VIVATO™

Wi-Fi EVERYWHERE

Vivato 2.4 GHz Wi-Fi Switch User Guide

Manual Part Number: 720-00381-01
Printed in U.S.A.

Copyright © 2002 Vivato, Inc.

Who Should Read This Book?

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 2.4 GHz 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 person installing the Vivato 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.

Ground the equipment: This product uses a protective earth ground terminal. An uninterruptible safety earth ground must be provided from the mains power source to the product's input wiring terminals or to the supplied power cable.

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.

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. 2.4 GHz Wi-FI Switch, model VLJ24WFSW
This product is intended for home or office use.

The Vivato Wi-Fi Switch has been evaluated under FCC Bulletin OET 65C and found to be compliant to the requirements set forth in CFR 47 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The Wi-Fi 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: 1mW/cm^2 at 20 cm distance from antenna face.
- Vivato Wi-Fi Switch worst case exposure (OET 65 upper bound method): 0.247 mW/cm^2 at 20 cm distance from antenna face with all three channels transmitting simultaneously.
- Worst case exposure at 20 cm from antenna face (three channels in adjacent pointing directions at the extreme left or right): <0.13 mW/cm^2.

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."
Labels	Items in a menu, such as the tabs shown on the configuration web pages.
Switch,Wi-Fi Switch	Both terms refer to the Vivato 2.4 GHz Wi-Fi Switch unless otherwise noted.
<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:

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

Mail:

Vivato, Inc.

139 Townsend St., Suite 200

San Francisco, CA 94107

To provide feedback on our documentation:

Feedback on the documentation shipped with the Vivato 2.4 GHz 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.)

Warranty and End User License

VIVATO END USER LIMITED WARRANTY AND LICENSE TERMS

LIMITED WARRANTY

Vivato warrants that for a period of one year from the date of shipment from Vivato, the hardware of the Vivato Products will be free from defects in material and workmanship under normal use. This limited warranty extends only to End Users as original purchasers.

REMEDY

For all Vivato Products or components thereof that do not comply with the warranty provided above, Vivato will either repair or replace such non-compliant Vivato Products or components thereof.

All warranty claims shall be directed to Vivato's technical assistance center at 1-415-495-1111. Vivato or its agent shall have the right to inspect the Vivato Product being claimed as non-compliant with the warranty provided above following any warranty claim, with reasonable notice during normal working hours. Vivato's technical assistance center will issue Return Material Authorizations (RMA's) for all Vivato Products or components thereof that are acknowledged by Vivato as qualifying for the warranty remedies specified herein.

After receiving an RMA for a Vivato Product, End User shall ship such Vivato Product or component thereof, clearly identifying it with its RMA, to Vivato's repair facility in its original shipping cartons or equivalent, freight prepaid. Vivato Products damaged during return shipment due to improper packing will not be covered by this warranty. Following receipt of the Vivato Product accompanied by an RMA number, Vivato, at its discretion, may repair or replace such product, and shall return the repaired or replaced product to End User freight prepaid by Vivato. Vivato at its option may replace any returned Vivato Product or component thereof with equivalent or better, new or refurbished products or parts. The remainder of the original warranty coverage shall apply to such repaired or replacement products.

If the product defect is found by Vivato to have been caused by misuse or abnormal operating conditions, repairs and/or replacement will be billed to End User's account. 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 Vivato Product is found by Vivato to be in compliance with the warranty above, Vivato may charge a fee for the evaluation, which may include reasonable travel and expenses, if applicable.

LIMITATIONS OF WARRANTY

This warranty does not apply to Vivato Products which exhibit failures or non-compliance resulting from: a) improper handling, installation, repair, maintenance or use; b) damage caused by vandalism, severe weather, lightning, chemical hazards, fire, contact with high-voltage power lines or other electrical stress; c) repairs, modifications, or any alterations performed or attempted by End User or any third party, unless authorized by Vivato as stated below; d) use in conjunction with equipment which is not compatible with Vivato Products; e) documentation errors; or f) software errors which do not cause Vivato Products to be materially non-compliant with their written specifications.

Vivato does not warrant or accept any responsibility in connection with any of its products which have been repaired or altered by anyone other than Vivato, unless Vivato has specifically authorized in writing in advance such repairs or alterations. 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. Non-payment of invoices for products, within the stated terms, shall cause this warranty to be suspended until late invoices are fully paid.

Minor or non-substantive defects or deviations from specifications, or documentation errors or omissions shall not constitute a warranty defect. Vivato reserves the right, without notice to End User, to discontinue products, and to change product specifications provided such changes in specifications do not adversely affect the performance of products scheduled for future delivery under an existing purchase contract.

End User's sole remedy with respect to any warranty or defect in the Vivato Products is as stated above.

EXCEPT AS SPECIFIED HEREIN, VIVATO MAKES NO OTHER WARRANTIES WITH RESPECT TO VIVATO PRODUCTS 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, 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 VIVATO PRODUCTS OR VIVATO SOFTWARE ARE ERROR-FREE OR THAT OPERATION OF THE VIVATO PRODUCTS OR VIVATO SOFTWARE WILL BE SECURE OR UNINTERRUPTED AND VIVATO HEREBY DISCLAIMS ANY AND ALL LIABILITY ON ACCOUNT THEREOF.

LIMITATION OF LIABILITY

NOTWITHSTANDING ANYTHING ELSE IN THIS WARRANTY, VIVATO SHALL NOT BE LIABLE UNDER ANY PROVISION OF THIS WARRANTY 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, OR (B) FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR (C) FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES.

END USER LICENSE

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

BY INSTALLING, USING OR DOWLOADING VIVATO SUPPLIED PRODUCT OR SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT WANT AGREE TO ALL OF THE TERMS OF THIS LICENSE THEN: 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 AFTER 30 DAYS AFTER PURCHSE FROM VIVATO OR AN AUTHORIZED VIVATO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGIAL PURCHASER.

The following terms govern your use of the Vivato Product or Software except to the extent to a particular program: a) is the subject of a separate written agreement with Vivato or b) includes separate "click-on" license agreement as a part of the installation and/or download process. 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, and 3) this End User License.

1. End user shall be granted a limited nonexclusive and nontransferable license to use the Vivato Products (including the Vivato Software) solely for its own internal business operations solely in the Territory. 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 Vivato Products in any way for any purpose.

2. End User acknowledges that the Vivato Products contain trade secrets of Vivato, and to protect them, End User shall not reverse engineer, disassemble, decompile, or otherwise attempt to derive the source code of the Software or algorithms or other aspects of the Vivato Products.

3. End User acknowledges that the Vivato Products are covered by patent, copyright, trade secret and other intellectual property rights. No right, title or interest, expressed or implied, in or to the Vivato 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 Vivato Software shall remain with Vivato and its licensors (if any). End User shall not alter or erase any proprietary notices appearing on the Vivato Products and shall reproduce all such proprietary notices on the Vivato Products.

4. End User acknowledges that the Vivato Products contain 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.

5. The Vivato Products are being provided to End User with the limited warranty specified in the Product Warranty, incorporated by reference herein. EXCEPT AS SPECIFIED IN THE PRODUCT WARRANTY, VIVATO MAKES NO OTHER WARRANTIES WITH RESPECT TO VIVATO PRODUCTS 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, 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 VIVATO PRODUCTS OR VIVATO SOFTWARE ARE ERROR-FREE OR THAT OPERATION OF THE VIVATO PRODUCTS OR VIVATO SOFTWARE WILL BE SECURE OR UNINTERRUPTED AND VIVATO HEREBY DISCLAIMS ANY AND ALL LIABILITY ON ACCOUNT THEREOF. End User’s sole remedy with respect to any breach of the Product Warranty shall be the remedies specified in the Product Warranty.

