



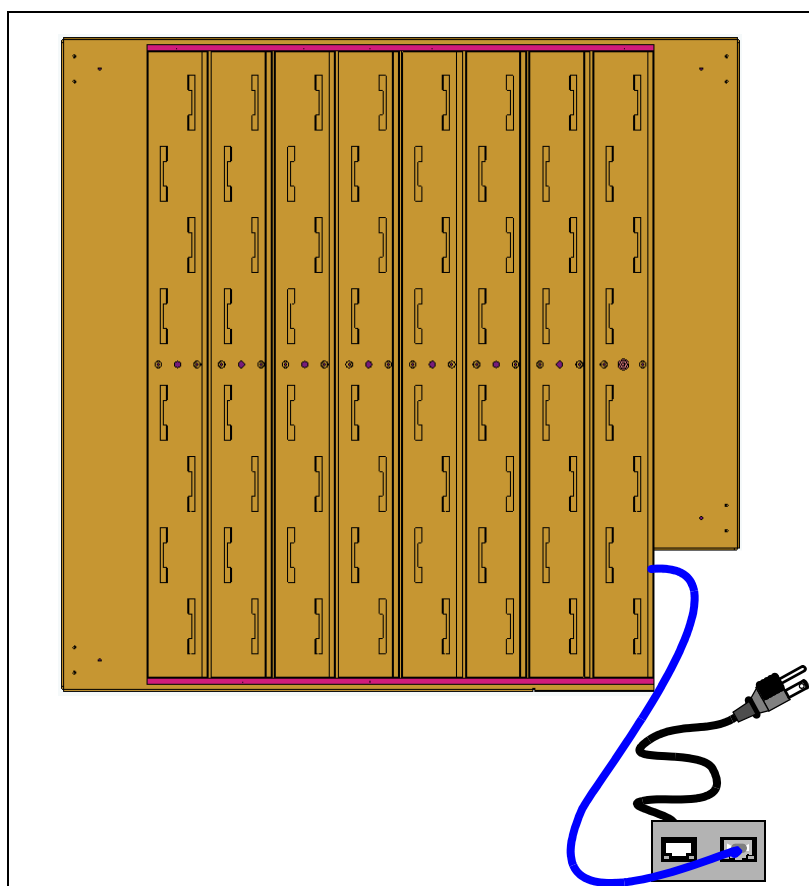
W i - F i E V E R Y W H E R E

VP2200 Series Wi-Fi Switch User Guide

Preliminary Documentation

Manual Part Number: 770-01564-01

Printed in U.S.A.



Copyright © 2004, Vivato, Inc.

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

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

Who Should Read This Document?

The Vivato Wi-Fi Switch is a new category of Wi-Fi products. Anyone installing this product, configuring this product for operation, or performing network management operations involving this product, should read this document before working with the Wi-Fi Switch.

Safety Information

You must heed any and all safety precautions and warnings in this document or indicated on the Vivato VP2200 Wi-Fi Switch 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 VP2200 Wi-Fi Switch must be professionally installed. The person installing the VP2200 Wi-Fi Switch 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.

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

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

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

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

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

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

Changes or modifications not expressly approved by Vivato could void the user's authority to operate the equipment.

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. VP2200 Wi-Fi Switch

This product is intended for home or office use.

The Vivato Wi-Fi Switch has been evaluated under FCC Bulletin OET 65 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 Switch should be at least 20 cm (7.8 in.) from people when operating.

FCC Indoor exposure limits for 2.4 GHz ISM Part 15 devices: $1\text{mW}/\text{cm}^2$ at 20 cm distance from antenna face.

- Vivato VP2200 Wi-Fi Switch worst case exposure (OET 65 upper bound method):
 $0.411\text{ mW}/\text{cm}^2$ at 20 cm distance from antenna face.

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 Wi-Fi Switch'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."
Menu Items	Items in a menu, such as the tabs shown on the configuration web pages.
VP2200	This term refers to the Vivato VP2200 Wi-Fi Switch.
<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 Vivato Wi-Fi Switch operation. Failure to comply with this information may degrade or prevent Wi-Fi operation.
Caution 	This symbol identifies information that must be complied with to keep the Wi-Fi Switch from being damaged.
Warning 	This symbol identifies information that must be complied with to reduce the possibility of electrical shock or other injury.

Contact Information

For customer support:

For technical support, contact your Vivato reseller.

For firmware and documentation updates, go to www.vivato.net and select the **Customer Support** link. If you have already registered your product, the password e-mailed to you after registering, and your e-mail address, are used to access the support site. If you have not registered your product, register it at www.vivato.net/wifiregistration.html to receive a password.

Mailing address:

Vivato, Inc.
12610 E. Mirabeau Parkway, Suite 900
Spokane, WA 99216, USA

To provide feedback on our documentation:

Feedback on the documentation shipped with the Vivato Wi-Fi Switch 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.)

Gerry Caesar
Technical Publications
Vivato, Inc.

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

VIVATO, INC. END USER LIMITED WARRANTY AND LICENSE TERMS

Limited Warranty

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.

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

Safety Information 3

FCC Declaration of Conformity 4

Conventions Used in This Document 6

Contact Information 7

VIVATO, INC. END USER LIMITED WARRANTY AND LICENSE TERMS 9

Limited Warranty 9

END USER LICENSE 11

Introduction 21

Dual Mode Operation 21

Wireless Distribution System (WDS) Connectivity 21

Power Over Ethernet (PoE) 21

Basic Service Set Operation 21

“Out of the Box” Settings 22

VP2200 Wi-Fi Switch Installation 23

Shipping Contents 24

Where to Mount The Indoor VP2200 24

Analyzing Room Shape for Best Coverage 25

Ceiling Height Considerations 26

Minimizing Obstructions 27

Interfering Signal Sources 27

Environmental Considerations For Indoor Use 27

Mounting the VP2200 28

Mounting the Wall Plate to the Wall 30

Mounting Weight Considerations 31

Power Connection and Requirements 31

Connections to the Vivato VP2200 32

Media Access Control (MAC) Addresses in the VP2200 33

Command Line Interface 35

Command Levels 35

Connections and Terminal Settings 36

Accessing the CLI 37

Accessing the Configuration Level 38

Configuration Example 39

Navigating the CLI 40

Moving the Cursor Around on the Command Line 40

Using the “?” to Get Online Command Help 41

Using the Tab Key to Complete a Command 41

Command Mode Access and Prompts 41

Command Conventions 42

Read Level Command Descriptions 43

enable 43

exit 43

Ping 43

Show Commands 44

terminal length <0-512> 56

traceroute <ipaddress|hostname> 56

Enable Level Command Descriptions 57

Capture Packets Commands 57

configure [terminal] 58

Commands for Managing Configuration Files 58

Configure Clock Commands 61

Configure Crypto (Generate Keys) Commands 61

Configure EAP (802.1x) Commands 62

Configure No EAP (802.1x) Commands 65

Configure Enable Secret Commands 65

Configure HTTP-Server Commands 66

Configure Interface Commands 66

Configure No Interface Commands 84

Configure IP Commands 84

Configure Log Commands 86

Configure Multi-MAC Controller 86

Configure Radio 87

Configure RAPD Commands 87

Configure SNMP-Server Commands 88

Configure No SNMP-Server Commands 90

Configure System (boot system flash:) 91

Configure Username Admin (Read Level) Secret 91

Configure WDS (Wireless Distribution System) 91

disable 94

edit flash: 94

exit 95

no <configuration command> 95

reboot 95

support 95

Verifying Wi-Fi Operation 97

Verification Process 97

Wireless Client Does Not “Find” the Vivato VP2200 98

Wireless Client Cannot Access the Local Wired Network 99

Wireless Client Cannot Access an Outside Network 99

Unauthorized Clients Are Able to Associate With The VP2200 99

Network Monitoring 101

SNMP Operations 101

Supported MIBs 102

Enabling SNMP Operation 104

Introduction

The Vivato VP2200 Wi-Fi Switch is an unlicensed (FCC Part 15) wireless device operating in the 2.4 GHz band, providing network connections to Wi-Fi (IEEE 802.11b and 802.11g) client devices.

The VP2200 replaces previous micro cellular style Wi-Fi deployments, while providing the highest level of wireless security, system management, and switching capabilities.

The Switch's design allows point-to-point packet transmission to client devices through an integrated high gain, electronically steered transmitting antenna. The same antenna also functions as a high gain receiving antenna, allowing the Switch to receive signals from standard 802.11b/g clients, even at long distances or with high signal attenuation. This design allows one VP2200 to provide high bit rate network coverage to one or more floors of an office building or any other large space requiring Wi-Fi coverage.

Dual Mode Operation

The Vivato VP2200 works with both 802.11b and 802.11g devices operating in the 2.4 GHz instrumentation, medical, and industrial (ISM) frequency band. Data rates for 802.11b operation are as high as 11 Mbps, and up to 54 Mbps for 802.11g operation.

Wireless Distribution System (WDS) Connectivity

The Vivato VP2200 extends in the line of WDS-ready Vivato Wi-Fi products that can be used to provide a secure wireless “backhaul” connection to another Vivato Wi-Fi Switch or Vivato Bridge/Router. Using a WDS connection, Vivato Wi-Fi products can easily and inexpensively fill previously blocked coverage areas where a wired LAN connection does not exist and would be impractical and/or expensive to provide.

Power Over Ethernet (PoE)

The highly-efficient VP2200 gets its power through one of its RJ-45 Ethernet connections using a supplied power injector. This provides the flexibility of supplying power to the VP2200 from the most convenient location anywhere along its LAN connection; eliminating the need to provide AC (mains) power at the VP2200's location.

Basic Service Set Operation

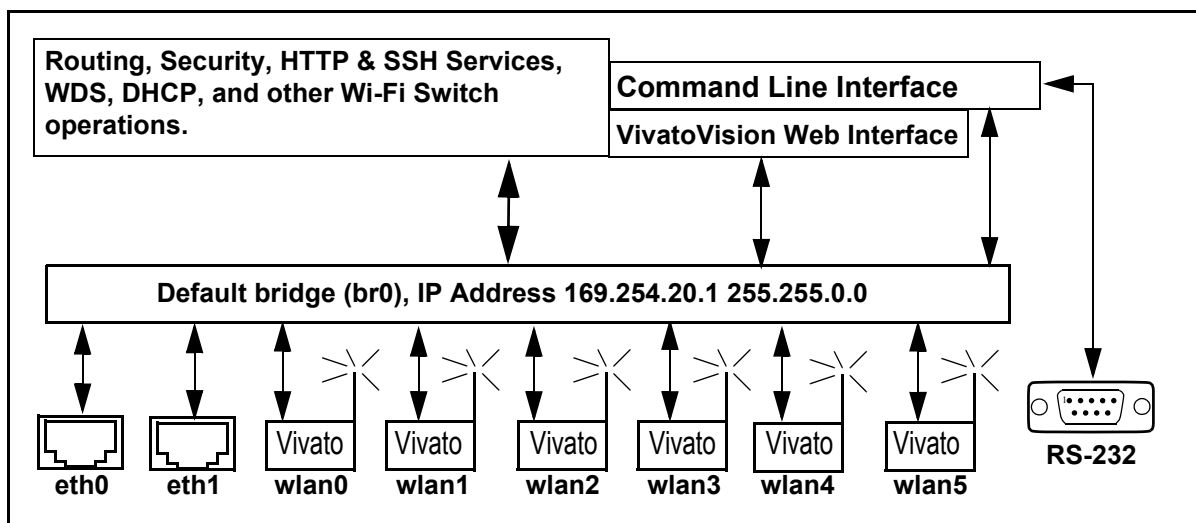
The VP2200 supports infrastructure basic service set (BSS) operation, providing all network communications between Wi-Fi clients and the wired network within the area of coverage. Independent basic service set (IBSS) operation, where clients can communicate directly with each other without using the Switch, is not supported.

“Out of the Box” Settings

The VP2200 is shipped with a default bridge connecting all of the Ethernet and wireless interfaces together. A default IP address is assigned to the bridge: 169.254.20.1. The wireless interfaces are enabled and are set to broadcast “Vivato” as the ESSID. These settings allow configuration changes to be made using the built-in VivatoVision™ web pages or using the command line interface (CLI), and can be accessed using either a wired or a wireless connection.

Using this configuration, an IP address does not need to be assigned to any of the Ethernet or wireless interfaces in order to pass traffic to the VP2200’s routing functions. Instead, all traffic passes through the default bridge using its IP address. When the Quick Setup VivatoVision web pages are used to configure the Switch, the IP address that you enter is applied to the bridge.

Note: No security is initially enabled, so don’t connect the Wi-Fi Switch to your secure wired network until security has been configured!



VP2200 Wi-Fi Switch Installation

The person installing the Vivato VP2200 must be qualified by Vivato, Inc. or by a Vivato authorized reseller.

We recommend that you prepare your VP2200 for operation in the following order:

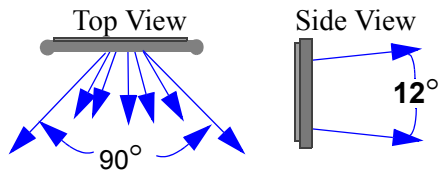
- 1 Verify the contents of the shipping container. See "[Shipping Contents](#)" on page 24.
- 2 **Register your VP2200!** Registering your Switch provides you with a password to access the Vivato Customer Support website, where the latest product release notes, Switch firmware, and application information can be viewed and downloaded. You can select **Register Online Now!** here or on the Vivato CD startup page, or go to <http://www.vivato.net/wifiregistration.html>.
- 3 Analyze your site to determine the best place to mount the VP2200. See "[Where to Mount The Indoor VP2200](#)" on page 24.
- 4 Configure the VP2200. You can configure the Switch before or after mounting it. However, it may be more convenient to perform the initial configuration before mounting the Switch on a wall.
- 5 Mount the VP2200. See "[Mounting the VP2200](#)" on page 28.
- 6 If not already connected, connect the power injector to the VP2200 and to your LAN. See "[Connections to the Vivato VP2200](#)" on page 32.
- 7 Verify VP2200 operation using your Wi-Fi client. See "[Verifying Wi-Fi Operation](#)" on page 97.

