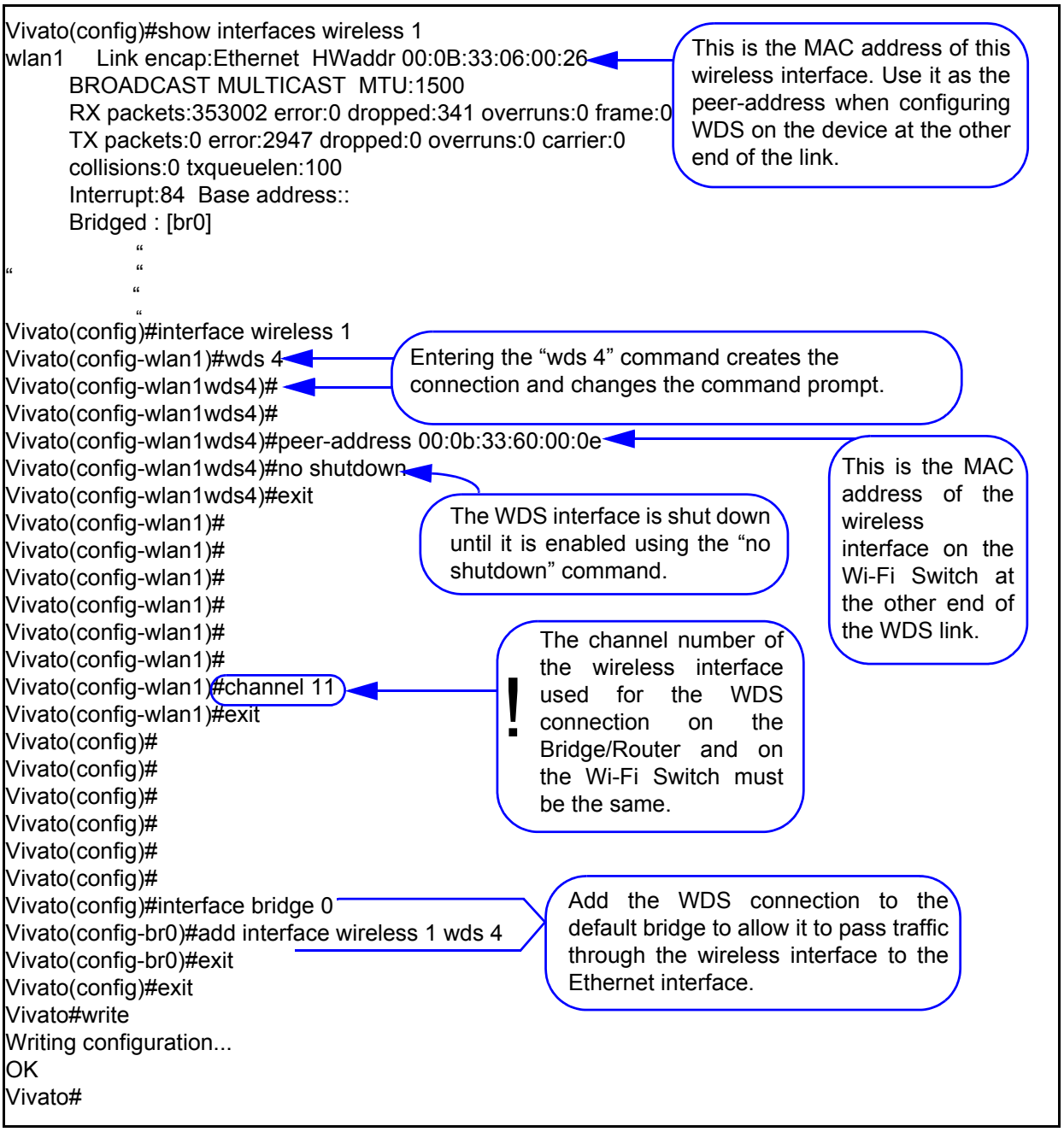


Figure 33—WDS Configuration Example

disable

Enter this command to leave the enable level and return to the read level.

edit flash:

After entering this command, you are prompted to enter the name of a configuration file in the Wi-Fi Bridge/Router to edit. The CLI then launches a vi editor to allow the configuration file to be modified and saved. CLI operation returns after exiting the vi editor.

To exit the editor without saving your changes, type :q!. To save your changes and exit, type **ZZ** or **:wq**.

exit

After using the **configure [terminal]** command to configure the Wi-Fi Bridge/Router, the CLI stays in the configuration mode until you enter the **exit** command. If you exit the configuration mode and enter the **exit** command again, the current CLI session is closed.

no <configuration command>

Override parameters you have entered. This operation is used extensively in the enable level commands to disable previously enabled operations or settings (as shown in this command list).

reboot

Issuing this command causes the Wi-Fi Bridge/Router to be reset, and powers on using the last saved configuration. See **write network flash:** or **"write [memory]"** on page 89 for commands to save the current configuration.

CAUTION — *Any changes made to the configuration that have not been saved are lost when this command is issued.*

support

This command causes an archive of the current configuration and system messages to be created and saved in a file called “VSupport_Vivato_<date>.tar”. This file can then be copied to a local host computer using the **copy flash: tftp:** command, and sent to Vivato Customer Support for assistance.

Network Monitoring

Three methods can be used to monitor Vivato Wi-Fi Bridge/Router operations and network traffic:

- The built-in web page user interface. To use the monitoring functions of the web interface, see **"Monitoring Clients and System Operations"** on page 51.
- Command line interface (CLI). A explanation of using the CLI and a list of the available commands to configure and monitor Bridge/Router operations is provided in **"Configuration Using The Command Line Interface"** on page 67.
- Simple network management protocol (SNMP).