6. NOTWITHSTANDING ANYTHING ELSE IN THIS WARRANTY, VIVATO SHALL NOT BE LIABLE TO END USER OR ANY THIRD PARTY UNDER ANY PROVISION OF THE WARRANTIES 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, OR (B) FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, 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.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Introduction

The Vivato 2.4 GHz Wi-Fi Switch is a three-channel unlicensed (FCC Part 15) wireless device operating in the 2.4 GHz band, providing network connections to Wi-Fi (IEEE 802.11b) client devices on up to three simultaneous channels.

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

The Wi-Fi 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 Wi-Fi switch to receive signals from standard 802.11b clients, even at long distances or with high signal attenuation. This design allows one Wi-Fi Switch 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.

Both indoor and outdoor versions of the Vivato Wi-Fi Switch are available, providing Wi-Fi service in almost any environment.

Multi-Channel Operation

The Vivato Wi-Fi Switch can communicate simultaneously on up to three 802.11b channels when used in areas of light Wi-Fi traffic, and on two channels when used in areas of heavy Wi-Fi traffic.

The Wi-Fi Switch's 100° antenna pattern is divided into 13 focused areas. If necessary, the channel assignment and other settings for each area can be changed to optimize overall Wi-Fi operation within the full antenna pattern.

Basic Service Set Operation

The Wi-Fi Switch 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 802.11b clients can communicate directly with each other without using the Wi-Fi switch, is not supported.

"Out of the Box" Settings

The Wi-Fi Switch is shipped with a default bridge, IP address, channel assignments, and ESSID. These settings allow configuration changes to be made using the built-in web pages or using the command line interface (CLI), and connecting through a wired or a wireless link. Refer to **"Default Configuration"** on page 36.

Indoor Wi-Fi Switch Installation

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

This section is specific to the Vivato 2.4 GHz Indoor Wi-Fi Switch. See **"Outdoor Wi-Fi Switch Installation"** on page 21 for information on installing the outdoor version.

We recommend that you prepare your Vivato 2.4 GHz Indoor Wi-Fi Switch for operation in the following order:

1 Verify the contents of the shipping container. See **"Shipping Contents"** on page 4.

2 Register your Vivato Wi-Fi Switch! You can select **Register Online Now!** here or on the Vivato CD startup page, or go to **http://www.vivato.net/wifiregistration.html.**

3 Attach the top and bottom rails, end caps, and fabric cover. See **"Assembling the Wi-Fi Switch"** on page 8.

4 Fill out the *Vivato Wi-Fi Switch Configuration Worksheet*.

5 Analyze your site to estimate the best place to mount the Wi-Fi Switch. See **"Where to Mount The Indoor Wi-Fi Switch"** on page 4.

6 Configure the Wi-Fi Switch. 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. See **"Initial Configuration Using the Built-In Web Pages"** on page 35.

7 If power and/or LAN connections are to be routed above the Wi-Fi Switch, route the cables on the rear panel before mounting. See **"Cable Routing to the Wi-Fi Switch"** on page 10.

8 Mount the Wi-Fi Switch. See **"Mounting the Wi-Fi Switch"** on page 11.

9 If not already connected, connect the Wi-Fi Switch to mains (AC) power and your LAN. See **"Connections to the Vivato Wi-Fi Switch"** on page 17

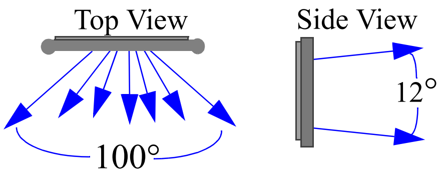
10 Verify Wi-Fi Switch operation using your Wi-Fi client. See **"Verifying Wi-Fi Operation"** on page 151.

Shipping Contents

The following items are included in the shipping container with the Vivato 2.4 GHz Indoor Wi-Fi Switch:

- Vivato Wi-Fi Switch.
- DB-9 null modem cable
- 100 Base-T Ethernet cable (white)
- 100 Base-T cable cross-over Ethernet (red)
- Power cable
- Mounting kit brackets (2), flange nuts (4), and hollow wall anchors (4)
- Fabric dress cover
- Top dress panel support rail
- Bottom dress panel support rail
- End caps (2)
- Quick Configuration Guide (11” x17” 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, 4-fold)

Where to Mount The Indoor Wi-Fi Switch



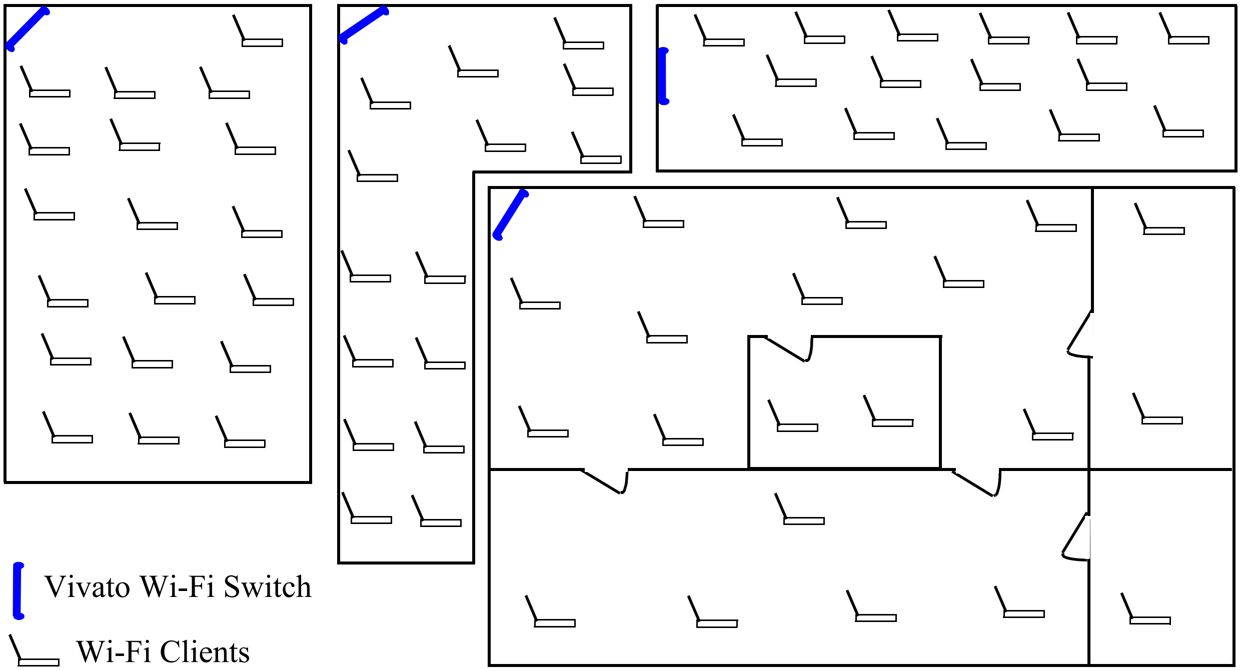
The Wi-Fi Switch’s antenna is designed to transmit and receive signals primarily in a 100° pattern from side to side (horizontally), and at a 12° pattern vertically. However, Wi-Fi operation outside of this pattern is typically available, especially near the Wi-Fi Switch. Also, various surfaces in the 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 Wi-Fi Switch depends on a number of factors, including:

- room shape and dimensions
- ceiling height
- availability of mains (AC) power and LAN connections
- wall construction materials and other obstructions (elevator shafts, metal panels, water pipes...)
- interfering signal sources (microwave ovens, 2.4 GHz cordless phones, other 802.11b devices...)

Analyzing Room Shape for Best Coverage

In general, position the Wi-Fi Switch to provide the greatest line of sight 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 Wi-Fi Switch flat against an end wall works well.



Ceiling Height Considerations

You should mount the Wi-Fi Switch 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 Wi-Fi Switch 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 Wi-Fi Switch higher would be beneficial.