Shipping Contents

The following items are included in the shipping container with the VP2200:

- Vivato VP2200 Wi-Fi Switch.
- DB-9 null modem cable
- 100 Base-T Ethernet cable (white)
- 100 Base-T cable cross-over Ethernet (red)
- Power-over-Ethernet (POE) power supply.
- Four 1/4" flat washers
- Four 1/4" hex head screws
- Four drywall anchors
- Quick Configuration Guide (11" x 17" sheet)
- User Guide CD-ROM: includes user documentation, management information bases (MIBs), and PDF copies of the Quick Configuration sheet and the Command Line Interface Quick Reference.
- Command Line Interface Quick Reference (11" x 17" sheet, 3-fold)

Where to Mount The Indoor VP2200



The VP2200's antenna is designed to transmit and receive signals primarily in a 90° pattern from side to side (horizontally), and at about 12° pattern vertically. However, Wi-Fi operation outside of this pattern is typically available, especially near the VP2200. Also, various surfaces in the indoor environment can reflect

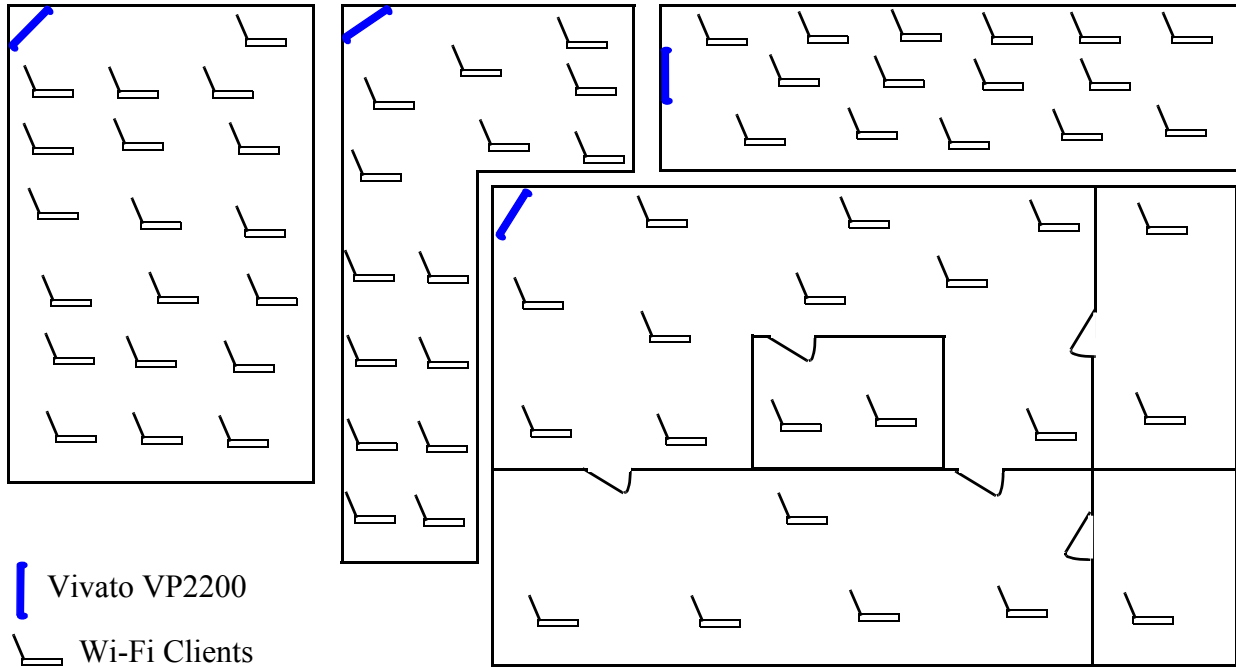
signals inside the antenna's defined pattern, often providing Wi-Fi operation outside of line-of-sight conditions.

Where you mount the VP2200 depends on a number of factors, including:

- room shape and dimensions
- ceiling height
- 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...)

Analyzing Room Shape for Best Coverage

In general, position the VP2200 to provide the greatest line of site access to the farthest clients. Mounting the switch in the corner of an open room is often the best solution. In an elongated rectangular room, mounting the VP2200 on an end wall works well.



Ceiling Height Considerations

You should mount the VP2200 several feet above any cubicle walls or other nearby obstructions. In a typical single-floor indoor environment with 9 to 12 ft (about 3 to 4 m) high ceilings, mount the top edge of the VP2200 close to the ceiling.

The figure below shows an open office where the ceiling is very high, and where clients are on more than one level. Location #4 is too low, being at the same height as office cubicle walls, much of the signal is blocked and the Switch's antenna pattern is not allowed to be fully focused (see [Minimizing Obstructions](#) below).

Location #3 is high enough to provide coverage to both levels of cubicles in this building. However, if the building were much longer or higher, locating the VP2200 higher would be beneficial.

Location #2 positions the VP2200 higher on the wall to maximize coverage on distant clients, and is tilted slightly downward to provide good coverage to the nearest clients below it. This is often the best location where Wi-Fi operation is being provided to distant clients or where more than one building floor is being served.

Location #1, while providing some Wi-Fi operation to close clients, is poorly positioned because metallic air ducts are situated a short distance from, and directly in front of, the VP2200.

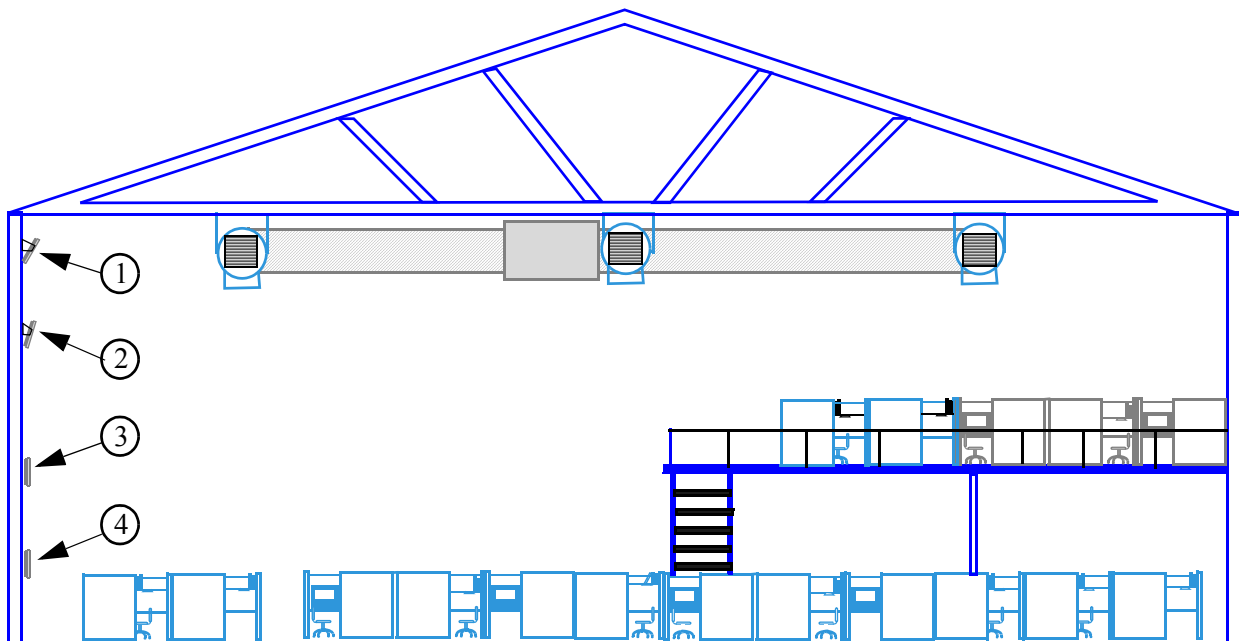


Figure 1—Location 2 Optimizes Wi-Fi Coverage

Minimizing Obstructions

Important 	The VP2200's antenna combines the signals of several elements into focused, low power antenna patterns. These patterns are fully focused at a distance of approximately 16 feet (about 5 meters) in front of the VP2200. To provide maximum coverage, it is important that objects are not placed closer than this distance directly in front of the VP2200. For example, do not position the VP2200 facing directly against a wall, window, or other surface to try to provide coverage on the other side of that object.
--	--

All materials provide some resistance to the wireless signal. However, very dense materials, such as metals and windows, degrade the signal more than less dense materials, such as cloth cubicle panels. To maximize the Wi-Fi coverage area and signal strength, position the VP2200 where there are no obstructions directly in front of it.

The VP2200's signal does go through typical gypsum (drywall) wall materials (with some signal loss) to provide Wi-Fi connectivity in conference rooms or other enclosed areas. However, metal duct work inside the walls, or machinery or appliances directly in the signal's path (heating, ventilation, air conditioning, electrical pannels...etc) cause additional decreases in the signal strength and may reduce the data rate to less than maximum.

Interfering Signal Sources

IEEE 802.11b/g devices share the same unlicensed frequency band as other common devices, such as some radio frequency identification (RFID) systems, some cordless telephones, wireless video links, and microwave ovens. These devices produce radio frequency (RF) energy that can interfere with the VP2200's signal. Whenever possible, you should eliminate or minimize the use of these devices within the switch's operating area in order to maximize Wi-Fi data rates.

The Vivato VP2200 uses the same frequencies as conventional access points (APs). To see if an access point is interfering, use the rogue access point detector (RAPD). See "[Appendix C: Assessing Traffic and Interference](#)" on page 207.

Environmental Considerations For Indoor Use

The following environmental specifications must be adhered to when mounting the Vivato VP2200:

- Operating temperature range: 32° to 122° F (0° to 50° C)
- Humidity: 10 % to 95% (non-condensing)

Mounting the VP2200

Use the supplied 4mm screws that thread into the VP2200 to a depth of ~0.5 inch.

Warning



The Vivato VP2200 must be fastened to a surface that can support its weight without compromising safety in the event of strong vibration (such as an earthquake) or from physical impact. Mounting the Vivato VP2200 in a manner that provides continued safety for persons and property is the sole responsibility of the installer.

The installer of the Vivato VP2200 is also responsible for complying with any applicable building and wiring regulations or codes.

Caution



The VP2200 is specifically designed to be operated with the power and data connectors positioned as shown below. Do not rotate the VP2200 to re-orient the connectors.