SNMP Operations

You can use third-party SNMP management software to monitor operations within the Vivato Wi-Fi Bridge/Router. These software packages are designed to use standard SNMP versions that have been defined to work with devices created by various manufacturers. The Wi-Fi Bridge/Router supports SNMP versions 1, 2c, and 3.

SNMP applications use management information bases (MIBs) - databases of objects that are used to monitor and configure a device.

Operating Considerations

Not all MIB objects are supported in this version of the Vivato Wi-Fi Bridge/Router. The following information describes which MIBs are provided and which objects are and are not supported in this firmware release:

- SNMP walk performance issues - Performing an snmpwalk or snmpbulkwalk may time-out when trying to walk the entire MIB tree. Use the -t option to set the timer value higher than the default: **snmpwalk -c public -v 2c -t 15 10.0.0.2 .1** will allow a full 15 seconds from start to finish.
- SNMP Sets - In general, sets are not supported in this release.
- SNMPv2 Support Only - Currently SNMPv2c is the only supported version, though version 3 will be supported in the near future. Some, but not all, SNMPv3 options are supported in this release (v3 traps for example, ARE supported).

Supported MIB

The following MIB is included on the Vivato Wi-Fi Bridge/Router CD. Operating limitations are relevant for this firmware release, but may not be present in future firmware releases.

RFC1213-MIB.txt

The following limitations exist for this MIB in this firmware release:

The following are not supported:

- ipRouteTable
- egp
- transmission

A not-writable error will be returned during the set operation if the CLI or Web UI has been used to set the following:

- sysContact
- sysName
- sysLocation

Enabling SNMP Operation

To use SNMP in the Wi-Fi Bridge/Router, you need to enter some information and enable SNMP. This can be done using the web interface or by using the CLI. Refer to **"Configure SNMP-Server Commands"** on page 104 for a listing of the CLI commands used for setting up and enabling SNMP.

Several web configuration menus are used to configure SNMP operation after selecting **Networks>SNMP**.

The **Base SNMP Options** screen is used to enable SNMP operation and provide information used for all version of SNMP.

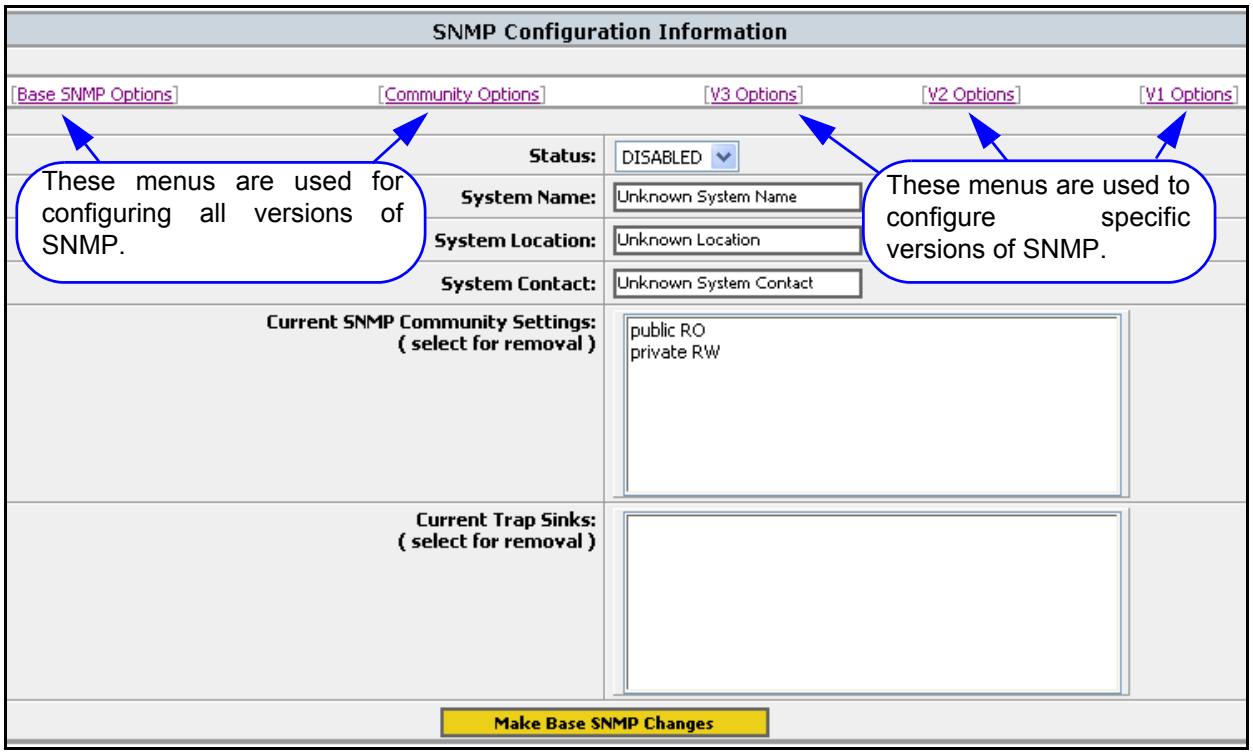


Figure 34—SNMP Base Settings For All Version of SNMP

The **Community Options** menu is used to specify read-only or read-write privileges. Enter the name of an SNMP community to create and whether it allows read only (RO) or read-write (RW) operation. If the IP address is entered, only SNMP requests from the source IP address are honored.