Location #2 positions the Wi-FI Switch higher on the wall to maximize coverage on distant clients, while still providing 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 Wi-Fi Switch.

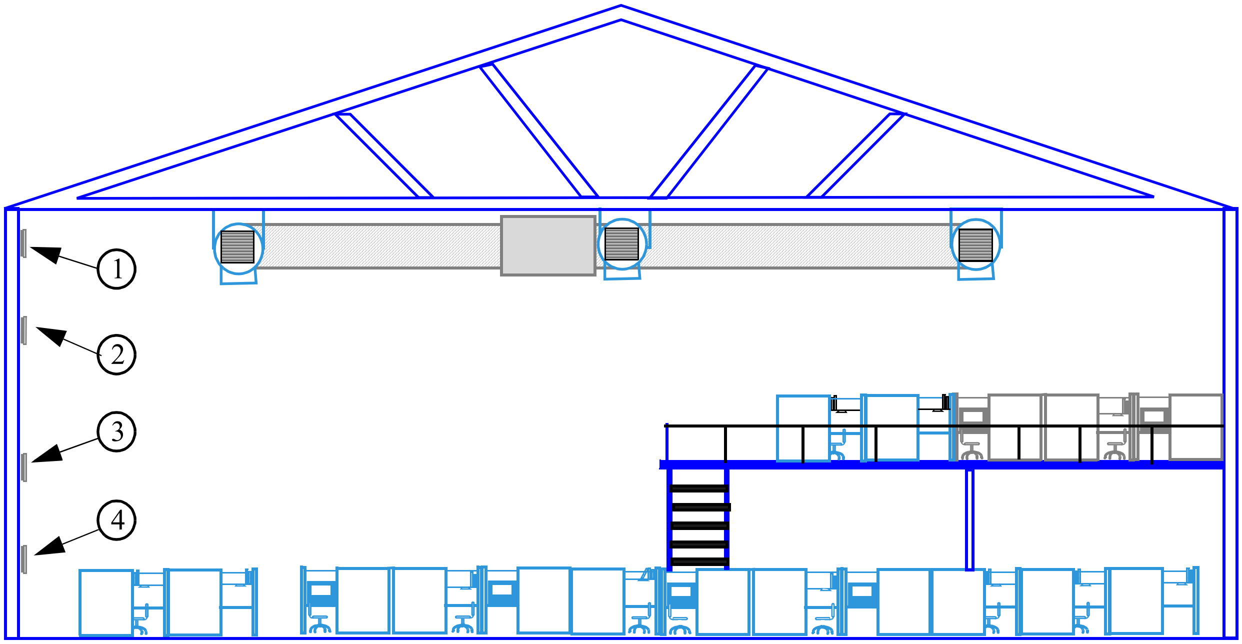


Figure 1—Location 2 Optimizes Wi-Fi Coverage

Minimizing Obstructions

Important ❗	The Wi-Fi Switch'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 Wi-Fi Switch. To provide maximum coverage, it is important that objects are not placed closer than this distance directly in front of the Wi-Fi Switch. For example, do not position the Wi-Fi Switch 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 Wi-Fi Switch where there are no obstructions directly in front of it.

The Wi-Fi Switch'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 the full 11 Mbps.

Interfering Signal Sources

IEEE 802.11b devices share the same unlicensed frequency band as other common devices, such as some radio frequency identification (RFID) systems, some cordless telephones, and microwave ovens. These devices produce radio frequency (RF) energy that can interfere with the Wi-Fi Switch'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 Wi-Fi Switch 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 **"Rogue Access Point Detection (RAPD) and Notification"** on page 83.

Environmental Considerations For Indoor Use

The following environmental specifications must be adhered to when mounting the Vivato 2.4 GHz Indoor Wi-Fi Switch:

- Operating temperature range: 32° to 122° F (0° to 50° C)
- Humidity: 10 % to 90% (non-condensing)

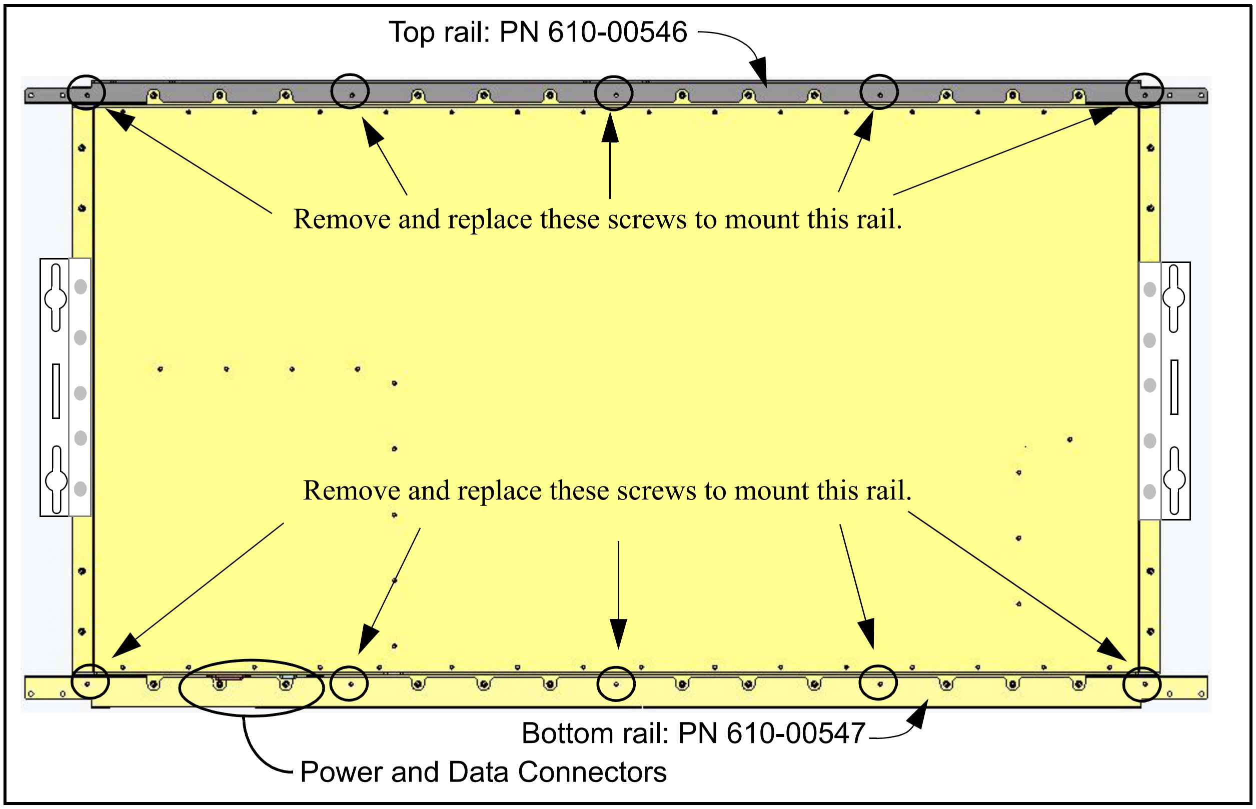
Assembling the Wi-Fi Switch

The top and bottom rails and end caps must be installed before mounting the Wi-Fi Switch. The fabric dress cover can be attached before or after mounting the Switch.

Attaching the Top and Bottom Rails

The top and bottom rails provide the mounting points for the end caps, Velcro® attachment area for the fabric cover, and channels for routing power and data cables. As shown below, the upper and lower rails have different part numbers and are not interchangeable.

Each rail is attached using five (5) screws that are pre-installed in the Wi-Fi Switch. To install the rails, remove the screws indicated below (#2 phillips), position the rails as shown, and replace the screws, tightening them to 10 in-lbs. (1.13 Nm).