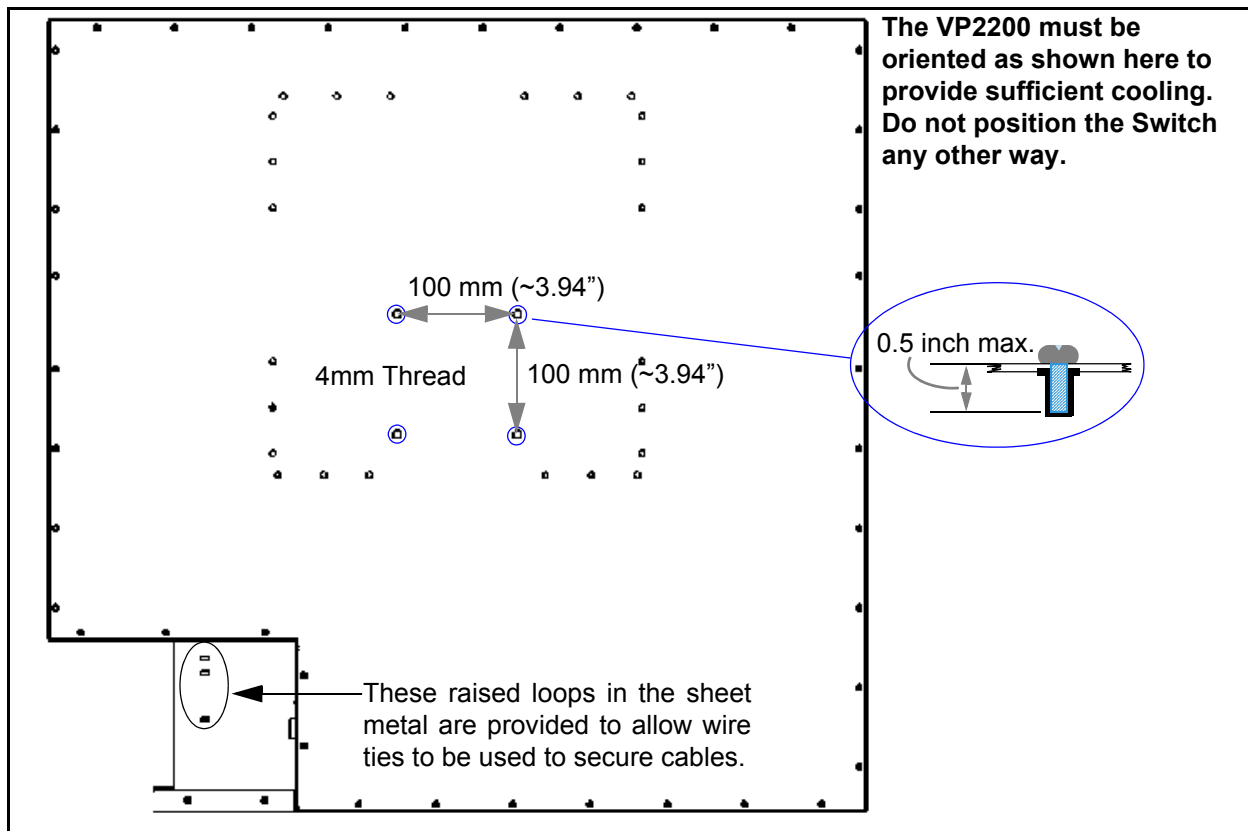


Figure 2—Back Panel Mounting Point Locations

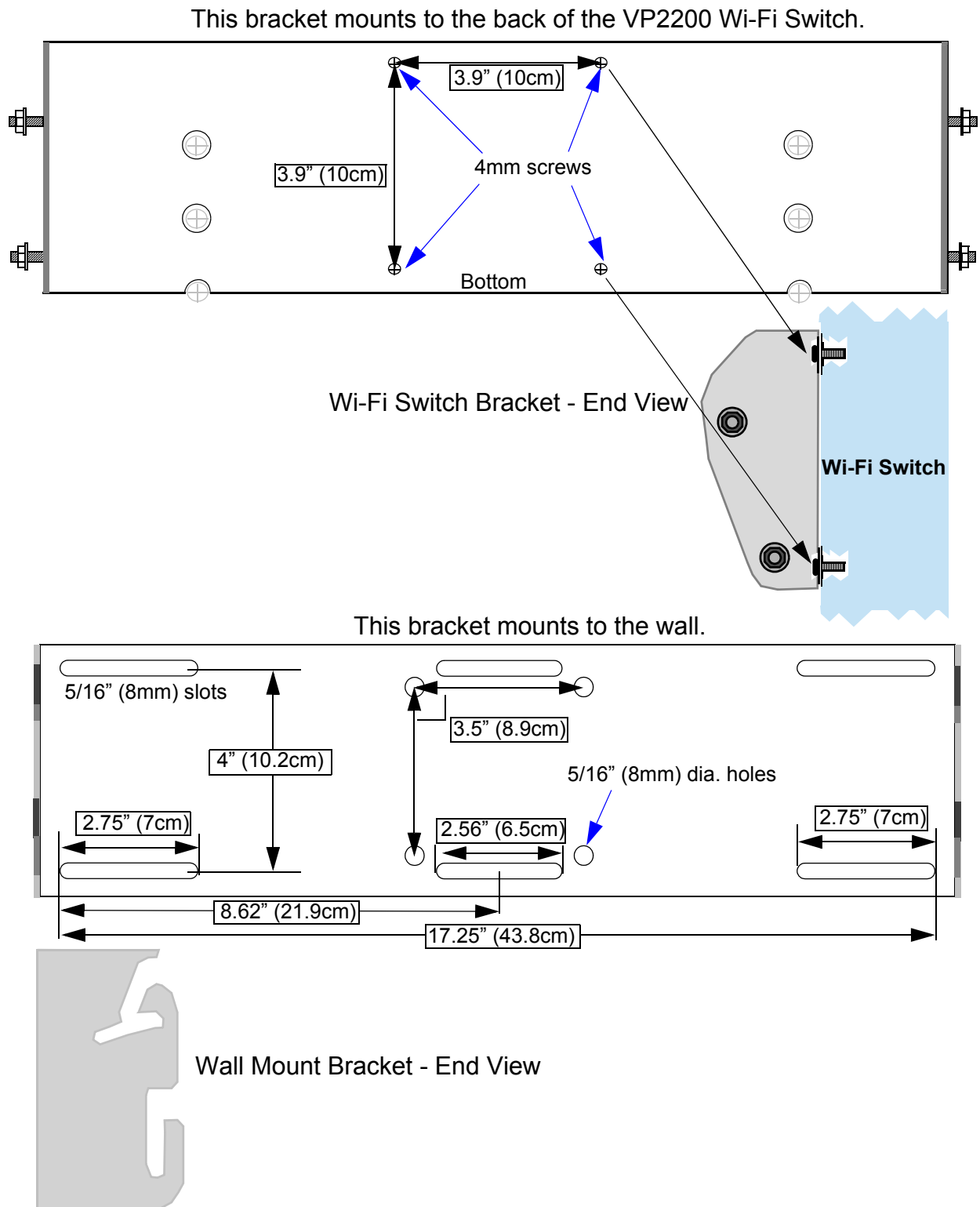


Figure 3—Identifying and Attaching the Supplied Wall Mount Parts

Mounting the Wall Plate to the Wall

Use the supplied drywall (gypsum board) anchors or hex head screws to mount the wall plate to your wall. *Note: The drywall anchors should only be used with 3/8" to 5/8" drywall.* A combination of drywall anchors and hex head screws can be used to accommodate building materials and building codes. Always comply with applicable building codes when mounting the Wi-Fi Switch.

To start, hold the wall bracket level at the intended mounting point on the wall and scribe through the mounting slots and/or holes you are going to use in order to identify where to place at least four of the supplied fasteners. Use one fastener at each corner of the mounting plate whenever possible.

Using the Supplied Drywall Anchors

- 1 Carefully drill a 7/16" hole for each anchor, making sure to keep the drill centered. (It may be easier to start with a 1/8" bit, and then drill again using the 7/16" bit.)
- 2 Insert the anchors into the 7/16" holes, and lightly tap on each anchor to seat it against the wall. See [Figure 4—Mounting the Wi-Fi Switch Using the Drywall Anchors](#).
- 3 Remove the anchor screws, and thread them through the flat washers and wall bracket and into the anchors until the screw heads are flush against the bracket.
- 4 Tighten the screws an additional 10 turns to seat the anchors - do not over-tighten. Verify that the bracket is level and adjust as necessary.

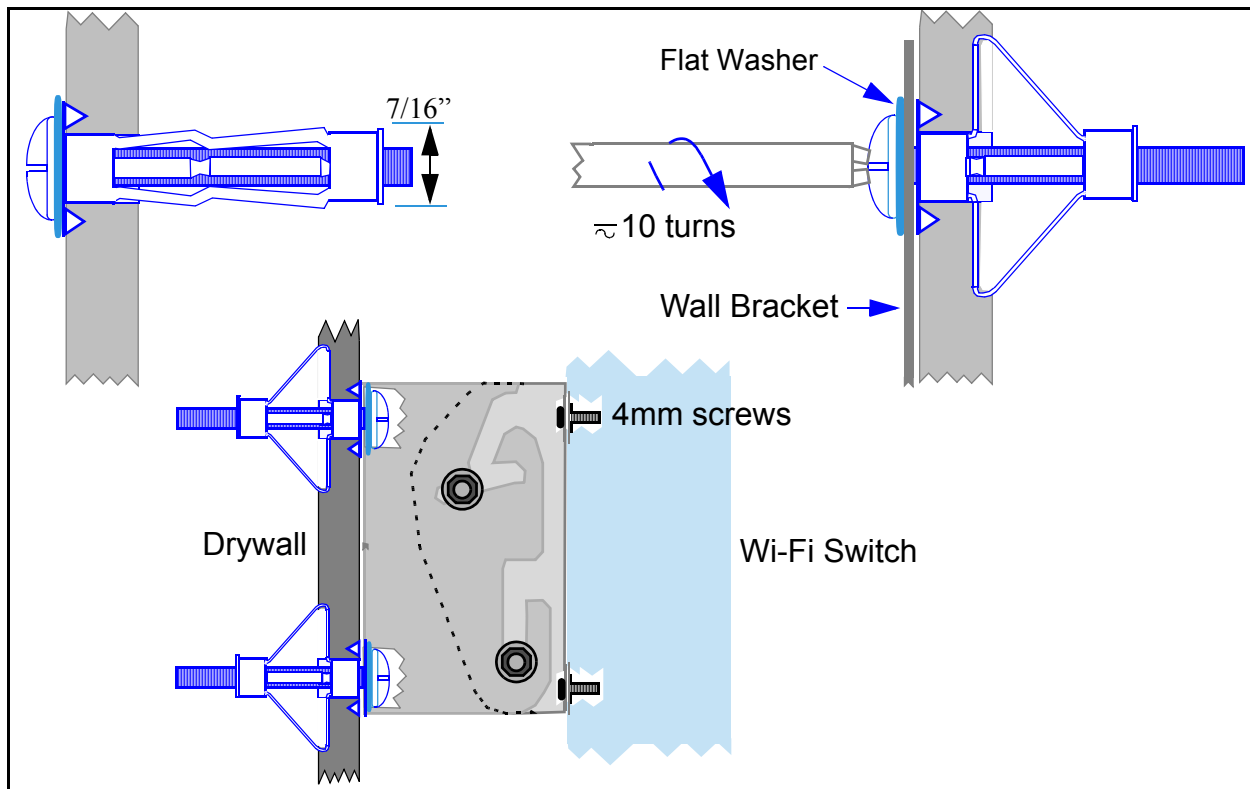


Figure 4—Mounting the Wi-Fi Switch Using the Drywall Anchors

Using the Supplied Hex Head Screws

Only use the hex head screws when they are being threaded into a wall stud or other dense wall structure that will not allow the screw to be pulled loose.

Step 1. To ease threading in the screws, drill a 1/8" pilot hole where each screw will be inserted.

Step 2. Insert one hex head screw through one of the supplied flat washers and through the wall plate hole or slot, and use a 1/2" socket wrench to thread the screw into its pilot hole - leaving the screw loose enough to allow the bracket to be easily repositioned.

Step 3. Insert the remaining screws through flat washers and the mounting plate.

Step 4. Tighten all of the screws until they pull the mounting plate firmly against the wall.

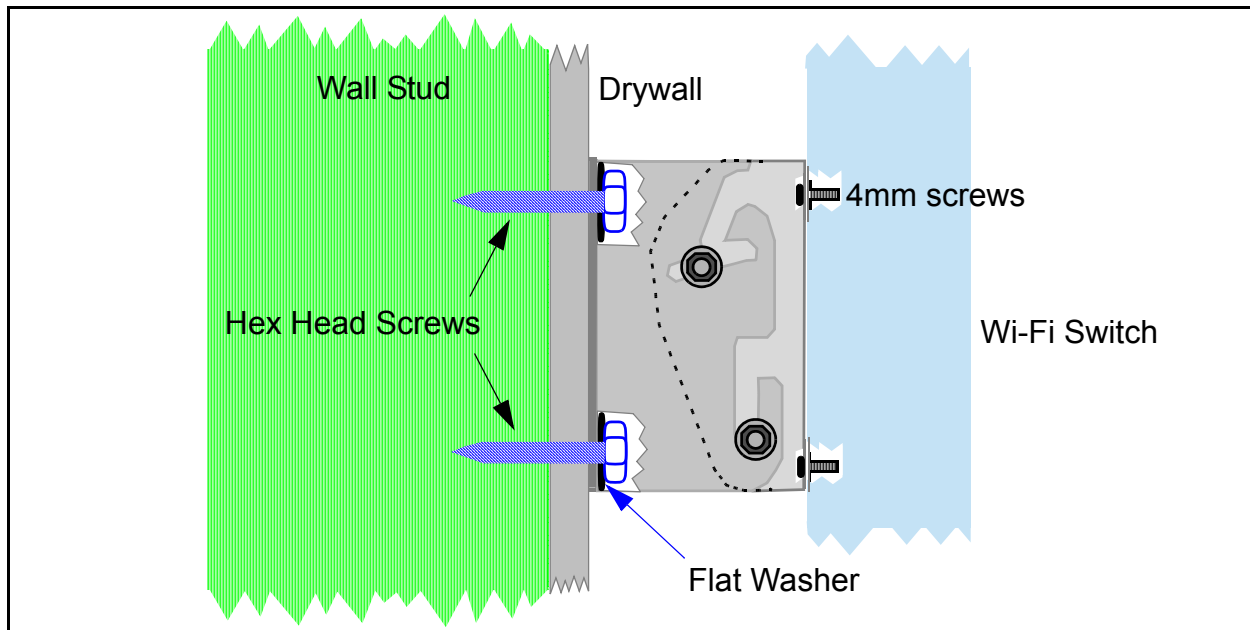


Figure 5—Mounting the Wi-Fi Switch Using the Hex Head Screws

Mounting Weight Considerations

The VP2200 Wi-Fi Switch weighs ~33 lbs (~15 kg).

Power Connection and Requirements

The Vivato VP2200 is powered using a factory-supplied integrated 48 VDC power-over-Ethernet (PoE) injector and power supply. A shielded twisted pair (STP) CAT-5 LAN cable is connected from the power supply's RJ-45 output connector to the VP2200's Eth0 RJ-45 connector. Another CAT5 LAN cable is connected from the power supply's data input to the wired network.

The PoE injector applies the 48 VDC to the normally unused wires in the Ethernet cable to supply power to the VP2200.

Caution



The factory-supplied power injector supply **MUST** be used with the factory-supplied STP CAT-5 (shielded) cable to power the Vivato VP2200. NEVER use a substitute power supply.

*Only the **eth0** port can be used to provide power to the VP2200 using the PoE injector. The eth1 port is not designed for PoE operation.*

Important



Do not exceed the maximum Ethernet cable length of 100 meters (about 328 feet) to the VP2200.

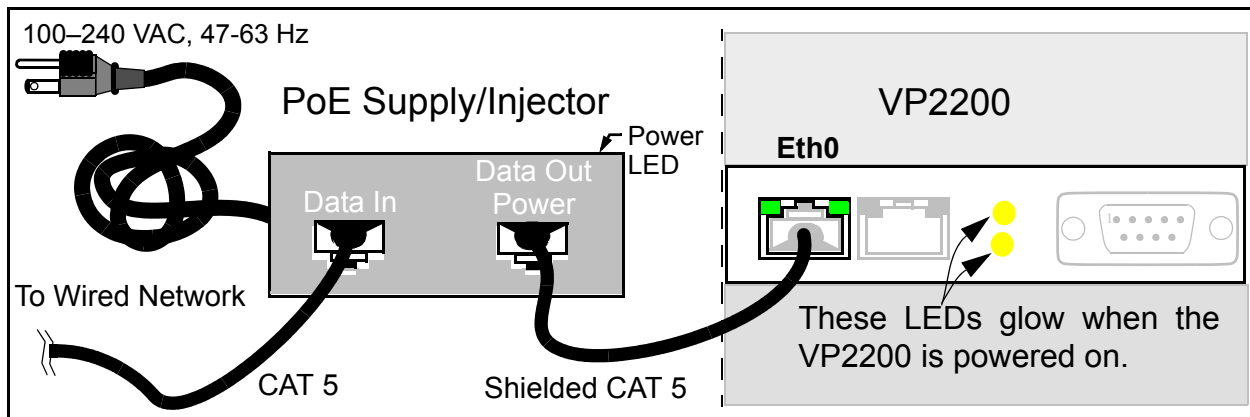


Figure 6—Power Connections to The VP2200

Power Supply Specifications:

- Line (mains) voltage: 100 – 240 VAC, 47 - 63 Hz.
- Maximum AC input current: ~1.5 A (180 Watts @ 120 VAC)
- Maximum VP2200 DC power requirement: 33.6 Watts (0.7 A @ 48 VDC)

Connections to the Vivato VP2200

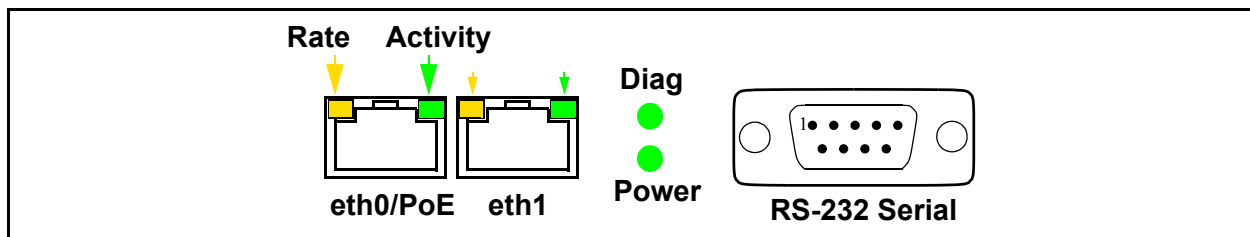


Figure 7—Connector Designations

Power LED - When lit, indicates that the VP2200 is powered on.