Figure 35—Creating an SNMP Community

The remaining three menus are used for configuring specific SNMP versions.

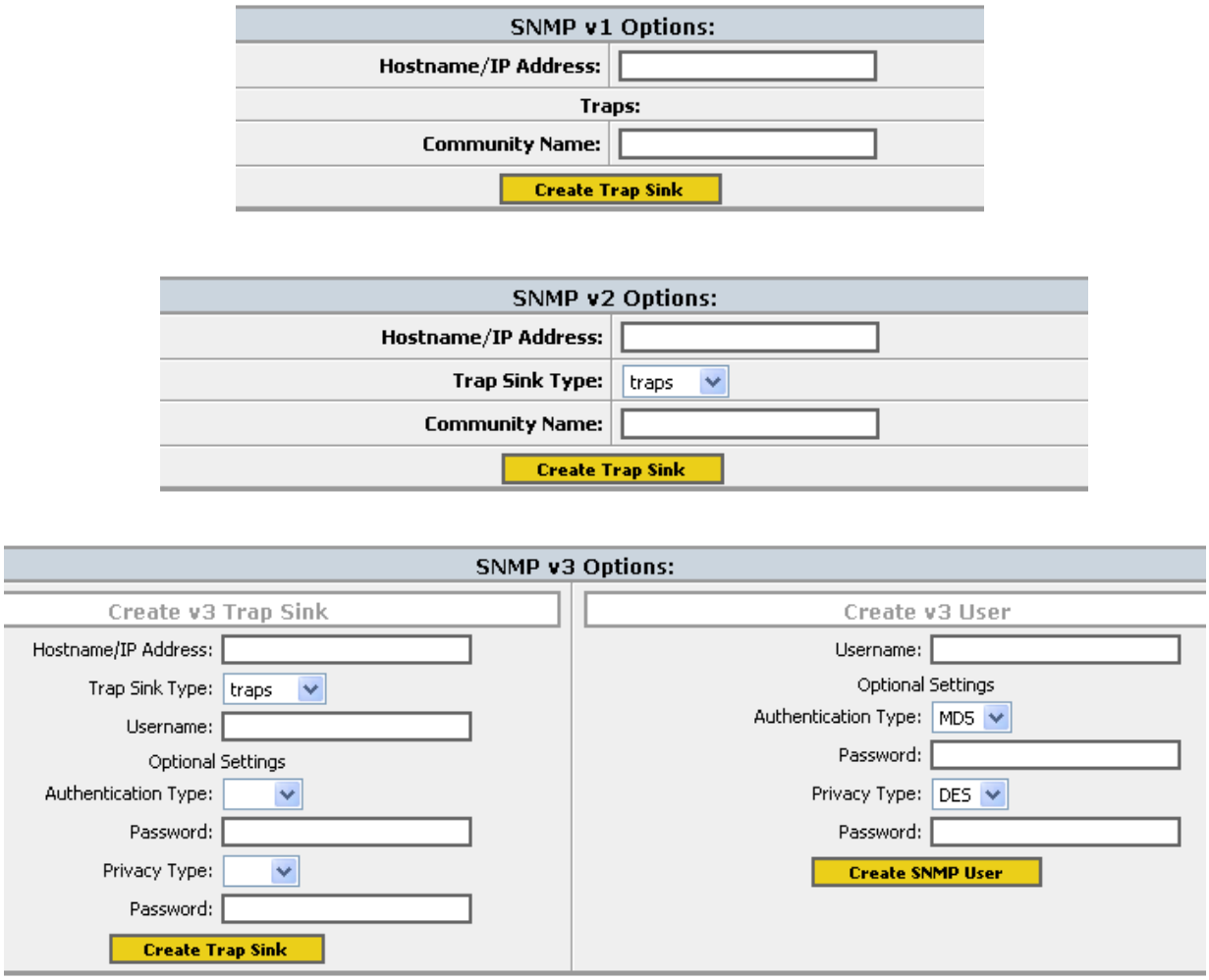


Figure 36—Specifying Settings for SNMP Versions 1, 2c, and 3

Verifying Wi-Fi Operation

After installing and configuring the Vivato Wi-Fi Bridge/Router, it is important to verify that it operates as intended. The information in this section is intended to help you verify Wi-Fi Bridge/Router operation and provides ideas to troubleshoot any configuration problems that you may have.

Use your Wi-Fi client's documentation to understand its configuration settings.

Verification Process

Use the following flowchart to verify Wi-Fi Bridge/Router operation and to identify some of the possible causes of problems you may encounter:

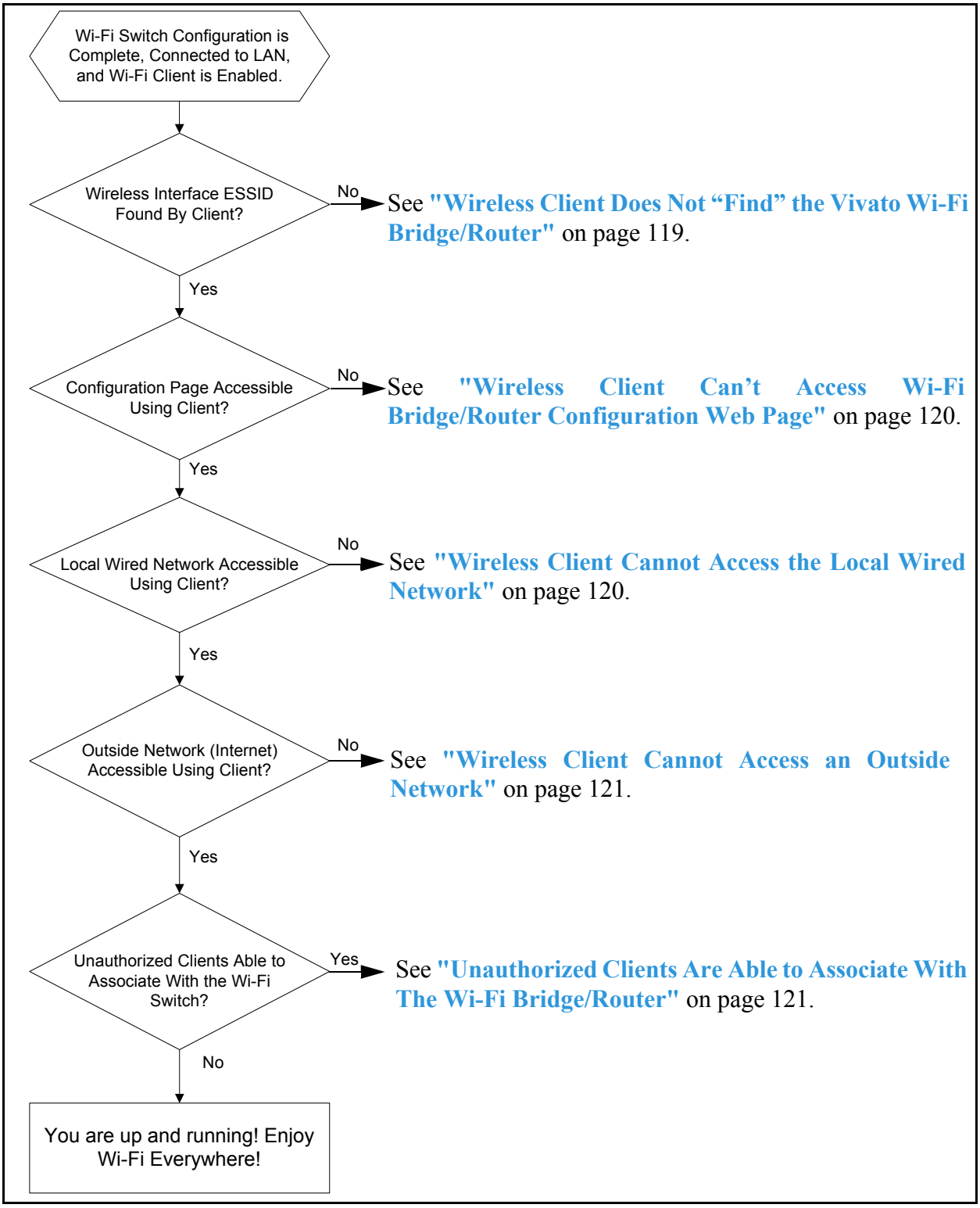


Figure 37—Wi-Fi Bridge/Router Verification Flowchart

Wireless Client Does Not “Find” the Vivato Wi-Fi Bridge/Router

Part of configuring the Wi-Fi Bridge/Router involves entering the extended service set identifier (ESSID) for each wireless interface. This is the name that is displayed on your client’s list of available Wi-Fi networks. The following conditions must be present for the ESSID to be displayed on your client’s network list.

- The Wi-Fi Bridge/Router’s power LED must indicate that the Bridge/Router is operating. See **"Connectors and Indicators"** on page 1.
- At least one of the Wi-Fi Bridge/Router’s wireless interfaces must be enabled and the ESSID specified. See **"Network>Wireless Interfaces"** on page 42.
- Your Wi-Fi client is configured and working correctly. Refer to your client’s documentation.

Variations in Client Performance Due to Physical Orientation

The physical orientation of the client can have a direct effect on Wi-Fi operation, due to the variance in the antenna designs of clients. Studies have shown that rotating the client can significantly change the level of received signal in some cases.

If you are in an area that is partially blocked from the Wi-Fi Bridge/Router’s antenna pattern, try rotating the client 90 degrees (horizontally) to see if your reception is improved. You can also bend the Bridge/Router’s antennas up to 90 degrees to see what angle works best with the most clients.

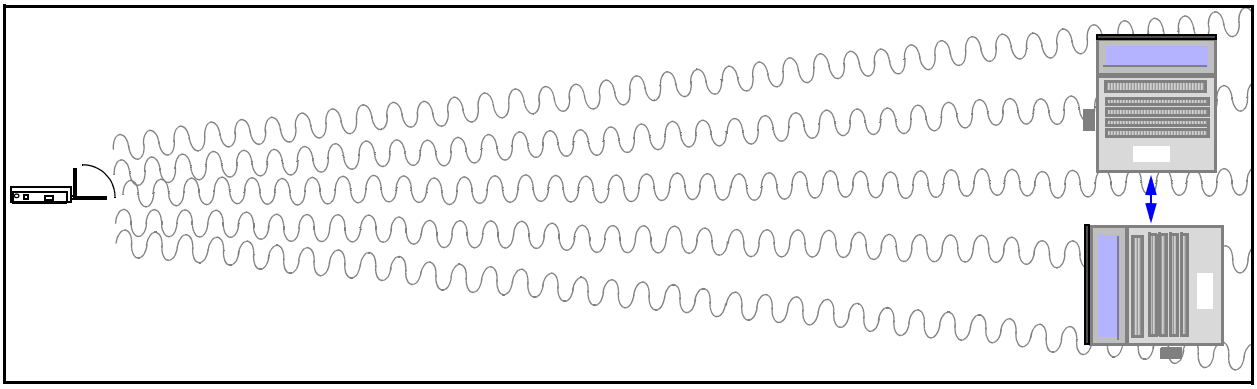


Figure 38—Rotating the Client to Improve Performance

Wireless Client Can't Access Wi-Fi Bridge/Router Configuration Web Page

For your client to associate with the Vivato Wi-Fi Bridge/Router, the following conditions must exist:

- The IP address of your wireless client must be within the same subnet range of the Wi-Fi Bridge/Router. The default IP address of the Wi-Fi Bridge/Router is 169.254.20.1. In some cases you can have your client automatically set its IP address within this range using automatic private IP addressing (see **"Using APIPA to Assign a Usable IP Address For Your Client"** on page 13).

  You can also configure the Wi-Fi Bridge/Router to be a dynamic host configuration protocol (DHCP) server that assigns an IP address to your client when the client associates. See **"Network>DHCP"** on page 39.

  You can also manually set the IP address of your client to use a static IP address by editing the **Internet Protocol (TCP/IP)** properties of your client, disabling automatic IP address assignment, and manually entering the address.

- The correct Address/Location must be specified in your web browser. See **"Configuration Connections"** on page 12.

- The security settings for your client and the Wi-Fi Bridge/Router must match. If you previously enabled security (such as WEP) in the Wi-Fi Bridge/Router, and your client's security settings are not providing access to the Wi-Fi Bridge/Router, you must use a wired connection to the Wi-Fi Bridge/Router to access the configuration web page and match the security settings between the Bridge/Router and your client. See **"Configuration Connections"** on page 12.

- The level of interfering signals must not be so great that the lowest allowed data rate (1 Mbps) cannot be used. Verify that Wi-Fi access points using the same channel assignments as the Wi-Fi Bridge/Router are not in close proximity. Also make sure that one or more microwave ovens are not operating within the Wi-Fi Bridge/Router's coverage area. See **"Network>Wireless Interfaces"** on page 42 and **"Interfering Signal Sources"** on page 8.

Wireless Client Cannot Access the Local Wired Network

If you are able to access the Vivato Wi-Fi Bridge/Router's configuration web page using your wireless client, but you are unable to access the wired network connected to one of the Bridge/Router's Ethernet ports, verify that the following conditions are present:

- The default bridge (br0) connecting the wireless interfaces to the Ethernet ports is enabled. See **"Network Settings"** on page 31.

- Your wired network is connected to the Wi-Fi Bridge/Router's Ethernet port.

- The Ethernet port you are connected to is enabled. The Vivato Wi-Fi Bridge/Router is pre configured with the Ethernet ports enabled. See **"Network>Ethernet Interface"** on page 41.

- The Vivato Wi-Fi Bridge/Router has been entered in the list of permissions for your local area network (LAN) server. If your server uses an access list to allow access to the network, make sure that the Wi-Fi Bridge/Router has been added to that list.
- The correct default gateway is specified. See **"Basic Network Setup"** on page 22.

Wireless Client Cannot Access an Outside Network

If you are able to connect to your local network through the Vivato Wi-Fi Bridge/Router, but you cannot access the Internet or another remote server, verify that the following conditions are present:

- The local network must have access to an Internet server; either its own server or through an internet service provider (ISP).
- If a modem (DSL or cable) is used to provide the internet connection through an ISP, the modem must be authenticated with the remote server. Refer to your modem's documentation or call your service provider for assistance.
- The correct default gateway must be specified. See **"Basic Network Setup"** on page 22.

Unauthorized Clients Are Able to Associate With The Wi-Fi Bridge/Router

Security is disabled in the Wi-Fi Bridge/Router when delivered. If the security settings have not been configured and enabled, anyone with an IEEE 802.11b client can associate with the Wi-Fi Bridge/Router. To prevent this situation, enable the highest levels of security in the Wi-Fi Bridge/Router and your clients.

Connecting Through a WDS Connection

When using a WDS link between the Bridge/Router and a Vivato Wi-Fi Switch, make sure the following configuration has been set ON BOTH DEVICES:

- A WDS interface was created AND ENABLED.
- The wireless interface MAC address used for the WDS connection of the opposing device has been set as the "peer address".
- The channel number of the wireless interface used for the WDS connection is the same.
- The wireless interface used for the WDS connection has been enabled.
- The WDS connection has been added to the bridge connecting the wireless interface to the Ethernet port (typically bridge 0).

Dynamic Assignment of Client IP Addresses

In order to communicate with the Bridge/Router, servers, and other devices on a network, clients must be configured to have an IP address within the same address range that is used by those devices. This is similar to a telephone connection, where only certain phone number prefixes are used within an area code to allow callers to talk to each other without being routed through long distance lines.

Client IP address assignment can be accomplished using statically configured IP addresses on each client or by using dynamic host control protocol (DHCP) operation to automatically set IP addresses.

Assigning static IP addresses requires each client to be manually configured by a user after being told what IP address to use by a system administrator. This is a slow and cumbersome operation when a large number of clients are used. It is also an inefficient use of IP addresses when some clients are not accessing the network.

How Does DHCP Work?