Top rail: PN 610-00546
Remove and replace these screws to mount this rail.
Remove and replace these screws to mount this rail.
Bottom rail: PN 610-00547
Power and Data Connectors

Attaching the End Caps

The end caps must be installed *before* mounting the Wi-Fi Switch. Each cap is attached using four (4) of the provided self-tapping screws on each end (as shown below). Turn each screw in until the end cap is just held against the rail.

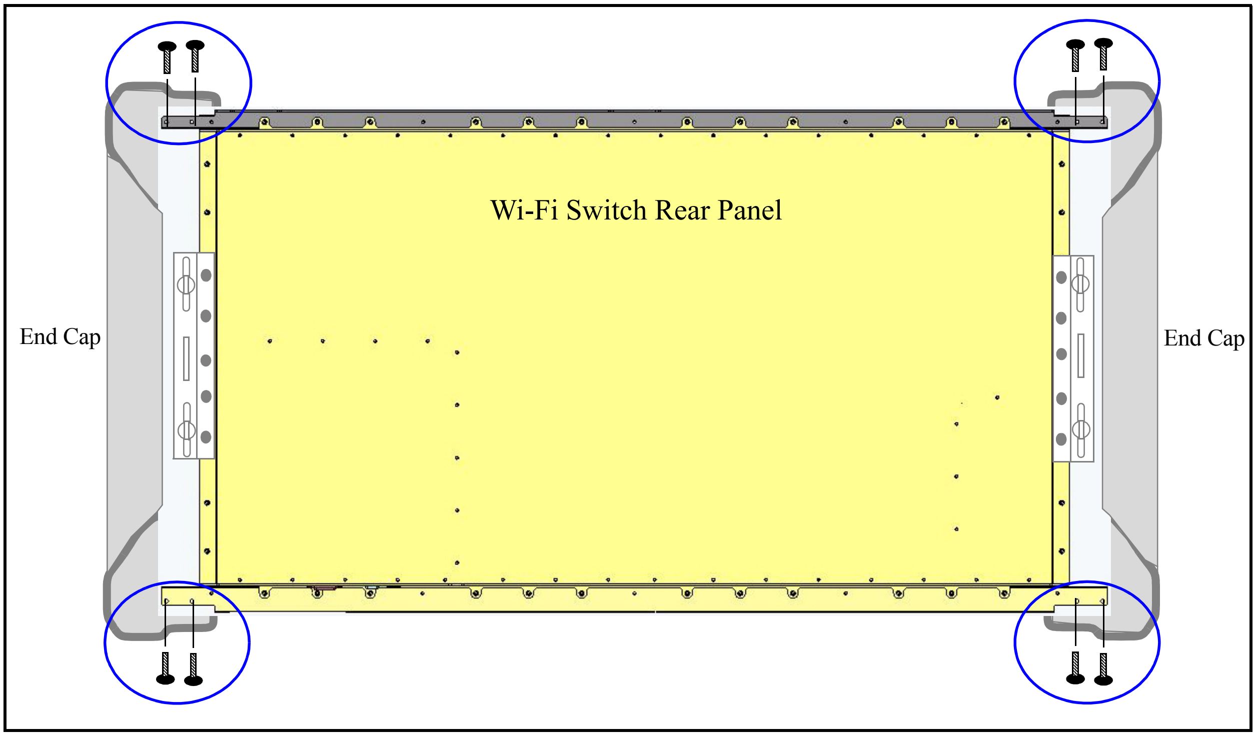


Figure 2—Installing the End Caps

Attaching the Fabric Cover

The fabric cover is attached to the Wi-Fi Switch using simple Velcro® strips. Position the cover over the Wi-Fi Switch's front panel and carefully press the fabric onto the corresponding velcro strips on the Switch. Be sure to orient the connector cut-outs in the Wi-Fi Switch's bottom flange with the openings in the fabric cover.

Cable Routing to the Wi-Fi Switch

Cabling for power and data connections for a wall-mounted Wi-Fi Switch can be routed above or below the Switch, through a center opening or through an offset opening.

Note: When routing cables through the top of the Wi-Fi Switch during the flush mount installation, be sure to route the cables *before* mounting the Switch. The optional corner mounts provides enough room behind the Wi-Fi Switch to allow cable routing after installation.

CAUTION —*Do not mount the Wi-Fi Switch upside down to change the orientation of the connections!*

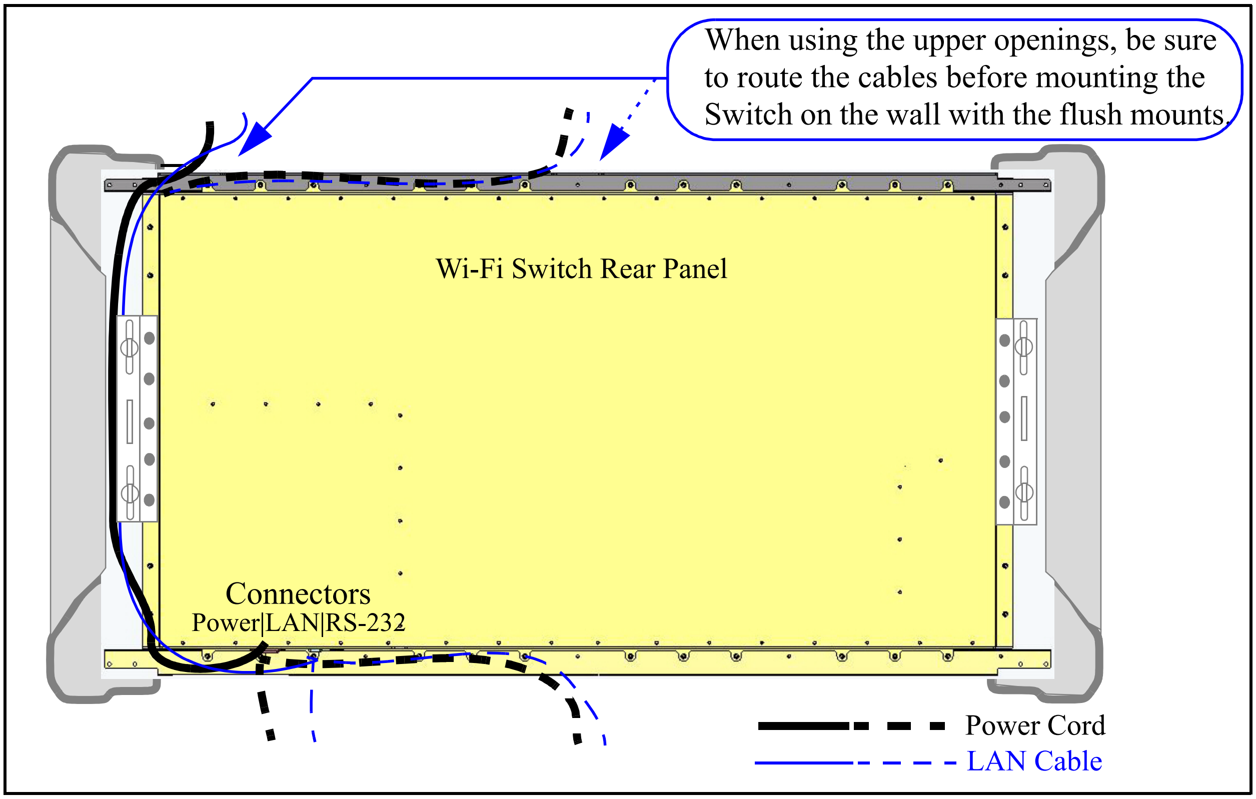

When using the upper openings, be sure to route the cables before mounting the Switch on the wall with the flush mounts.
Wi-Fi Switch Rear Panel
Connectors
Power|LAN|RS-232
Power Cord
LAN Cable

Figure 3—Available Cable Routing Methods

Mounting the Wi-Fi Switch

Mounting brackets are provided for flat wall installation. You can also order an optional corner mount bracket.