Diag LED - Used to track boot-up events. No user functions have been implemented at this time. Normally lit any time the VP2200 is powered on.

eth0/PoE RJ-45 - 10/100 Base-T Ethernet port and Power-Over-Ethernet (PoE). This non-autosensing port is enabled by default, and remains enabled unless you disable it during configuration.

eth1 - 10/100 Base-T Ethernet port. This non-autosensing port is enabled by default, and remains enabled unless you disable it during configuration.

Rate Indicators - Indicates the data rate of the link. This LED is off during a 10 Mbps link, and is on during a 100 Mbps link.

Link Activity Indicators - On but not blinking indicates a connection, but no link activity. Blinking indicates link activity. Not lit indicates no recognized connection to a device.

RS-232 Serial (m)- This serial communications (console) port is provided to access the command line interface (CLI) using a terminal emulator. These are the default settings:

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

Media Access Control (MAC) Addresses in the VP2200

The product label on the VP2200 lists the MAC address of that Switch. This is the MAC address that is assigned to the eth0 port and the default bridge (br0), and is also the “base” address that is incriminated (in hexadecimal) to create the MAC addresses assigned to the other interfaces on the VP2200. When making network connections that require entering the MAC address of the Switch, use the following table to determine the MAC address to enter. You can also use the command line interface (CLI) to view the MAC addresses. (The “xx:xx:x” values shown below are unique to each VP2200.)

Table 1—Interface MAC Address Assignments

Interface	MAC Address	Example
eth0	00:0B:33:xx:xx:xx	00:0B:33:00:34:10
eth1	00:0B:33:xx:xx:xx+1h	00:0B:33:00:34:11
wireless interface 0 (wlan0)	00:0B:33:xx:xx:xx+2h	00:0B:33:00:34:12
wireless interface 1	00:0B:33:xx:xx:xx+3h	00:0B:33:00:34:13
wireless interface 2	00:0B:33:xx:xx:xx+4h	00:0B:33:00:34:14
wireless interface 3	00:0B:33:xx:xx:xx+5h	00:0B:33:00:34:15
wireless interface 4	00:0B:33:xx:xx:xx+6h	00:0B:33:00:34:16
wireless interface 5	00:0B:33:xx:xx:xx+7h	00:0B:33:00:34:17

Command Line Interface

Refer to ["“Out of the Box” Settings"](#) on page 22 before performing additional configuration using the CLI.

The command line interface (CLI) is used to change settings and query values in the Vivato VP2200. The CLI can be used to initially configure the VP2200 for operation and to update the configuration after installation. Configuration files can be saved and retrieved to backup the configuration or to reconfigure the switch. The CLI can also be used to monitor activity during switch operation. Passwords are used to prevent unauthorized access to the CLI.

Caution



To prevent unauthorized access to the switch'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 Switch into service.

Understanding How the CLI is Used

[Command Levels](#)

[Connections and Terminal Settings](#)

[Accessing the CLI](#)

[Configuration Example](#)

[Navigating the CLI](#)

Command Descriptions

[Read Level Command Descriptions](#)

[Enable Level 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 switch and perform some troubleshooting operations.

The second command level is the **“enable”** level. Enable level commands are used to configure the switch. Every function in the Vivato VP2200 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 VP2200 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 VP2200's Eth0 Ethernet port. See "[Connections to the Vivato VP2200](#)" on page 32. Use the switch'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". Your network interface's IP address must be set to be able to work with the VP2200. See "[Enabling Your Network Adapter to Access the Wi-Fi Switch](#)" on page 36.
- Running a terminal emulator and connecting to the switch'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: None

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 switch 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 VP2200 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).

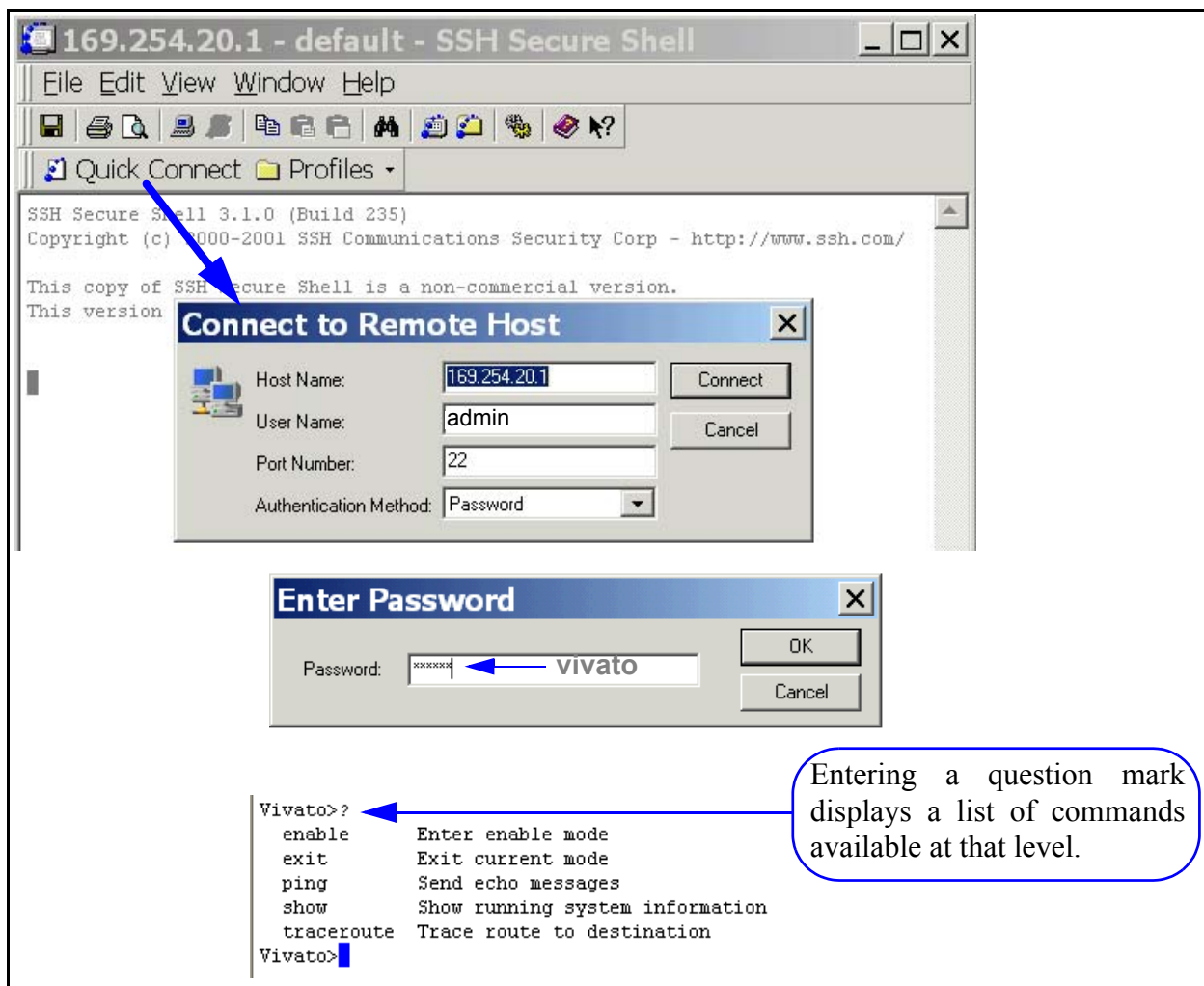


Figure 8—Using Secure Shell to Access the CLI and Display Read Level Commands

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 VP2200 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 VP2200.

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

Figure 9—Accessing the Global Configuration Level

Configuration Example

This example mimics setting the VP2200 to its *delivered default state* using a terminal program connected to the RS-232 (console) port through a null modem cable. Additionally, WEP security is configured and enabled.

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)# ssid Vivato	Set ESSID to Vivato

Configure WEP security

vivato (config-wlan-all)# key s:gmV8a18436572 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 two channel operation.

```
vivato (config)# interface wireless 0
vivato (config-wlan0)# channel 11
vivato (config-wlan0)# exit
vivato (config)# interface wireless 1
vivato (config-wlan1)# channel 11
vivato (config-wlan1)# exit
vivato (config)# interface wireless 2
vivato (config-wlan2)# channel 11
vivato (config-wlan2)# exit
vivato (config)# interface wireless 3
vivato (config-wlan3)# channel 11
vivato (config-wlan3)# exit
vivato (config)# interface wireless 4
vivato (config-wlan4)# channel 1
vivato (config-wlan45)# exit
vivato (config)# interface wireless 5
vivato (config-wlan5)# channel 1
vivato (config-wlan5)# 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 ethernet 1
vivato (config-br0)# add interface wireless 0
vivato (config-br0)# add interface wireless 1
```

Command Line Interface

Navigating the CLI

```
vivato (config-br0)# add interface wireless 2
vivato (config-br0)# add interface wireless 3
vivato (config-br0)# add interface wireless 4
vivato (config-br0)# add interface wireless 5
vivato (config-br0)# no shutdown
```

Specify the IP address and netmask for bridge 0 (br0). Unless you enter an IP address for another interface, this becomes the IP address for the VP2200 in your network.

```
vivato (config-br0)# ip address 169.254.20.1 255.255.0.0
vivato (config-br0)# exit
```

Generate the secure shell key and enable the secure shell daemon.

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

Enable the HTTP daemon for web access.

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

Ensure that 802.1x and VPN security are disabled.

```
vivato (config)# no eap
vivato (config)# no pptp
```

Enable Traffic Shaping and Multi-MAC Control

```
vivato (config)# ip traffic-shaping sfq
vivato (config)# mmc
```

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.

```
vivato (config)# username admin secret vivato<enter> Set the read level password.
vivato (config)# enable secret vivato <enter> Set the enable level password.
```

Save the configuration inside the VP2200 and end the configuration session.

```
vivato (config)# write
vivato (config)# exit
vivato# 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 2—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 “s **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 3—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”.

Table 3—Command Mode Navigation

Command Level	How to Access	Resulting Command Line Prompt	To Go Back to the Previous Level
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**. Never 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 switch 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 VP2200 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 10—Example “show arp” Output

show clock

Displays the system clock’s day, month, date, time, time zone, and year.

```
Vivato(config)#show clock
Fri May 16 10:39:33 UTC 2003
Vivato(config)#
```

show cpu

Displays system processor information, including the manufacturer and type, hardware revision number, relative performance (“bogomips”), and current operating temperature.

```
cpu           : 82xx
revision      : 16.20 (pvr 8081 1014)
bogomips      : 166.29
vendor        : Vivato
machine       : Riley
processor      : PVID: 0x80811014, vendor: Motorola
bus speed     : 100Mhz
cpu temp (F)  : 78
cpu temp (C)  : 25.5
Vivato#
```

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

show dhcp-server interface ethernet <0-3>

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

show dhcp-server interface vlan <1-4094>

Enter the VLAN ID number to display the DHCP settings for that interface.

show dhcp-server interface wireless <1-13>

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

show eap

Displays the current settings and configuration for extensible application protocol (EAP).

```
Vivato(config)#show eap
eapSrvr    Enabled
           Server 1 192.163.0.245 1812 5 1
           Secret 1 XXXXXX
           Authentication threshold:20    max_error:3
           Encryption threshold:5        max_error:3
           Ifname:br0
           NAS:eapclient1
           Conn-Info:CONNECT_11Mbps_802.11b

Vivato(config)#
```

Figure 12—Example “show eap” Output

show http-server

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

show interfaces

Displays information about bridge, ethernet, vlan, 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**”).

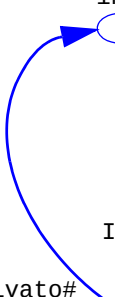
The Bridge ID consists of two values: the bridge’s priority setting is the value to the left of the decimal point (default is 8000), the lowest MAC address in the VP2200 is to the right of the decimal point. The priority setting is used by spanning tree protocol to determine which bridge has priority when multiple Switches 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 <1-13>](#).

```
Vivato#show interfaces bridge 0
br0      Link encap:Ethernet  HWaddr 00:0B:33:00:60:00
        inet addr:192.163.20.1 Bcast:192.163.20.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500
        RX packets:3779 error:0 dropped:0 overruns:0 frame:0
        TX packets:42 error:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        Interrupt:0 Base address::

        Bridge ID:8000.000b33006000, STP:Disabled
        Interface: eth0, eth1, wlan1, wlan2, wlan3, wlan4, wlan5, wlan6

Vivato#
```



“UP” Signifies that this interface is enabled.

Figure 13—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 14—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 \[0-3\]](#)

Displays the configuration for all or (optionally) a specific 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 <1-13>](#).

```
vivato(config)#show interfaces ethernet 0
eth0      Link encap:Ethernet  HWaddr 00:0B:33:00:60:00
          inet  addr:192.163.20.6    Bcast:192.163.20.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:6131 error:0 dropped:0 overruns:0 frame:0
          TX packets:236 error:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:16  Base address::0xd000
          Bridged : [br0]

vivato(config)#
```



“UP” Signifies that this interface is enabled.

Figure 15—Example “show interfaces ethernet” Output

show interfaces vlan [vlan id]

Displays the configuration of all or (optionally) a specific virtual local area network (VLAN), including configured MAC addresses for that VLAN, the transmit and receive statistics, and which interfaces are part of each VLAN.

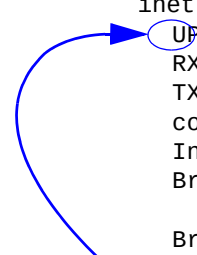
Also shown is the status of that interface. When the interface is enabled, “UP BROADCAST RUNNING MULTICAST” is displayed. If the interface is disabled, the “UP” part is removed (“BROADCAST RUNNING MULTICAST”).

For information on RX and TX packet statistics, see [show interfaces wireless <1-13>](#).

```
vivato#show interfaces vlan 3
vlan3      Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          inet  addr:192.163.20.44  Bcast:192.163.20.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:0 error:0 dropped:0 overruns:0 frame:0
          TX packets:0 error:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          Interrupt:0  Base address::
          Bridged : [no]

          Bridge ID:8000.000000000000, STP:Disabled

vivato#
```



“UP” Signifies that this interface is enabled.

Figure 16—Example “show interfaces vlan” Output

show interfaces vlan [vlan id] fdb

Enter the name of a VLAN to display the MAC values of packets that have been forwarded through that VLAN; also called the forwarding data base. A “local” device indicates an interface on the VP2200 that is part of this VLAN. The “ageing timer” lists the time elapsed since a device last began associating through the VLAN (in seconds).