If clients are configured to use DHCP, IP addresses are automatically assigned to clients whenever they associate. If a DHCP server exists on your wired network, clients that associate with the Bridge/Router can request and receive an IP address from a pool of addresses configured on that server. Using this form of DHCP, all clients are assigned IP addresses that are on the same subnet as the Bridge/Router and its connected wired network (as shown below). This has the effect of using IP addresses from the same pool of addresses that are used by the wired network, reducing the number of devices that can exist on the network. This also allows wireless users to see the base IP address of your wired network by looking at their client settings.

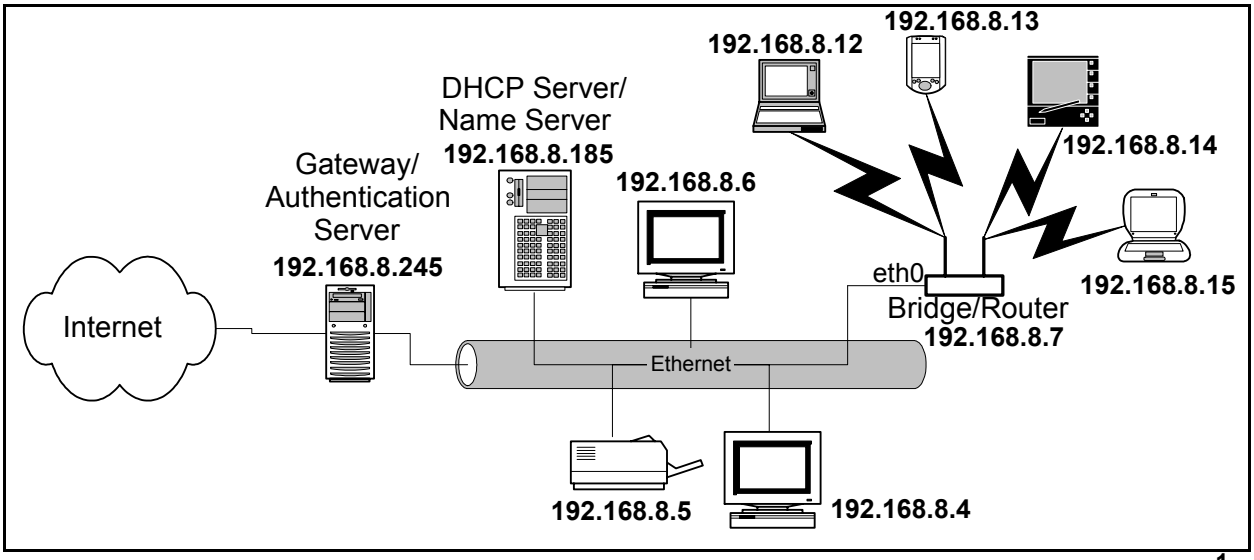


Figure 1—Wireless Client IP Address Assignment Using Your Network's DHCP Server[1]

1. Network drawings shown in this document are for illustration purposes only.

The Vivato Wi-Fi Bridge/Router can be configured as a DHCP server. In conjunction with network address translation (NAT), this allows a totally different range of IP addresses to be used by your wireless clients than are used by your wired network. This results in only one IP address being used for all traffic to/from the Bridge/Router's connection to the wired network. In the network illustrated below, the Bridge/Router's Ethernet 0 (eth0) port is connected to the wired network using IP address 192.168.8.7. DHCP server operation is configured to issue IP addresses to wireless clients from a pool of addresses starting at 10.0.4.1. Even though they are on different subnets, the wireless clients are able to exchange packets with the wired network by using NAT.

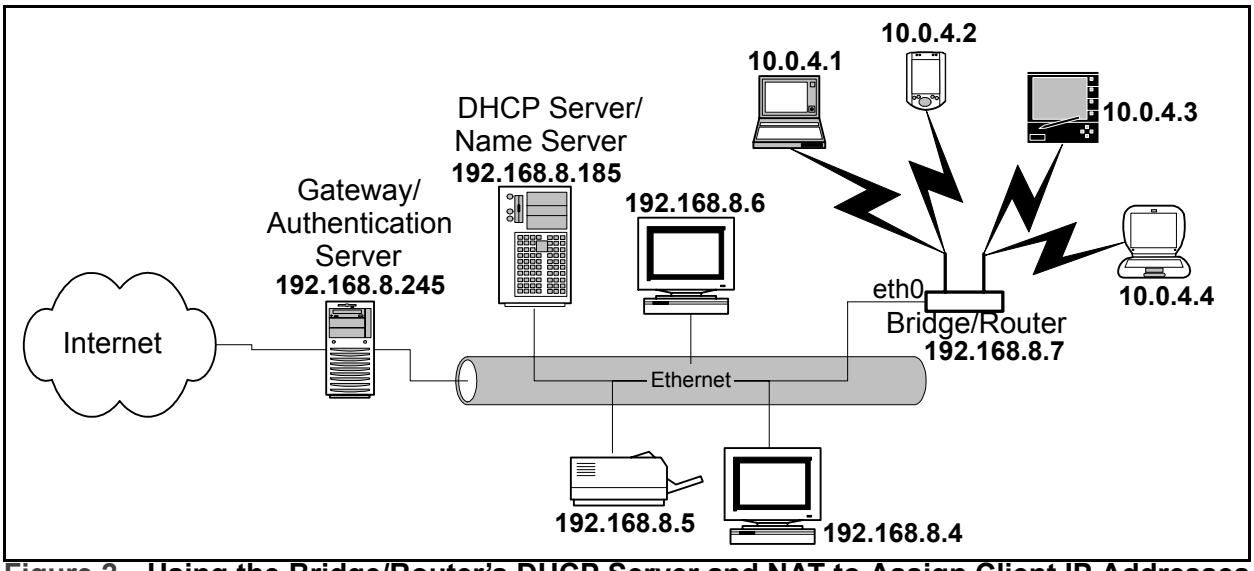


Figure 2—Using the Bridge/Router's DHCP Server and NAT to Assign Client IP Addresses

What is Network Address Translation?