Four metal hollow wall anchors are provided for use with 5/8” commercial gypsum board (drywall). When installed and used properly, these fasteners can easily support the weight of the Wi-Fi Switch.

When mounting against brick, the use of lead anchors, or some other expanding fastener system that will not loosen in the bricks over time, is recommended.

Warning *The Vivato Wi-Fi Switch 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 Wi-Fi Switch in a manner that provides continued safety for persons and property is the sole responsibility of the installer. Do not mount the Wi-Fi Switch using brackets other than those approved by Vivato, Inc.*

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

Caution The Wi-Fi Switch is specifically designed to be operated with the power and data connectors pointing down. Do not mount the Wi-Fi Switch upside down to re-orient the connectors.

Mounting Weight Considerations

The total weight of the installed Wi-Fi Switch, including the top and bottom dress rails, end caps, and dress cover, is 40.5 lbs (18.4 kg).

Mounting The Wi-Fi Switch on a Wall (Flush Mount)

The following instructions show how to mount the Wi-Fi Switch flush against a wall by installing the supplied mounting brackets to the wall and then attaching the Wi-Fi Switch to those brackets.

1. Position one of the brackets a minimum of 7.5 in. (19 cm) below the ceiling. Using a level, make sure that the bracket is plumb (straight up and down) and that the notch in the side of the bracket faces outward from where the other bracket will be mounted. See **"Installing the Flush Mount Wall Brackets"** on page 12.
2. Mark the position for the supplied hollow wall anchors through the horizontal slots at the top and bottom of the bracket. Put the marks slightly in from the center of the notches.
3. 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.)
4. Insert the anchors into the 7/16” holes, and lightly tap on each anchor to seat it against the wall. See **"Installing the Wall Bracket Using the Hollow Wall Anchors"** on page 12.

5 Remove the anchor screws, and thread them through the wall bracket and into the anchors until the screw heads are flush against the bracket. Tighten the screws an additional 10 turns to seat the anchors - do not over-tighten. Verify that the bracket is plumb and adjust as necessary.

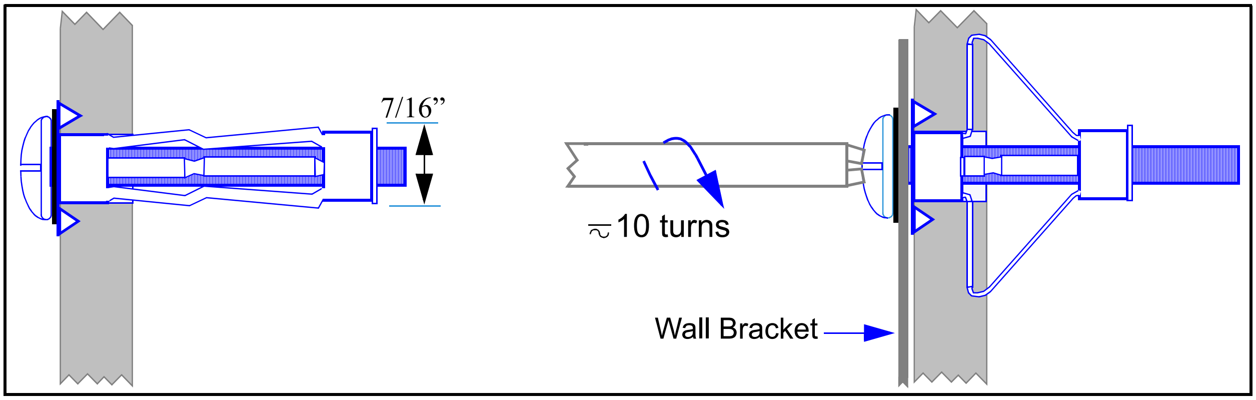
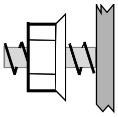


Figure 4—Installing the Wall Bracket Using the Hollow Wall Anchors

6 Mount the second bracket so that it is level with the first bracket, and is spaced exactly 40.5 in. (102.9 cm) apart from the first bracket at the inside edges.

7 Thread the supplied flange nuts out about half way on the bracket mounting studs.



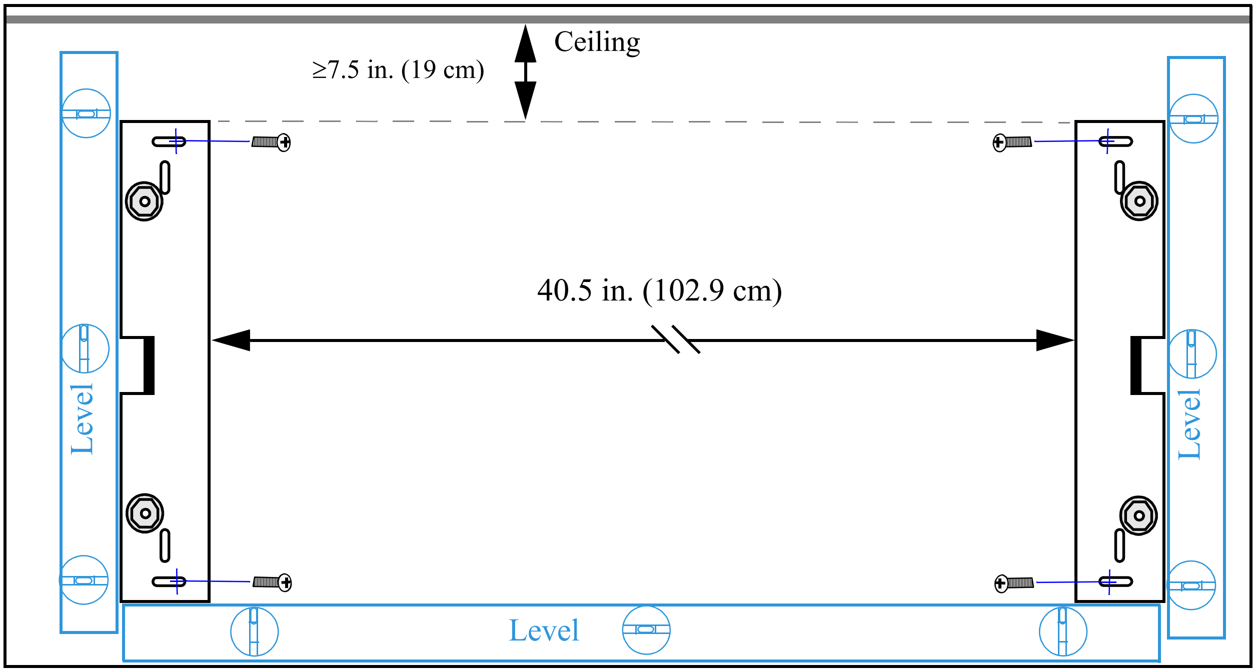


Figure 5—Installing the Flush Mount Wall Brackets

8 **This step should be performed with two people supporting the Wi-Fi Switch!** With its connectors and power switch towards the floor, position the Wi-Fi Switch so that the holes in its pre-installed brackets fit over the flange nuts on the wall brackets. See **Figure 6—Mounting the Wi-Fi Switch to the Flush Mount Wall Brackets**.