```
Vivato#show interfaces vlan 3 fdb
vlan3:
port no mac addr          is local?    ageing timer
3      00:02:2d:66:53:8d   no           171.00
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
Vivato#
```

Figure 17—Example “show interfaces vlan fdb” 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 18—Example “show interfaces wireless 1” Output](#), for an example of what is displayed for each interface.

show interfaces wireless <1-13> associations

Displays information about clients associating through the specified wireless interface.

```
Vivato#show interfaces wireless 1 associations
WLAN MAC Addr      SNR Sig Noi  Rate      IP      Rx      Tx Idle
=====
1 00:00:00:00:00:00  0 -102 -102  0Mbps      0.0.0.0  0.0KB
0.0KB 278
1 -45              110 -84  39 19Mbps      2.3KB   3.2KB
198 (null)

Total number of associated stations = 1.
Vivato#
```

WDS connection information is not included (see [show interfaces wireless <1-13> wds <1-6>](#)).

show interfaces wireless <1-13>

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

- Link encap: 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 VP2200 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 VP2200 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-ssid**" on page 80.
- 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 80.
- Sensitivity: See "[sensitivity <1-5>](#)" on page 83.
- 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 18—Example "show interfaces wireless 1" Output

[show interfaces wireless <1-13> 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 <1-13>](#) 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 dhcp-client

Displays IP assignment information for any interfaces that are configured to use dynamic host control protocol (DHCP) to obtain an IP address from a DHCP server on the network.

```
Vivato# show ip dhcp-client
DHCP client status for br0:
  ip-address 192.168.10.157
  netmask 255.255.255.0
  broadcast-address 192.168.10.255
  gateway 192.168.10.247
  name-server 192.168.10.135
  name-server 192.168.10.198
  domain-name mabuhay
  lease-time 3600
  server-address 192.168.10.135
  server-hwaddr 00:03:47:B0:C7:4B

Vivato#
```

show ip domainname

Displays the domain name for the VP2200.

show ip host

Displays the host table for the VP2200, containing host names and their IP addresses.

show ip hostname

Displays the host name for the VP2200.

show ip nameserver

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

show ip route

Displays IP routing information for the VP2200. 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 vlan3. All hosts on the 195.145.0.0 network can be accessed directly through interface vlan3. 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 4—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	vlan3
195.145.0.0	0.0.0.0	255.255.255.0	U	0	0	0	vlan3
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 <1-13>|ethernet <1-3>|bridge <0-4094>|vlan <1-4094>)** command, that interface is also listed.

show ip traffic-shaping

Displays the state of traffic shaping: enabled or disabled.

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 switch.

show mmc

Displays the status of the multi-MAC control feature. See "**Configure Multi-MAC Controller**" on page 86.

show pptp

Displays the status and configuration for point to point tunneling protocol (PPTP) security.

```
Vivato(config)#show pptp
pptpSrvr  Enabled
          Auth:chap
          CHAP SECRETS: XXXXXX
          Listen:192.163.20.100
          LocalIP:10.0.2.200
          RemoteIP:192.163.20.1-99
          MS-DNS primary: 10.0.2.245
          MS-WINS primary: 10.0.2.240
Vivato(config)#
```

Figure 19—Example “show pptp” Output

show rapd

Displays the SSID, MAC, channel number, and signal strength (dBm) of access points detected at each pointing direction in the VP2200's antenna pattern (see "[interface wireless <1-13>all](#)" on page 79). The results for each detected signal are only displayed for the channel with the greatest signal strength for any MAC address.

MAC Addr	SSID	ch	Pointing Direction (Signal dBm) (Behind Panel Left to Right)												
			1	2	3	4	5	6	7	8	9	10	11	12	13
00:0b:33:01:03:e9	Vivato	11	0	0	0	0	0	-72	0	0	0	0	0	0	0
00:0b:33:01:04:29	long_ap	1	0	0	0	0	0	-59	0	0	0	0	0	0	0
00:0b:33:01:04:4b	larrys	11	0	0	0	0	0	-85	0	0	0	0	0	0	0
00:0b:33:01:04:50	larrys	11	0	0	0	0	0	-91	0	0	0	0	0	0	0
00:0b:33:01:04:f2	bjo-tes	11	0	0	0	0	0	-85	0	0	0	0	0	0	0
00:0b:33:01:05:a9	jt_ap	11	0	0	0	0	0	-81	0	0	0	0	0	0	0
00:0b:33:01:05:aa	jt_ap	11	0	0	0	0	0	-76	0	0	0	0	0	0	0
00:0b:33:01:06:09	sidley	1	0	0	0	0	0	-73	0	0	0	0	0	0	0
00:40:96:54:77:64	C350_AP	11	0	0	0	0	0	-67	0	0	0	0	0	0	0

Figure 20—Example “show rapd” Output

show rapd-full

Displays the SSID, MAC, channel number, and signal to noise ration (SNR) of access points detected at each pointing direction in the VP2200's antenna pattern (see "[interface wireless <1-13>all](#)" on page 79). Because a signal can “bleed over” into an adjacent channel, the power of the signal with a particular MAC address may be displayed for more than one channel (as shown in the example below).

MAC Addr	SSID	chan	Pointing Direction (SNR) (Behind Panel Left to Right)												
			1	2	3	4	5	6	7	8	9	10	11	12	13
00:0b:33:01:04:50	larrys_ppc8	10	0	0	0	0	0	2	0	0	0	0	0	0	0
00:0b:33:01:04:50	larrys_ppc8	11	0	0	0	0	0	5	0	0	0	0	0	0	0
00:0b:33:01:04:f2	bjo-test	10	0	0	0	0	0	12	0	0	0	0	0	0	0
00:0b:33:01:04:f2	bjo-test	11	0	0	0	0	0	8	0	0	0	0	0	0	0
00:0b:33:01:05:a9	jt_ap	10	0	0	0	0	0	1	0	0	0	0	0	0	0
00:0b:33:01:05:a9	jt_ap	11	0	0	0	0	0	16	0	0	0	0	0	0	0
00:0b:33:01:05:aa	jt_ap	10	0	0	0	0	0	15	0	0	0	0	0	0	0
00:0b:33:01:05:aa	jt_ap	11	0	0	0	0	0	19	0	0	0	0	0	0	0
00:0b:33:01:06:09	sidley	1	0	0	0	0	0	24	0	0	0	0	0	0	0
00:0b:33:01:06:09	sidley	2	0	0	0	0	0	26	0	0	0	0	0	0	0
00:0b:33:01:06:09	sidley	3	0	0	0	0	0	5	0	0	0	0	0	0	0
00:40:96:54:77:64	C350_AP	10	0	0	0	0	0	31	0	0	0	0	0	0	0
00:40:96:54:77:64	C350_AP	11	0	0	0	0	0	24	0	0	0	0	0	0	0

Figure 21—Example “show rapd-full” Output

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 R0
snmp-server community private RW
snmp-server community icehouse RW 192.163.20.1
snmp-server engineID A52D
snmp-server
!
harvey(config)#
```

Figure 22—Example “show snmp-server” Output

show uptime

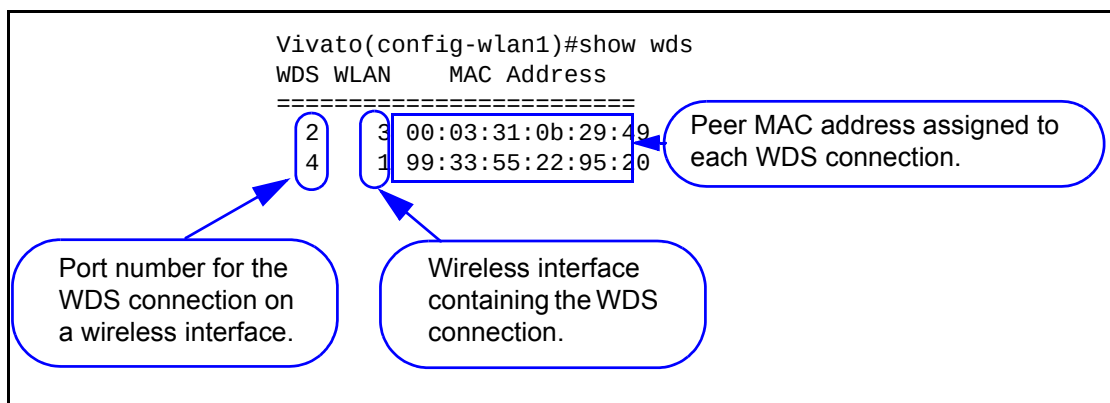
Displays the of day, how long the switch has been up since it was last rebooted (days, hours, minutes), the number of users that have accessed the switch, and the average load through the switch.

show version [merlin|bootloader]

Displays the product serial number, base MAC address for the VP2200, and the versions of software (“Vino Version”), boot loader code, and MAC controller code installed . The optional “merlin” and “bootloader” entries are used to only display the version of MAC controller and boot loader, respectively.

show wds

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



Enable Level Show Commands

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

show flash:

Displays the names of configuration files that have been saved in the VP2200. Configuration files are saved using the **write network flash:**.

show running-config

Displays the current running configuration of the VP2200, including any dynamic settings that are in effect.

terminal length <0-512>

Enter the maximum number of lines of information to display on the terminal at one time. Some show commands, such as **show running-config**, output several lines of information that may extend beyond the terminal window area. This command sets the maximum number of lines to send to a terminal before pausing and requiring the space bar to be pressed at the **--More--** prompt in order to show additional information. 0 = show all information without pausing.

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 VP2200 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 43).

Table 5—Enable Level Commands

"configure [terminal]" on page 58	"Configure No Interface Commands" on page 84
"Commands for Managing Configuration Files" on page 58	"Configure IP Commands" on page 84
"Configure System (boot system flash:)" on page 91	"Configure Log Commands" on page 86
"Configure Clock Commands" on page 61	"Configure Multi-MAC Controller" on page 86
"Configure Crypto (Generate Keys) Commands" on page 61	
"Configure EAP (802.1x) Commands" on page 62	
"Configure No EAP (802.1x) Commands" on page 65	
"Configure Enable Secret Commands" on page 65	"Configure Radio" on page 87
"Configure HTTP-Server Commands" on page 66	"Configure RAPD Commands" on page 87
"Configure Interface Commands" on page 66 "interface bridge <0-4094>" on page 66 "interface ethernet <0-3>" on page 72 "interface vlan <vlan id>" on page 74 "interface wireless <1-13 all>" on page 79	"Configure No SNMP-Server Commands" on page 90
"Configure SNMP-Server Commands" on page 88	
"Configure WDS (Wireless Distribution System)" on page 91	"Configure Username Admin (Read Level) Secret" on page 91
"disable" on page 94	"edit flash:" on page 94
"exit" on page 95	"reboot" on page 95
"support" on page 95	

Capture Packets Commands

The following commands are available to capture and store the first 68 bytes of each packet passing through an Ethernet or a wireless interface. A utility called “tcpdump” is used to capture and store the packets in a file called /conf/capture. . The capture file can be copied to another system for analysis using a software tool such as “tcpdump” or “Ethereal”. See www.tcpdump.org and www.ethereal.com for more information on these public domain utilities.

capture interface ethernet <0-3> count <1-10000>

This command is used to capture and store the first 68 bits of each packet on the specified Ethernet interface. Specify the interface number and the number of packets to capture: the default is 2000. To halt operation before the specified number of packets has been captured, press **Cntl-C**.

capture interface wireless <1-13> channel <1-11> count <1-10000>

This command is used to capture and store the first 68 bytes of each packet on the specified wireless interface and channel. Specify the wireless interface number, the channel to analyze,

and the number of packets to capture: the default is 2000. To halt operation before the specified number of packets has been captured, press **Cntl-C**.

This operation performs a “sniff” of all wireless traffic on the specified interface and channel. The captured data are 802.11 packets that include the management and control frames.

configure [terminal]

This command tells the CLI to use your terminal to configure the switch after accessing the enable level (see "**enable**" on page 43). 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 configuration files to configure the VP2200. All of these commands are available at the enable level prompt, **Vivato#**, but are not available at the configuration prompt, **Vivato(config)#**.

configure network flash:

This command is used to configure the switch 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 VP2200 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 VP2200, 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.

copy flash: flash:

This command is used to make a copy of an existing configuration file on the VP2200 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 VP2200 to another system. After entering this command, you are prompted to enter the name of the configuration file on the VP2200, 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.

Vivato#**copy flash: scp:**

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

Username: (Enter the user name to access the other device.)

Password: (Enter the password for that user name.)

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

Directory [/]: **/vivato_switch/configurations**

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

copy flash: tftp:

This command is used to copy a file on the VP2200 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. TFTP transfers can take several minutes to complete when large files are being copied.

For example, when using the **support** command to send in a copy of your configuration when requesting customer support for your Switch, 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: flash:

This command is used to copy a configuration file from another device to the VP2200. 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 VP2200 (as shown below):

Vivato#**copy scp: flash:**

Username: **gerry**

Password:

Hostname: **gardenhose**

Directory [/]: **wifibackups**

Source file: **north_switch_config**

Destination file [north_switch_config]: **renew_config**

copy tftp: flash:

This command is used to copy a file from another device to the VP2200 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 VP2200. A TFTP server must be running on the source device to enable the file transfer.

TFTP transfers can take several minutes to complete when large files are being copied.

delete flash: <filename>

Enter the name of a configuration file to remove from the VP2200's memory. Use the **show flash:** command to see what configuration files have been saved.

dir

List the contents of the VP2200'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 VP2200'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 [/]: **wifiswitch/backups**

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

write terminal

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

Configure Clock Commands

The system clock is configured using the following commands:

clock set <hour> <minutes> <seconds> <day> <month> <year>

Enter the time and date information to set the system clock. The “month” entry is the first three letters of that month, such as “Apr” for April. Example: **clock set 14 30 00 10 Apr 2003** sets the clock to 2:30 PM, 10 April, 2003.

clock timezone

Enter the timezone in hours relative to Greenwich Mean Time (GMT). For example, pacific standard time in the United States is 8 hours after GMT, and would be set using the following command: **clock set timezone GMT-8**.

By entering **clock timezone ?** you can view the names of some cities and countries and their time zones.