NAT translates the source IP address for packets to/from different subnets to allow communication between them. In the figure above, the Bridge/Router replaces the source IP address on packets from wireless clients (10.0.4.x) with the IP address assigned to the eth0 port (192.168.8.7). Since the eth0 port's IP address is within the subnet used by the wired network, the packets are routed just as any other packet on the wired network. When a packet intended for a wireless client is received on the eth0 port, the Bridge/Router translates the IP address from the source 192.168.8.x address to the intended 10.0.4.x address.

"Breaking the Bridge"

As shown below, the Bridge/Router's default configuration connects the Ethernet port (eth0) to both wireless interfaces (wlan0 & wlan1) using a bridge called "br0".

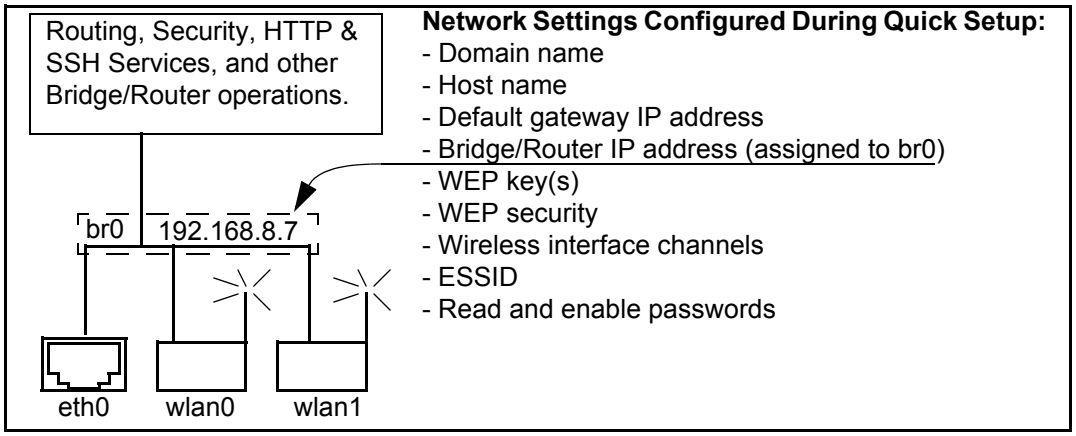


Figure 3—Default Configuration After Using the Quick Setup Web Pages

This is not a problem when using a network DHCP server to assign client IP addresses (as shown in **Figure 1— Wireless Client IP Address Assignment Using Your Network's DHCP Server**).

However, to use the Bridge/Router as a DHCP server for your wireless clients, the Ethernet port must be removed from the bridge, otherwise the Bridge/Router will also respond to DHCP requests from devices connected to the Ethernet port. If a DHCP server already exists on your wired network, this could cause conflicts.

To isolate the Ethernet port from the default bridge, it must be removed using either the command line interface (CLI) or the Web interface. An IP address must then be assigned to the Ethernet port to enable access to the Bridge/Router from the wired network. After removing the Ethernet port from the bridge, IP routing must be enabled to route packets between the Ethernet port and the wireless interfaces. Going back to the telephone analogy, this is like routing a long distance call between different area codes.