9 Slide the Wi-Fi Switch down fully into the slots in the brackets.

10 Carefully squeeze the end caps in to expose the flange nuts, and tighten the nuts using a 3/8" open end wrench.

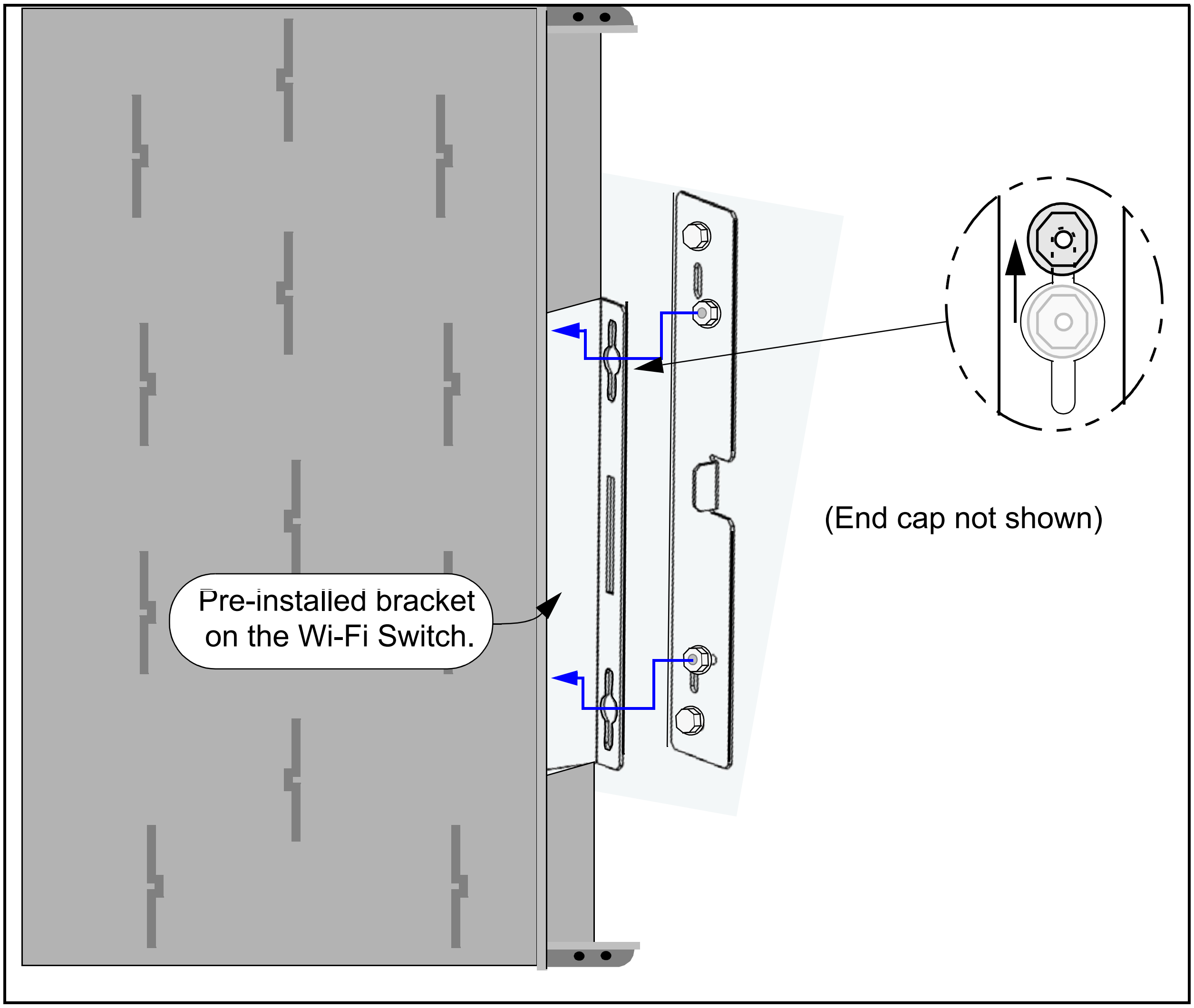


Figure 6—Mounting the Wi-Fi Switch to the Flush Mount Wall Brackets

Mounting the Wi-Fi Switch Using the Optional Corner Mount Kit

Follow these steps to mount the Wi-Fi Switch in a corner using the optional corner mount kit. **Locating the bracket mounting holes and mounting the Wi-Fi Switch on the bracket is best performed with two people!**

1. Position the bracket in the corner, a minimum of 9 in. (23 cm) below the ceiling. When positioned squarely between the walls, the distance from the corner to the inside edge of the hinged mounting plates is 22 7/16 in. (57 cm). See **Figure 7— Installing the Corner Mount Bracket**.
2. While holding the bracket in place, scribe a mark through each of the four mounting holes in both hinged mounting plates.
3. Using the scribe marks as a guide, install anchors or other reinforcements as necessary for your fasteners.

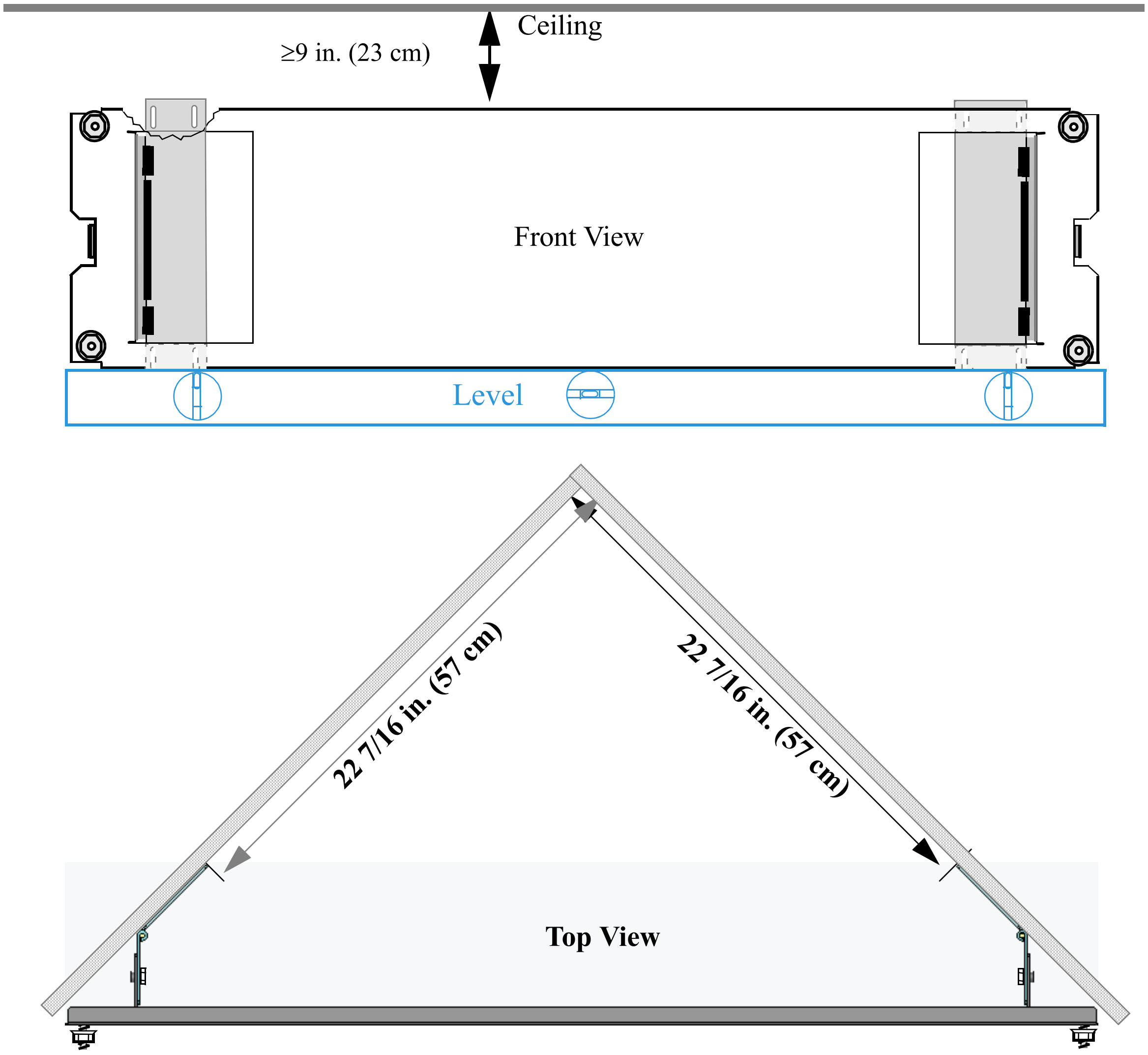


Figure 7—Installing the Corner Mount Bracket

4 Loosen the bracket adjustment screws to allow free movement of the hinged brackets on their mounting plates. See **Figure 8— Fastening and Adjusting the Corner Mount**.