Configure Crypto (Generate Keys) Commands

Use the following commands to configure the VP2200 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 VP2200 through its configuration web pages or when connecting using a secure shell. These keys are automatically generated whenever the VP2200 is rebooted, but you can regenerate these keys using this command.

See **"ip ssh genkey"** on page 85 to enable secure shell operation on the VP2200. This command also provides regeneration of the encryption keys.

Configure EAP (802.1x) Commands

The following commands are available for setting up 802.1x extensible authentication protocol (EAP), transport layer security (TLS), and protected EAP (PEAP). See "[Configuring EAP \(802.1x\) in Your Client](#)" on page 109 for setting up clients to use EAP/PEAP.

See "[Configure No EAP \(802.1x\) Commands](#)" on page 65 to disable EAP security.

Windows 2000 Internet Access Server Setup

Use the following guidelines when configuring EAP/TLS/PEAP on your Windows 2000 IAS to work with the Vivato VP2200. For more information on configuring Microsoft® Windows® XP clients and a Windows 2000® Internet Access Server (Win2K IAS) for EAP or PEAP security, see *Windows XP Win2kIAS Deployment.pdf*© on the Vivato VP2200 Wi-Fi Switch CD.

To work with Win2K IAS, users should be grouped based on the VLAN ID in the Active Directory. A policy for each user group must be added by, 1) setting the "Windows Group" as the "condition to match" and selecting the user group, and 2) adding the three tunneling attributes specified in item #4 below (VLAN Configuration).

(1) **Encryption Key Length** - Set by **Profile>Encryption**: Use either (a) Basic : 64 bit key, or (b) Strongest: 128 bit key. Regardless of the type of RADIUS server used, encryption must conform to RFC 2548 MS-MPPE-Encryption-Types.

(2) **Session Timeout** - Set by **Profile>Dial-in Constraint>Restrict Maximum Session To**: Value: session timeout period (minutes). When a client reaches session timeout, the VP2200 forces the client to re-authenticate and deliver new session key. Regardless of the type of RADIUS server used, operation must conform to RFC 2865 Attribute Type 27.

(3) **Key Refresh Timeout** - Set by **Profile>Advanced>Vendor Specific Attribute**: Vendor code: 14615 Confirm to RADIUS RFC: Yes. Vendor Type: 60. Attribute format: Decimal. Attribute value: key refresh period (minute). When a client reaches key refresh timeout, the VP2200 delivers a new session key to the client.

The administrator may configure: (a) Key refresh and session timeout. (b) Key refresh only. (c) Session timeout only. If Key Refresh Timeout $\geq$ Session Timeout, the Key Refresh Timeout is ignored.

(4) **VLAN Configuration** (only when VLANs are used)- Set by **Profile>Advanced**:¹

- **Tunnel-Medium-Type**: value = 6, (802 media)
- **Tunnel-Type**: value = 13, (VLAN)
- **Tunnel-Private-Group-ID**: value = ASCII coded VLAN ID (a string without a null terminator).
This is the VLAN in the VP2200 that clients are assigned to after authentication.

After a client is authenticated, if its VLAN is configured, the client MAC address is added to the configured VLAN by the VP2200. If there is no VLAN configuration for the client, then:

- (a) if there is default VLAN configured on the VP2200, then the client is added to default VLAN, if not...
- (b) the client data packets are dropped by the switch.

If item 1 is changed on the Windows 2000 IAS, then the VP2200 needs to be rebooted in order to force all clients to re-authenticate using the new policy. Items 2, 3, and 4 can be changed and applied to the next authenticated client without system reboot.

VP2200 802.1x Configuration Example

The following example shows how 802.1x may be configured on the VP2200 to work with Windows 2000 IAS:

Note: When making changes to an existing 802.1x configuration, you should disable 802.1x before making the changes, and then re-enable 802.1x after making the changes to re-initialize 802.1x using the new configuration.

```
vivato (config)# no eap
vivato (config)# eap server 1 191.173.0.149 1812 5 3
vivato (config)# eap secret 1 authserveronesecretforpeap
vivato (config)# eap max-auth-error 3
vivato (config)# eap max-encrypt-error 3
vivato (config)# eap auth-threshold 20
vivato (config)# eap encrypt-threshold 5
vivato (config)# eap ifname interface bridge 0
vivato (config)# eap nas myauthclient
vivato (config)# eap conn-info CONNECT_11Mbps_802.11b
vivato (config)# eap
```

eap

Enable the EAP security daemon. This command must be issued before EAP can be used, and re-issued after making any changes to the EAP configuration. The default EAP state is disabled.

1. These tunneling attributes must be set regardless of the type of RADIUS server you are using.

eap auth-threshold <1-60>

The amount of time, in minutes, used to measure client authentication errors for the **eap max-auth-error <1-10>** command. The value must be in the range of 1 to 60; 20 is typical.

eap conn-info <text>

Enter the connection information required by the RADIUS server. The default is set for Win2000 IAS as follows: CONNECT_11Mbps_802.11b. Other RADIUS servers may have different settings.

eap encrypt-threshold <1-10>

Enter the length of time, in minutes, that the **eap max-encrypt-error <1-10>** command uses to measure encryption errors in packets before disassociating the client from the VP2200. The value must be in the range of 1 to 10; 5 is typical.

eap ifname interface <bridge 0-4094|vlan 1-4094>

Enter the name of the interface used to access the RADIUS authentication server, such as "bridge 0". An IP address must be assigned to this interface and the interface must be currently enabled, otherwise the setting is not made and an error message is displayed.

eap max-auth-error <1-10>

Enter the maximum amount of authentication errors that occur within the time specified by the auth-threshold that are allowed during the authentication attempt before an authentication failure is reported and the client is blocked from further authentication attempts. The range is 1-10; 3 is typical.

eap max-encrypt-error <1-10>

Enter the maximum number of encryption errors from the client that are allowed during the time specified in **eap encrypt-threshold <1-10>** before an authentication failure is reported. The range is 1-10; 3 is typical.

eap nas <text>

Enter the name *configured on the RADIUS server* that is used to identify the VP2200.

eap secret <secret number(1-4)> <secret>

Enter the RADIUS authentication server secret number in the range of 1 to 4, and the shared secret string in the range of 22 to 255 characters. The secret appears as clear text as it is entered.

eap secret <secret number(1-4)> <ENTER> (prompt) <secret>

Enter the RADIUS authentication server secret number in the range of 1 to 4, and press the **Enter** key. You are prompted to enter the shared secret string in the range of 22 to 255 characters. The secret is not displayed as it is entered. The secret must be entered twice before it is changed.

eap server <RADIUS Server id(1-4)> <ipaddress> <portnum> <timeout> <max retry>

This command specifies the RADIUS server to use to authenticate clients and its operating conditions. Enter the RADIUS Server ID to specify the priority level of the specified server, from 1 (highest priority) to 4 (lowest priority). If the primary server (1) is not found, the VP2200 attempts to use the next server in numerical order. You also need to enter the IP address and port number for accessing the RADIUS server. The timeout value is the maximum number of seconds to wait for a reply from the RADIUS server after an authentication request is sent: range 5-30 seconds, typical = 5. Enter the maximum number of times a packet is re-transmitted to the RADIUS server without a reply from the server before ending the authentication attempt: range 1-3, typical=1.

Configure No EAP (802.1x) Commands

The following command is used to turn off 802.1x security. See "**Configure EAP (802.1x) Commands**" on page 62 for configuring 802.1x security.

no eap

Disable 802.1x security.

no eap server <RADIUS Server ID (1-4)> <ipaddress> <portnum> <timeout> <max retry>

Enter the device number of the RADIUS server that is providing 802.1x security in order to stop authenticating through this server.

Configure Enable Secret Commands

The enable password must be entered before the configuration of the VP2200 can be changed.

When using a secure shell or a terminal connection to access the VP2200, 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 VP2200, 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 VP2200’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.

http-server redirect

Enter this command to redirect authenticated clients to a special web page that requires the user to enter identifying information before being allowed access through the VP2200’s backhaul. Once the information is supplied, it is added to the “jail” information and the client is allowed access to the backhaul. The next time that client authenticates, the VP2200 sees its identifying information in the jail and allows access to the backhaul without requiring the identification information to be entered again.

no http-server redirect

Enter this command to disable the http redirect feature.

no http-server

Disable the http daemon.

Configure Interface Commands

The following commands are used to configure the ethernet and wireless interfaces in the switch.

DHCP Server Operation

Dynamic host configuration protocol (DHCP) is used to automatically assign IP addresses to clients associating through the VP2200. The bridge, Ethernet, VLAN, 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.

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 two RJ-45 Ethernet interfaces (eth0 & eth1) 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.

Important 	Use EITHER bridges OR VLANs to connect interfaces. Do not attempt to use VLANs and bridges at the same time. If VLANs are being used, be sure to DELETE the default bridge (br0) and any other bridges before configuring VLANs. If bridges are being used, do not configure any VLANs.
---	---

add interface ethernet <0-3>

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

Note: An ethernet interface cannot be added to the bridge if an IP address has been assigned to that interface. Remove the IP address from that interface in order to add it to the bridge. The IP address of the bridge is then used to access this port (and any other ports) on the bridge.

no add interface ethernet <0-3>

Remove the specified Ethernet interface from this bridge.

add interface wireless <1-13>

Enter the number of the wireless interface to add to the bridge. *Note:* A wireless interface cannot be added to the bridge if an IP address has been assigned to that interface. Remove the IP address from that interface in order to add it to the bridge. The IP address of the bridge is then used to access this port (and any other ports) on the bridge.

no add interface wireless <1-13>

Remove the specified wireless interface from this bridge.

add interface wireless <1-13> 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 91.

Note: A WDS interface cannot be added to the bridge if an IP address has been assigned to that interface. Remove the IP address from that interface in order to add it to the bridge. The IP address of the bridge is then used to access this port (and any other ports) on the bridge.

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.

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 VP2200. 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.

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 0-3|wireless 1-13> <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 1-13> 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.

port-priority <ethernet 0-3|wireless 1-13> <0-255>

Enter the port priority for a specific port on the bridge. The port priority is used in the spanning tree protocol to determine which port to use when a bridge has two ports connected to the same network; resulting in a loop. The port with the lower priority number is used.

port-priority <wireless 1-13> wds <1-6> <0-255>

Enter the port priority for a specific wireless distribution system (WDS) port on the bridge. The port priority is used in the spanning tree protocol to determine which port to use when

a bridge has two ports connected to the same network; resulting in a loop. The port with the lower priority number is used.

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. The default value is 32768, and is reset anytime the “no priority” command is issued.

no priority

Reset the bridge priority to the default value of 32768.

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 46.

shutdown

Disable the bridge.

source-nat interface <bridge <0-4094>|ethernet <0-3>|vlan <1-4094>|wireless <1-13>>

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 <0-3>

Enter the number of the ethernet interface to be configured. See "[Connections to the Vivato VP2200](#)" on page 32. Issuing this command changes the prompt to indicate which interface you are configuring, such as **vivato (config -eth0)#** if you entered 0 for the value. 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 68.

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> [secondary]

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. The optional "secondary" entry is used to create a secondary IP address on this interface.

Note: The IP address of the default bridge that bridges the Ethernet and wireless interfaces (bro) is initially used provide access to the VP2200. See "[interface bridge <0-4094>](#)" on page 66.

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.

no ip broadcast-address [secondary]

Enter this command to remove a previously assigned broadcast IP address from this interface. The optional "secondary" entry is used to delete a previously assigned secondary broadcast IP address. If a secondary broadcast IP address was assigned on this interface, it must be removed before the primary broadcast 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 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 routing

Enter this command to enable IP routing on this interface.

jail [add mac <mac address>]

This command is used with the **http-server redirect** command to create a list of clients authenticating through this interface to access a web page. The MAC address of each client must be added to a “jail” list before it is allowed access to the VP2200’s backhaul and go to its intended destination (get out of jail). The optional **add mac <mac address>** entry can be used to add a mac to the jail list manually. The default state is disabled.

show <text>

See “**show interfaces ethernet [0-3]**” on page 47.

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 <0-3>|vlan <1-4094>|wireless <1-13>>

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 vlan <vlan id>

Enter a number to be used to identify a VLAN. The value must be in the range of 1 to 4094. Issuing this command changes the prompt to indicate which interface you are configuring, such as **vivato (config -vlan3)#** if you entered 3 for the value. This prompt must be displayed when issuing any of the following VLAN interface commands.

Important 	Use EITHER bridges OR VLANs to connect interfaces. Do not attempt to use VLANs and bridges at the same time. If VLANs are being used, be sure to DELETE the default bridge (br0) and any other bridges before configuring VLANs. If bridges are being used, do not configure any VLANs.
Important 	After being created, a VLAN it is not <u>enabled</u> until the no shutdown command is issued. Use the show interfaces vlan [vlan id] to display the current status of a VLAN.

add interface ethernet <0-3>

Enter the number of the Ethernet interface to add to the VLAN.

Note: An Ethernet interface cannot be added to the VLAN if an IP address has been assigned to that interface. Remove the IP address from that interface in order to add it to the VLAN. The IP address of the VLAN is then used to access this port (and any other ports) on the bridge.

no add interface ethernet <0-3>

Enter the number of the Ethernet interface to remove it from the VLAN.

add interface wireless <1-13>

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

Note: A wireless interface cannot be added to the VLAN if an IP address has been assigned to that interface. Remove the IP address from that interface in order to add it to the VLAN. The IP address of the VLAN is then used to access this port (and any other ports) on the bridge.

no add interface wireless <1-13>

Enter the number of the wireless interface to remove if from the VLAN.

add mac <mac address>

Enter the 12-digit hexadecimal medium access control (MAC) address of a device to allow it to associate through this VLAN. Be sure to save your configuration after entering the MAC addresses so that they are not lost if a reboot or power loss occurs.

no add mac <mac address>

Enter the 12-digit hexadecimal medium access control (MAC) address of a device to remove it from the VLAN.

aging-time <10-1000000>

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

default

Enter this command to make this the default VLAN. The default VLAN cannot also be used as a guest VLAN.

no default

Enter this command to not use this VLAN as the default VLAN.

DHCP Server Operation

Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface. See "[dhcp-server](#)" on page 68.

exit

Stop configuring this VLAN.

forward-time <4-200 seconds>

VLANs are a form of bridge. 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.

guest <wep key>

Enter a WEP key to use this VLAN as a guest VLAN. 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 (example; s:gmV8a18436572). Unlike WEP keys configured for wireless interfaces, the guest VLAN WEP key does not use a key index; defaulting to using an index of "1".