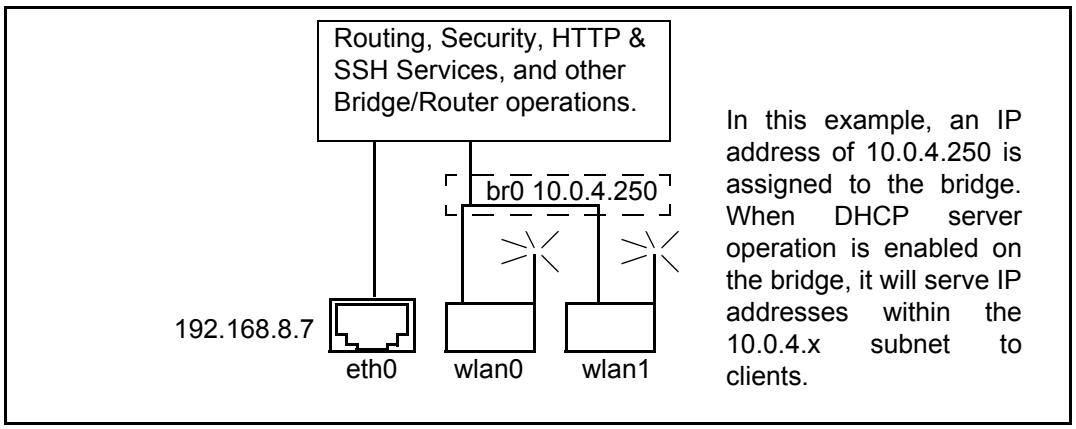


Figure 4—Removing Eth0 From the Default Bridge (br0) For DHCP Operation

Configuring DHCP Server Operation on the Bridge/Router

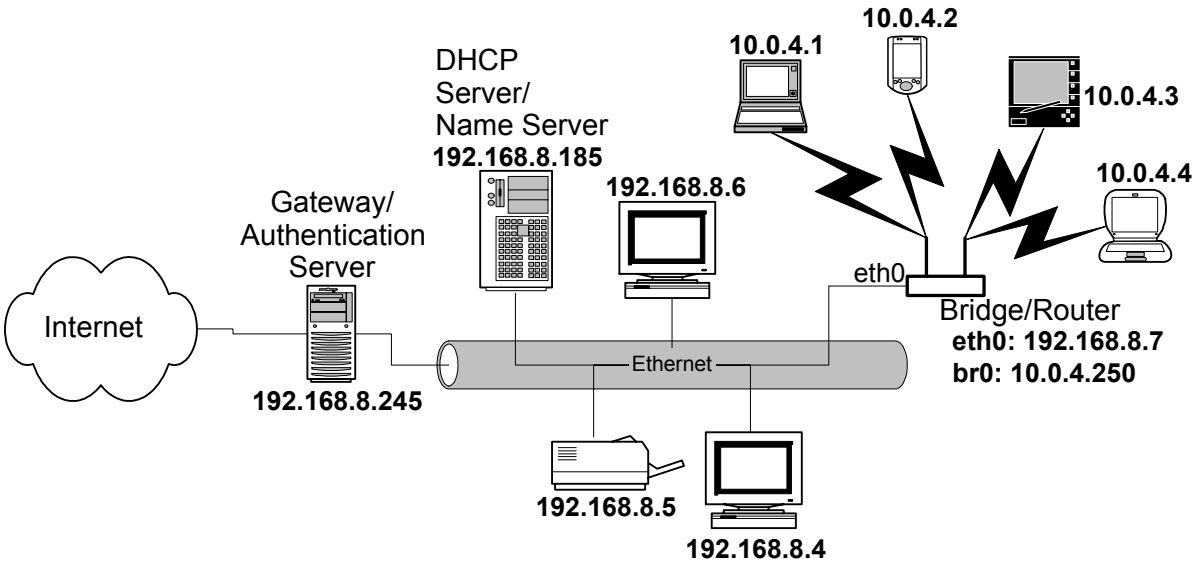
The following steps are used to configure DHCP server operation to provide client IP addresses. Entries marked optional indicate setting that are not absolutely necessary to have DHCP server operation working, but may be needed to access some wired network features.

These steps assume that the Bridge/Router was initially configured using the Quick Setup pages, and therefore the default bridge configuration exists:

- Remove eth0 from the default bridge (br0).
- Assign an IP address to br0 that is within the same subnet as the addresses to be assigned to wireless clients.
- Assign an IP address to the Ethernet interface (eth0) that is within the range of addresses used by your wired network.
- Set the DHCP broadcast address. This is the address used to send broadcast messages to all wireless clients.
- Set the DHCP domain name (optional). This is the name that refers to the bridge and the wireless clients associating with the Bridge/Router.
- Set the DHCP gateway IP address. This is the path (gateway) that the DHCP server uses to access the router function of the Bridge/Router. This is normally the IP address of the bridge.
- Enter the starting and ending IP addresses and net mask that define the pool of IP addresses that are served to wireless clients. Make sure that the IP address of the bridge is NOT inside this pool of addresses.
- Enter the DHCP lease time (optional). This value determines how long a client can continuously use an assigned IP address before it must ask to either renew this address or lose the IP connection.
- Enter the name server IP address. This is the name server on your wired network used to translate host names into IP addresses.
- Enter the network time protocol (ntp) server IP address (optional). This is used to sync the clock settings of your wireless client to your wired network.
- Enter the Windows internet naming service (WINS) server IP address (if used).
- Enable NAT for the bridge, specifying the Ethernet interface (eth0) as the source. This tells the DHCP server to use eth0's IP address as the source address for packets through the bridge.
- Enable the DHCP server for the bridge. The DHCP server is off by default, and must be enabled after it is configured.
- Enter a default route to your wired network's gateway. This tells the Bridge/Router where to send packets destined for an address outside of the local network.
- Enable global IP routing. This allows packets to be routed between the ethernet and bridge interfaces. Since the bridge no longer contains eth0, IP routing must be used to move packets between the Ethernet and wireless interfaces.

DHCP Server Configuration Example

The following CLI configuration example shows how the Bridge/Router can be configured to act as a DHCP server for clients connecting to the network shown below.




```
Vivato(config)#interface bridge 0
Vivato(config-br0)#no add interface ethernet 0
Vivato(config-br0)#ip address 10.0.4.250 255.255.255.0
Vivato(config-br0)#exit
Vivato(config)#interface ethernet 0
Vivato(config-eth0)#ip address 192.168.8.7 255.255.255.0
Vivato(config-eth0)#exit
Vivato(config)#interface bridge 0
Vivato(config-br0)#dhcp-server broadcast-address 10.0.4.255
Vivato(config-br0)#dhcp-server gateway 10.0.4.250
Vivato(config-br0)#dhcp-server ip-pool 10.0.4.5 10.0.4.50 255.255.255.0
Vivato(config-br0)#dhcp-server lease 28800
Vivato(config-br0)#dhcp-server name-server 192.168.8.185
Vivato(config-br0)#dhcp-server wins 192.168.8.185
Vivato(config-br0)#source-nat interface ethernet 0
Vivato(config-br0)#dhcp-server
Vivato(config-br0)#exit
Vivato(config)#ip rout 0.0.0.0 0.0.0.0 192.168.8.245
Vivato(config)#ip routing
Vivato(config)#
```

Figure 5—Configuring the Bridge/Router for DHCP Server Operation

Index