5 Mount the bracket to the walls using your fasteners and anchors (shown below), making sure your fasteners are tight.

6 Using a level, adjust the bracket so that it is plumb (straight up and down), then tighten the adjustment screws.

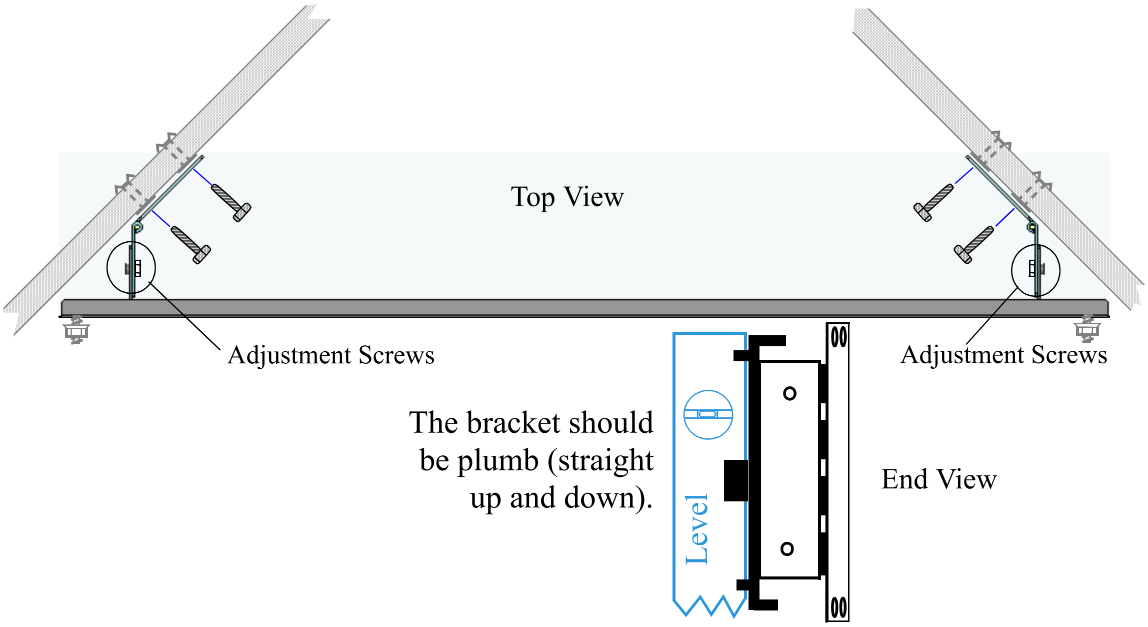
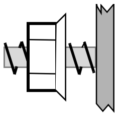


Figure 8—Fastening and Adjusting the Corner Mount

7 Thread the supplied flange nuts out about half way on the bracket mounting studs.



8 **This step should be performed with two people supporting the Wi-Fi Switch!**
With its connectors and power switch towards the floor, position the Wi-Fi Switch so that the holes in its pre-installed brackets fit over the flange nuts on the corner mount bracket. See **Figure 9— Mounting the Wi-Fi Switch to the Corner Bracket**.

9 Slide the Wi-Fi Switch down fully into the slots in the brackets.

10 Tighten the flange nuts using a 3/8” wrench.

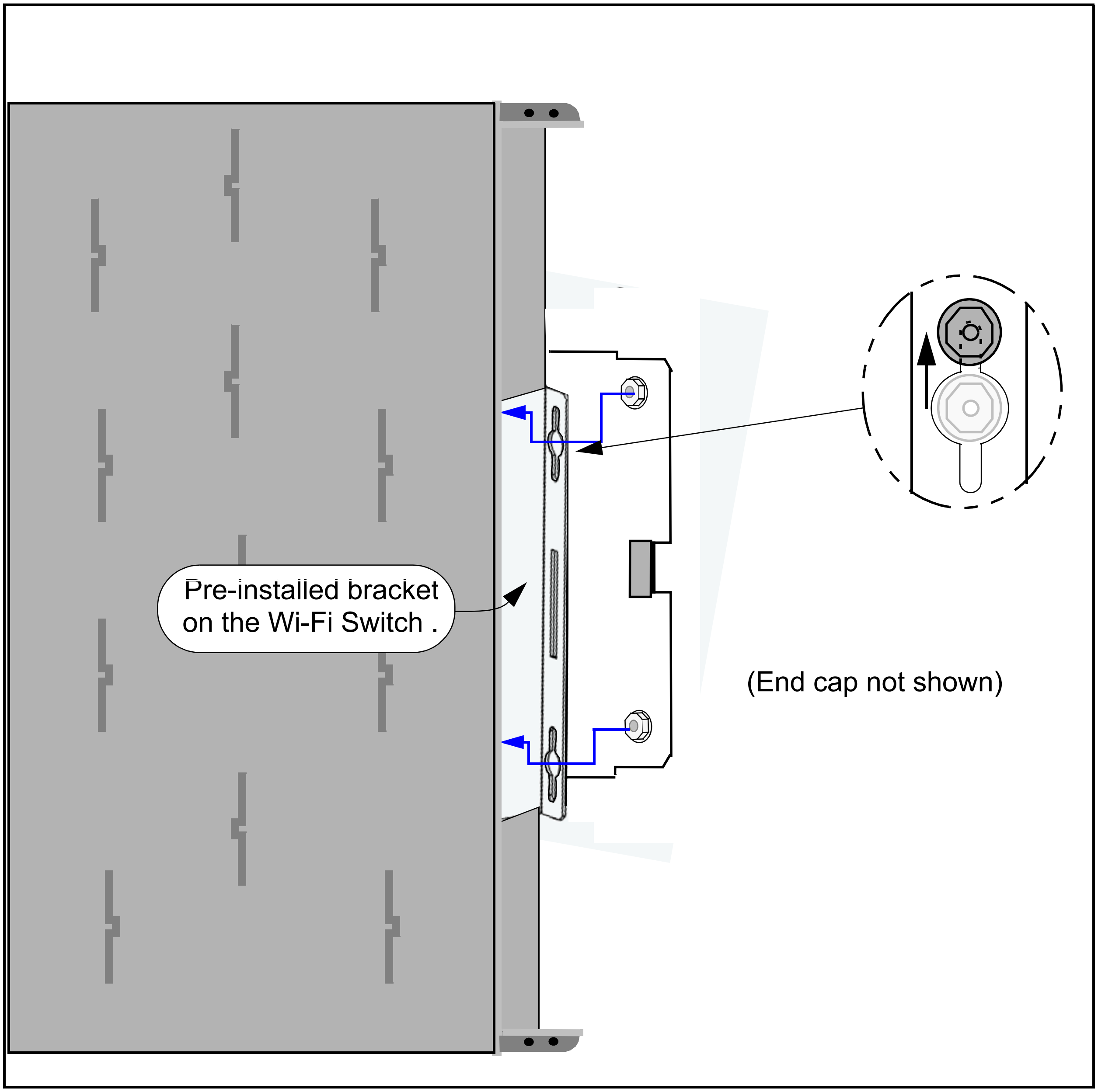


Figure 9—Mounting the Wi-Fi Switch to the Corner Bracket

Mains (AC) Power Requirements

The Vivato 2.4 GHz Indoor Wi-Fi Switch has the following power requirements:

Warning ⚠ *The Vivato Wi-Fi Switch uses a protective earth ground that must be supplied by the connected power cable. Do not attempt to bypass the earth ground terminal by using a two-conductor power cable or by removing the ground connection on the supplied power cable.*