When EAP security is enabled on the VP2200, guest VLANs permit clients that have not been configured on the RADIUS authentication server to associate with the VP2200. *Guest VLANs are only used when both EAP and VLANs are enabled.* The guest client is configured to use the guest VLAN's WEP key just as it would be configured for regular WEP operation, except that the key index is always set to "1" for guest VLANs. See "[Configuring WEP in Your Client](#)" on page 108.

A guest VLAN cannot also be used as the default VLAN.

hello-time <1-10 seconds>

VLANs are a form of bridge. 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>

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

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 secondary

Removes the secondary IP address on this interface.

ip broadcast-address <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 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 and allow it to be reassigned.

ip routing

Enter this command to enable IP routing on this interface.

jail [add mac <mac address>]

This command is used with the **http-server redirect** command to create a list of clients authenticating through this interface to access a web page. The MAC address of each client must be added to a “jail” list before it is allowed access to the VP2200’s backhaul and go to its intended destination (get out of jail). The optional **add mac <mac address>** entry can be used to add a mac to the jail list manually. The default state is disabled.

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 0-3|wireless 1-13> <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.

port-priority <ethernet 0-3|wireless 1-13> <0-255>

Enter the port priority for a specific port on the bridge. The port priority is used in the spanning tree protocol to determine which port to use when a bridge has two ports connected to the same network; resulting in a loop. The port with the lower priority number is used.

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

shutdown

Disables the VLAN indicated on the command prompt.

no shutdown

Enable the VLAN indicated on the command prompt.

source-nat interface <bridge <0-4094>|ethernet <0-3>|vlan <1-4094>|wireless <1-13>>

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 VLAN, and the IP address of the desired source interface, must be configured before address translation can occur.

interface wireless <1-13|all>

This command selects the wireless interface for configuration. The VP2200 contains 13 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) and Ethernet 1 (eth1) interfaces for wireless clients to be able to access the wired network. See "[interface bridge <0-4094>](#)" on page 66.

“Pointing Directions” and Wireless Interfaces

Each wireless interface configures approximately a 15 degree portion of the VP2200’s antenna pattern. These are referred to as the 6 “pointing directions”. Standing behind the VP2200, these pointing directions are numbered from left-to-right, 1 to 6. For example, when you configure wireless interface 5, you are configuring the operation of signals being transmitted and received for pointing direction 5; which is at the far right of the pattern. See "[Example Wi-Fi Switch Wireless Interface Assignments](#)" on page 76.

beacon-interval <0-8191>

Specify the amount of time, in milliseconds, between beacons. Entering 0 disables 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.

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 802.11b 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.

channel <1-11>

Enter a channel number for the wireless interface. The value must be in the range of 1 to 11. Channel assignments are paired to automatically “mirror” across the pointing directions of the VP2200’s antenna. Therefore, any time you change a wireless interface channel other than the center direction (wlan7), the channel assignment of the corresponding wireless interface on the other side of the center of the VP2200 is changed to match. See “**Example Wi-Fi Switch Wireless Interface Assignments**” on page 76 for more information.

Important	Under most circumstances, the default channel assignments should be used; especially when using the VP2200 in areas of heavy Wi-Fi traffic. For information on determining if you need to use different channel assignments, see “ Appendix C: Assessing Traffic and Interference ” on page 227.
-----------	---

DHCP Server Operation

Refer to the bridge interface’s DHCP command descriptions for DHCP operation on any interface. See “**dhcp-server**” on page 68.

disable beacon-ssid

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 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 VP2200. The default state is to send the ESSID in beacons until this command is sent.

no disable beacon-ssid

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.

ssid <text>

Enter an identifying name for the extended service set for this wireless interface. The name must be in the range of 1 to 30 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 and allow it to be reassigned.

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.

jail [add mac <mac address>]

This command is used with the **http-server redirect** command to create a list of clients authenticating through this interface to access a web page. The MAC address of each client must be added to a “jail” list before it is allowed access to the VP2200’s backhaul and go to its intended destination (get out of jail). The optional **add mac <mac address>** entry can be used to add a mac to the jail list manually.

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 -wlan-all)#** prompt: **key s:gmcv818436572 1**

mode <b|g>

Enter “b” or “g” to set this wireless interface to operate in 802.11b or 802.11g mode, respectively.

multicast rate <1|2|5.5|11>

Enter a value to set the multicast/broadcast transmit rate (including beacons) in Mbps. This is sometimes referred to as the “basic rate”.

power <0-4>

Enter a value in the range of 0 to 4 to represent the level to attenuate (decrease) the wireless signal transmitted from all wireless interfaces. 0 = full power (no attenuation); 1 = -6dB; 2 = -12 dB; 3 = -18 dB; 4 = -24 dB (minimum power). Reducing the transmit power can sometimes improve performance when most clients are close-in, and can help prevent interference between Wi-Fi Switches when multiple Switches are installed in an area.

This command can only be used to change the transmit power of all wireless interfaces; it cannot be used to change an individual interface's transmit power.

sensitivity <1-5>

Change the receiver sensitivity for all wireless interfaces: 1 = most sensitive (default), 5 = least sensitive. Under most conditions this value should be left at "1" to receive signals from far away clients. If the data rate for close-in clients appears to be *lower* than for clients that are farther away, the receiver may be getting too strong of a signal from the closer clients. In that case, reduce the sensitivity as needed to improve close-in client data rates. Also, if another VP2200 is close enough to effect operation on this Switch, reducing the sensitivity may help reduce any interference from the other Switch.

This command can only be used to change the sensitivity of all wireless interfaces; it cannot be used to change an individual interface's sensitivity.

shutdown

Issuing this command disables the wireless interface.

show <text>

See "**show interfaces wireless <1-13>**" on page 50.

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 <0-3>|vlan <1-4094>|wireless <1-13>>

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 VP2200 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 91.

```
Vivato(config-wlan1)#wds 1
Vivato(config-wds1-1)#
```

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 this WDS connection.

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.

Because 802.1x security automatically configures WEP as part of its operation, WEP cannot be configured on a wireless interface if 802.1x security is currently being used.

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 switch.

no interface bridge <0-4094>

Specify the number of the bridge interface to disable.

no interface vlan <1-4094>

Specify the number of the VLAN 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 VP2200. 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 52 to view the contents of the host IP table.

ip hostname <hostname>

Enter a host name for the VP2200 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 VP2200 to route all IP datagrams destined for the 135.228.6.0/24 network through a gateway whose 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. The default state is disabled.

ip ssh genkey

Generate encryption keys for a secure shell connection to the VP2200. 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 <1-13>|ethernet <1-3>|bridge <0-4094>|vlan <1-4094>)

Specify the interface on the VP2200 to use for SSH access. When this command is issued, only the IP address on that interface can be used to access the Switch through SSH. If an IP address has not been assigned to this interface, SSH access is not restricted.

no ip ssh bind [interface (wireless <1-13>|ethernet <1-3>|bridge <0-4094>|vlan <1-4094>)]

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

ip traffic-shaping sfq

Begin traffic shaping using a stochastic fairness queue. Traffic shaping is used to provide relatively equal packet priority for all clients. The default state is enabled.

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 VP2200's memory. Use the "**show logging**" on page 53 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 Multi-MAC Controller

This feature coordinates traffic among all wireless interfaces sharing the same channel, and should be used whenever client traffic loads are high.

mmc

Enable packet shaping. The default state is enabled.

no mmc

Disable packet shaping.

Configure Radio

The following commands effect all wireless interfaces. These commands cannot be used to alter individual radio settings.

radio power <0-4>

Enter a value in the range of 0 to 4 to represent the level to attenuate (decrease) the wireless signal transmitted from all wireless interfaces. 0 = full power (no attenuation); 1 = -6dB; 2 = -12 dB; 3 = -18 dB; 4 = -24 dB (minimum power). Reducing the transmit power can sometimes improve performance when most clients are close-in, and can help prevent interference between Wi-Fi Switches when multiple Switches are installed in an area.

This command can only be used to change the transmit power of all wireless interfaces; it cannot be used to change an individual interface's transmit power.

radio sensitivity <1-5>

Change the receiver sensitivity for all wireless interfaces: 1 = most sensitive (default), 5 = least sensitive. Under most conditions this value should be left at "1" to receive signals from far away clients. If the data rate for close-in clients appears to be lower than for clients that are farther away, the receiver may be getting too strong of a signal from the closer clients. In that case, reduce the sensitivity as needed to improve close-in client data rates. Also, if another VP2200 is close enough to effect operation on this Switch, reducing the sensitivity may help reduce any interference from the other Switch.

This command can only be used to change the sensitivity of all wireless interfaces; it cannot be used to change an individual interface's sensitivity.

Configure RAPD Commands

These commands enable and disable rogue access point detection (RAPD). RAPD looks for signals from Wi-Fi access points within the coverage area of the Vivato VP2200. These access points can interfere with the operation of the VP2200, and should be removed or be re-configured to operate on non-interfering channels. To view a list of detected access points, use the **show rapd** command.

rapd

Enable rogue access point detection. The default state is disabled.

no rapd

Disable rogue access point detection.

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 <1-13>|ethernet <1-3>|bridge <0-4094>|vlan <1-4094>)

Specify the interface on the VP2200 to use for SNMP access. When this command is issued, only the IP address on that interface can be used to access the Switch 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 ip address>] 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 6—Examples for Creating Traps/Informs Sinks on page 89](#).

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 6—Examples for Creating Traps/Informs Sinks on page 89](#).

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 6—Examples for Creating Traps/Informs Sinks on page 89](#).

Table 6—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 7—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

Table 7—Examples for Configuring an SNMPv3 User

Setting	Command
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 System (boot system flash:)

The “boot system flash:” command is used to specify which software image file in the VP2200’s flash memory to use when rebooting the VP2200. When this command is entered, you are prompted to specify the name of this boot image. This allows you to update the VP2200’s software after downloading a new boot image. See ["Wi-Fi Switch Firmware Updates"](#) on page 205.

After using this command, be sure to save your configuration using the [write \[memory\]](#) command *before* rebooting the VP2200. When you then reboot the VP2200, it will load the new software image and the last stored “startup-config” configuration file.

Configure Username Admin (Read Level) Secret

The read level secret is used to access the VP2200 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.

Configure WDS (Wireless Distribution System)

A wireless distribution system uses two Wi-Fi Switches, or a VP2200 and a Vivato Bridge/Router, to provide a wireless data link that can span large distances to provide a network connection to remote clients or to connect two network segments together. The WDS link can be used in place of a wired backhaul connection, requiring only mains power to provide 802.11b service to clients through the remote Switch or Bridge/Router.

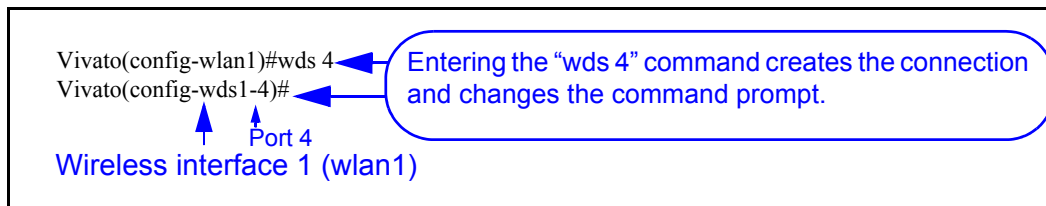
The link is created by enabling WDS operation on a wireless interface on each Switch or Bridge/Router and specifying the MAC address of the other device’s wireless interface as the “peer address”.

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, and the WDS connection can be added to the default bridge to pass traffic to other interfaces within the Bridge/Router or VP2200.

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 <1-13> 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 interfaces wireless <1-13> wds <1-6>"** on page 51 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:

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 <1-13>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 other VP2200 (or Bridge/Router) being used for a WDS link (in the format 00:0B:33:31:85:A3).

A specific peer 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.

Command Line Interface

Enable Level Command Descriptions

```
Vivato(config)#show interfaces wireless 5
wlan5 Link encap:Ethernet HWaddr 00:0B:33:00:60:87
UP BROADCAST RUNNING MULTICAST MTU:1500
RX packets:95 error:0 dropped:0 overruns:0 frame:0
TX packets:3964 error:952 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
Interrupt:23 Base address::0xd280
Bridged : [br0]

Essid:glasair TD
Beacon Essid: Enabled
Channel:6 Access Point:00:0B:33:00:60:0E
"" ""

Vivato(config)#interface wireless 5
Vivato(config-wlan5)#wds 1
Vivato(config-wds5-1)#
Vivato(config-wds5-1)#peer-address 00:0B:33:06:00:27
Vivato(config-wds5-1)#
Vivato(config-wds5-1)#no shutdown
Vivato(config-wds5-1)#exit
Vivato(config-wlan5)#channel 11
Vivato(config-wlan5)#exit
Vivato(config)#
Vivato(config)#
Vivato(config)#
Vivato(config)#
Vivato(config)#
Vivato(config)#Vivato(config)#interface bridge 0
Vivato(config-br0)#add interface wireless 5 wds 1
Vivato(config-br0)#exit
Vivato(config)#exit
Vivato#write
Writing configuration...
OK
Vivato#
```

This is the MAC address of this wireless interface. Use it as the peer-address when configuring WDS on the device at the other end of the link.

Entering the "wds 1" command creates the connection and changes the command prompt.

The WDS interface is shut down until it is enabled using the "no shutdown" command.

This is the MAC address of the wireless interface on the Wi-Fi Switch at the other end of the WDS link.

The channel number of the wireless interface used for the WDS connection on the Bridge/Router and on the Wi-Fi Switch must be the same.

Add the WDS connection to the default bridge to allow it to pass traffic through the wireless interface to the Ethernet interface.

Figure 23—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 VP2200 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 VP2200, 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 VP2200 to be reset, and powers on using the last saved configuration. See **write network flash:** or "**write [memory]**" on page 60 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 to be saved in a file titled "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

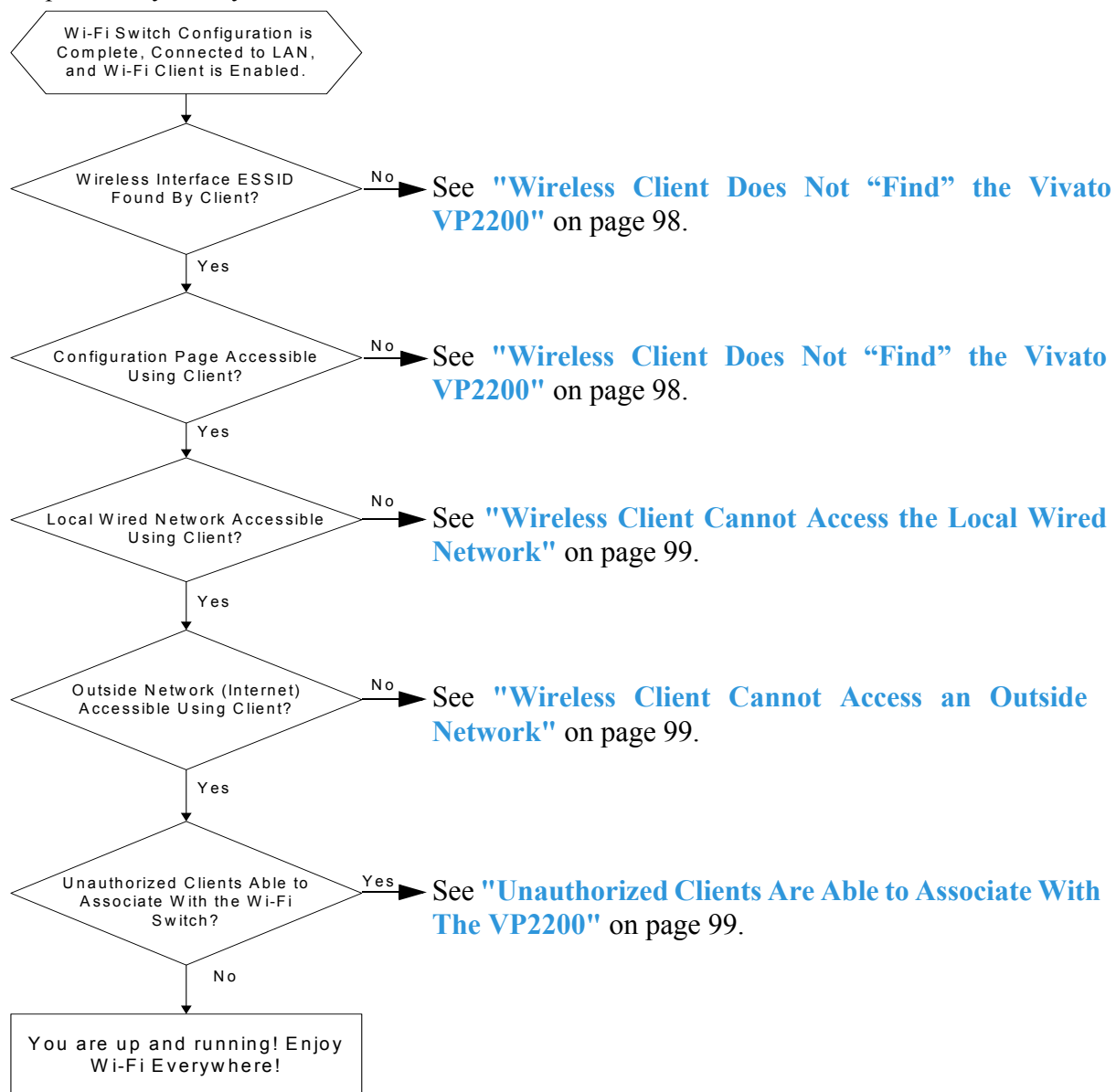
Verifying Wi-Fi Operation

After installing and configuring the Vivato VP2200, it is important to verify that it operates as intended. The information in this section is intended to help you verify VP2200 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 VP2200 operation and to identify some of the possible causes of problems you may encounter:



Wireless Client Does Not “Find” the Vivato VP2200

Part of configuring the VP2200 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 VP2200’s power LED must indicate that the switch is operating. See ["Connections to the Vivato VP2200"](#) on page 32.
- The VP2200’s wireless interfaces must be enabled and their ESSID specified. If only a portion of the wireless interfaces have been enabled, the Vivato VP2200 will not be transmitting through its entire 90° pattern. See ["Network>Wireless Interfaces"](#) on page 74.
- To ensure access, the client should be within the antenna pattern of the VP2200. See ["Network>Wireless Interfaces"](#) on page 74.
- 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 VP2200’s antenna pattern, try rotating the client 90 degrees (horizontally) to see if your reception is improved.

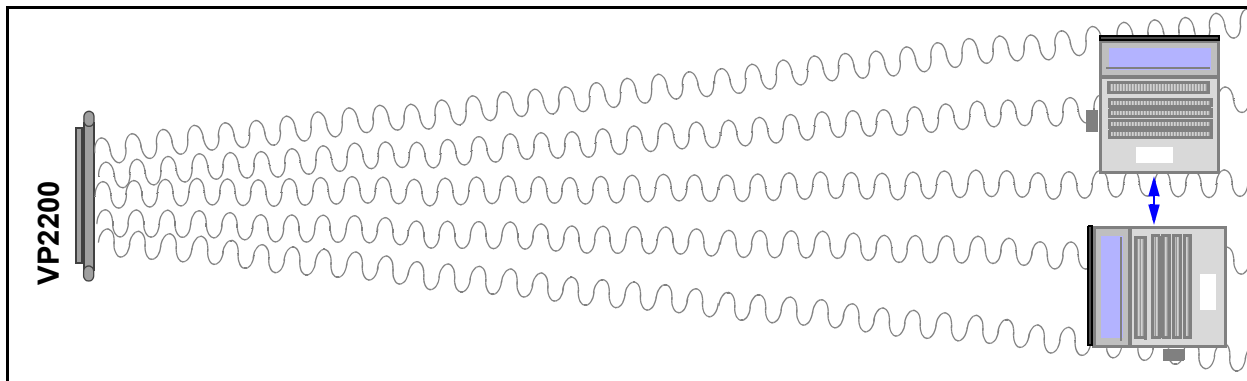


Figure 24—Rotating the Client to Improve Performance

Wireless Client Cannot Access the Local Wired Network

If you are unable to access the wired network connected to one of the Switch's Ethernet ports, verify that the following conditions are present:

- The default bridge (br0) connecting the wireless interfaces to the Ethernet ports is enabled, or you have created a VLAN connecting the wireless interface that you are associating with to the appropriate Ethernet port(s). See ["Network Settings"](#) on page 57.
- Your wired network is connected to one of the VP2200's Ethernet ports. See ["Connections to the Vivato VP2200"](#) on page 32.
- The Ethernet port you are connected to is enabled. The Vivato VP2200 is pre configured with the Ethernet ports enabled. See ["Network>Ethernet Interfaces"](#) on page 73.
- The Vivato VP2200 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 VP2200 has been added to that list.
- When authenticating through a RADIUS service, the RADIUS configuration information must be correctly entered. See ["Security> 802.1x"](#) on page 82.
- The correct default gateway is specified. See ["Basic Network Setup"](#) on page 44.

Wireless Client Cannot Access an Outside Network

If you are able to connect to your local network through the Vivato VP2200, 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.
- When authenticating through a RADIUS service, the RADIUS configuration information must be correctly entered. See ["Security> 802.1x"](#) on page 82.
- The correct default gateway must be specified. See ["Basic Network Setup"](#) on page 44.

Unauthorized Clients Are Able to Associate With The VP2200

Security is disabled in the VP2200 when delivered. If the security settings have not been configured and enabled, anyone with an IEEE 802.11b client can associate with the VP2200. To prevent this situation, enable the highest levels of security in the VP2200 and your clients.

Verifying Wi-Fi Operation

Verification Process

Network Monitoring

Three methods can be used to monitor Vivato VP2200 operations and network traffic:

- The built-in web page user interface. To use the monitoring functions of the web interface, see "[Monitoring Rogue APs, Clients, and System Operations](#)" on page 91.
- Command line interface (CLI). A explanation of using the CLI and a list of the available commands to configure and monitor switch operations is provided in "[Command Line Interface](#)" on page 35.
- Simple network management protocol (SNMP)

SNMP Operations

You can use third-party SNMP management software to monitor operations within the Vivato VP2200. These software packages are designed to use standard SNMP versions that have been defined to work with devices created by various manufacturers. The VP2200 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 VP2200. 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, with exceptions noted below.
- 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 MIBs

The following MIBs are included on the Vivato VP2200 Wi-Fi Switch CD. Operating limitations for each MIB are relevant for this firmware release, but may not be present in future firmware releases.

IEEE8021-PAE-MIB.txt

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

- The following are not supported:
 - ◇ ?????

80211-MIB.txt

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

- The following are not supported:
 - ◇ dot11AuthenticationAlgorithmsTable
 - ◇ dot11WEPPDefaultKeysTable
 - ◇ dot11WEPKeyMappingsTable
 - ◇ dot11PrivacyTable
 - ◇ dot11FrameDuplicateCount
 - ◇ dot11RTSSuccessCount
 - ◇ dot11RTSFailureCount
 - ◇ dot11ACKFailureCount
 - ◇ dot11GroupAddressesTable
 - ◇ dot11PhyAntennaTable
 - ◇ dot11PhyTxPowerTable
 - ◇ dot11PhyFHSSTable
 - ◇ dot11CCAModeSupported
 - ◇ dot11CurrentCCAMode
 - ◇ dot11PhyIRTable
 - ◇ dot11AntennasListTable
- The following are not supported in this release but will be included in a future release:
 - ◇ dot11DisassociateReason

- ◇ dot11DisassociateStation
- ◇ dot11DeauthenticateReason
- ◇ dot11DeauthenticateStation
- ◇ dot11AuthenticateFailStatus
- ◇ dot11AuthenticateFailStation
- ◇ dot11SMTnotification

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

RFC1493-MIB.txt

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

- The following are not supported:
 - ◇ dot1dBasePortCircuit
 - ◇ dot1dBasePortDelayExceedDiscards
 - ◇ dot1dBasePortMtuExceededDiscards
 - ◇ dot1dStp
 - ◇ dot1dTpLearnedEntryDiscards
 - ◇ dot1dTpPortTable

VIVATO-EXP-MIB.txt

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

- The following are not supported:
 - ◇ Sets of any kind
 - ◇ sysLogRemoteLoggingIPAddress
 - ◇ viVlan

SNMPv2-MIB.txt

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

- The following are not supported:
 - ◇ snmpUsmMIB
 - ◇ snmpVacmMIB

Enabling SNMP Operation

To use SNMP in the VP2200, 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 88 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.

SNMP Configuration Information	
[Base SNMP Options]	[Community Options] [V3 Options] [V2 Options] [V1 Options]
These menus are used for configuring all versions of SNMP. Status: DISABLED System Name: Unknown System Name System Location: Unknown Location System Contact: Unknown System Contact These menus are used to configure specific versions of SNMP.	
Current SNMP Community Settings: (select for removal)	public RO private RW
Current Trap Sinks: (select for removal)	
Make Base SNMP Changes	

Figure 25—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.

Create SNMP Community:	
Community Name:	
Type:	RO
IP Address (Optional):	
Create New Community	

Figure 26—Creating an SNMP Community

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

SNMP v1 Options:	
Hostname/IP Address:	
Traps:	
Community Name:	
Create Trap Sink	

SNMP v2 Options:	
Hostname/IP Address:	
Trap Sink Type:	traps v
Community Name:	
Create Trap Sink	

SNMP v3 Options:	
Create v3 Trap Sink	Create v3 User
Hostname/IP Address:	Username:
Trap Sink Type: traps v	Optional Settings
Username:	Authentication Type: MDS v
Optional Settings	Password:
Authentication Type: v	Privacy Type: DES v
Password:	Password:
Privacy Type: v	Create SNMP User
Password:	
Create Trap Sink	

Figure 27—Specifying Settings for SNMP Versions 1, 2c, and 3

Index

A

Activity LED 32

B

basic rate (multicast/broadcast) (CLI) 82

boot loader version, displaying (CLI) 55

BSS 21

C

capture ethernet packets 57

ceiling height (indoor switch) 26

CLI (command line interface) 35

CLI commands

- bridge interface 66

- capture interface ethernet 57

- clock set 61

- configure network flash 58

- copy flash flash 58

- copy flash scp 59

- copy scp flash 59

- delete 60

- eap 62

- enable 43

- enable secret 65

- ethernet interface 72

- exit 43

- http server 66

- IP configuration 84

- ip domainname 85

- ip hostname 85

- ip name-server 85

- log 86

- ping 43

- rapd 87

- reboot 95

- show (user level) 44

- show interfaces 50

- SNMP 88

- traceroute 56

- username secret 91

- wireless interface 79

- write network flash 60

- write network scp 60

- write terminal 61

CLI, connections 36

command line interface (CLI) 35

configuration (CLI), example 39

configuration (CLI), saving 60

connections 32

customer support 7

D

DHCP client control (CLI) 70

DHCP server configuration (CLI) 66

documentation feedback 7

domain name, specifying (CLI) 85

E

enable level password (CLI) 65

environmental considerations

- indoor switch 27

ESSID beacons, disable (CLI) 80

ethernet ports 32

F

feedback, documentation 7

G

gateway, specifying default 85

H

host name, specifying (CLI) 85

I

IBSS 21

installation

- indoor 23

interference, signal

- indoor switch 27

L

Link LED 32

location

- indoor Wi-Fi Switch 24

M

MAC address

- product label 33

- show version (CLI) 55

manual feedback 7

CLI commands

- write 60

MIB (mngmnt info base) 101
monitoring, network (SNMP) 101
mounting the indoor Wi-Fi Switch 28
multicast 82
multi-MAC controller (CLI) 86

N
name server, specifying (CLI) 85

O
obstructions, indoor 27

P
password
 enable level (CLI) 65
 read level (CLI) 91
Power Injector 31
Power LED 32
power over Ethernet connection 32
power requirements 31
Power Supply 31

R
read level password (CLI) 91
register your Wi-Fi Switch 23
RJ-45 connectors 32
rogue access point detection (CLI) 87
route, creating (CLI) 85
RS-232 connector 32
RS-232, CLI access 36

S
saving CLI configuration (write file) 60
serial number, displaying (CLI) 54
serial port 33
shipping contents
 indoor switch 24
SNMP (Network Monitoring) 101
SSID (ESSID) beacons, disable (CLI) 80
SSID blocking (disable beacon-ssid CLI) 81
support, customer 7

T
troubleshooting operation 97

U
user name, specifying (CLI) 91

V
verifying operation 97

W
Warranty and End User License 9
WDS, display configuration 50
weight
 indoor switch 31
WEP, CLI configuration 82
Win 2K IAS configuration for EAP 62