- Line (mains) voltage: 100 - 240 VAC ± 10%, 50 - 60 Hz.
- Power consumption: 200 Watts (maximum)

Connections to the Vivato Wi-Fi Switch

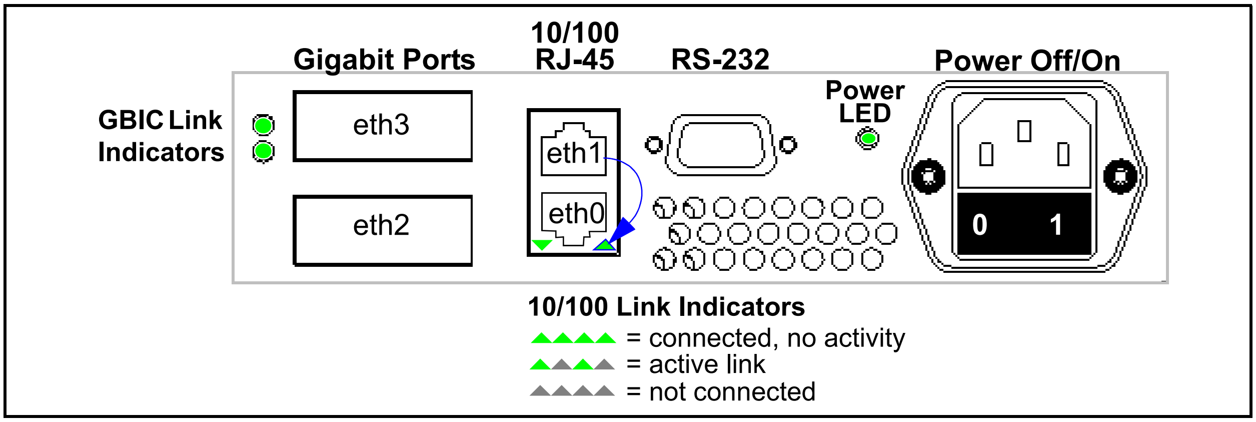


Figure 10—Connector Designations

Power Off/On - Mains (AC) power switch and connection.

Power LED - Indicates that the Wi-Fi Switch is turned on.

10/100 RJ-45 - 10/100 Base-T Ethernet ports designated as "eth0" and "eth1". These non-autosensing ports are enabled at delivery, and remain enabled unless you disable them during configuration.

10/100 Link Indicators - Lit but not blinking indicates connection to a device, but no link activity. Blinking indicates link activity. Not lit indicates no recognized data connection to a device.

Gigabit Ports - GBIC ports that accept fiber optic and wired adapters (adapters are not supplied with the Wi-Fi Switch). These ports are designated "eth2" and "eth3", and are for 1 gb operation only.

Warning ⚠ Fiber optic GBIC adapters use laser radiation (often invisible) that can be emitted when the cables are not connected. To avoid possible eye injury, do not look into the connector's fiber apertures.

RS-232 - 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 Wi-Fi Switch

The product label on the Wi-Fi Switch lists the MAC address of that Switch. This is the MAC address that is assigned to the eth0 port, and is also the "base" address for the MAC addresses assigned to the other interfaces on the Wi-Fi Switch. 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 are unique to each Wi-Fi Switch.)

Table 1—Interface MAC Address Assignments

Interface	MAC Address
eth0	00:0B:33:xx:xx:xx
eth1	00:0B:33:xx:xx:x+1
eth2	00:0B:33:xx:xx:x+2
eth3	00:0B:33:xx:xx:x+3
Reserved internal addresses	00:0B:33:xx:xx:x+4 to 00:0B:33:xx:xx:x+7
wireless interface 0 (wlan0)	00:0B:33:xx:xx:x+8
wireless interface 1	00:0B:33:xx:xx:x+9
wireless interface 2	00:0B:33:xx:xx:x+A
wireless interface 3	00:0B:33:xx:xx:x+B
wireless interface 4	00:0B:33:xx:xx:x+C
wireless interface 5	00:0B:33:xx:xx:x+D
wireless interface 6	00:0B:33:xx:xx:x+E
wireless interface 7	00:0B:33:xx:xx:x+F
wireless interface 8	00:0B:33:xx:xx:x+10

Table 1—Interface MAC Address Assignments

Interface	MAC Address
wireless interface 9	00:0B:33:xx:xx:x+11
wireless interface 10	00:0B:33:xx:xx:ss+12
wireless interface 11	00:0B:33:xx:xx:xx+13
wireless interface 12	00:0B:33:xx:xx:xx+14
wireless interface 13	00:0B:33:xx:xx:xx+15

Outdoor Wi-Fi Switch Installation

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

We recommend that you prepare your Vivato 2.4 GHz Outdoor Wi-Fi Switch for operation in the following order:

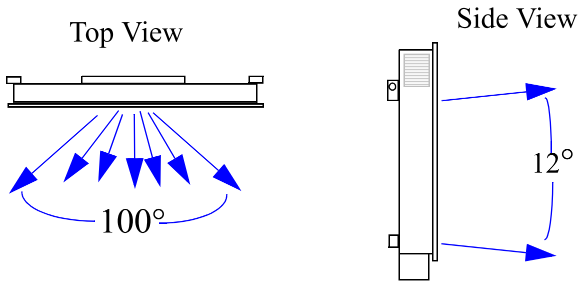
1. Verify the contents of the shipping container. See **Shipping Contents**.
2. Register your Vivato Wi-Fi Switch! You can select **Register Online Now!** here or on the Vivato CD startup page, or go to **http://www.vivato.net/wifiregistration.html.**
3. Fill out the *Vivato Wi-Fi Switch Configuration Worksheet*.
4. Analyze your sight to estimate the best place to mount the Wi-Fi Switch. See **"Where to Mount The Outdoor Wi-Fi Switch"** on page 22.
5. Configure the Wi-Fi Switch. 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. See **"Initial Configuration Using the Built-In Web Pages"** on page 35.
6. Mount the Wi-Fi Switch. See **"Mounting the Outdoor Wi-Fi Switch"** on page 24.
7. Connect the Wi-Fi Switch to mains (AC) power and your LAN. See **"Data Connections"** on page 33
8. Verify Wi-Fi Switch operation using your Wi-Fi client. See **"Verifying Wi-Fi Operation"** on page 151.

Shipping Contents

The following items are included in the shipping container with the Vivato 2.4 GHz Outdoor Wi-Fi Switch:

- Vivato Outdoor Wi-Fi Switch.
- DB-9 null modem cable
- 100 Base-T Ethernet cable (white)
- 100 Base-T cable cross-over Ethernet (red)
- Pipe mounting brackets (4)
- Quick Configuration Guide (11” x17” 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, 4-fold)

Where to Mount The Outdoor Wi-Fi Switch



The Wi-Fi Switch is designed to maximize operation in a 100° pattern from side to side (horizontally), and at a 12° pattern vertically. The Wi-Fi Switch's ability to communicate with clients at higher data rates begins to diminish as you get farther outside of this pattern. However, reliable Wi-Fi operation is often available outside of this pattern, especially when relatively close to the Wi-Fi Switch.

Figure 11—Wi-Fi Switch Antenna Pattern

Use the following guidelines to determine the best location for the Outdoor Wi-Fi Switch:

- For best performance, position the Outdoor Wi-Fi Switch where there are no outdoor obstructions close to a line of sight path to the intended client operating area. For example, trees contain large amounts of water, which can greatly weaken Wi-Fi signals. Make sure that no tree limbs or other foliage are within several feet of the line of sight path from the Wi-Fi Switch to the intended client coverage area.
- Do not position the Wi-Fi Switch farther away from the intended coverage area than is necessary. At a distance of 100 feet, the Wi-Fi Switch's antenna covers a *minimum* area of about 240 feet wide by 21 feet high (see below).

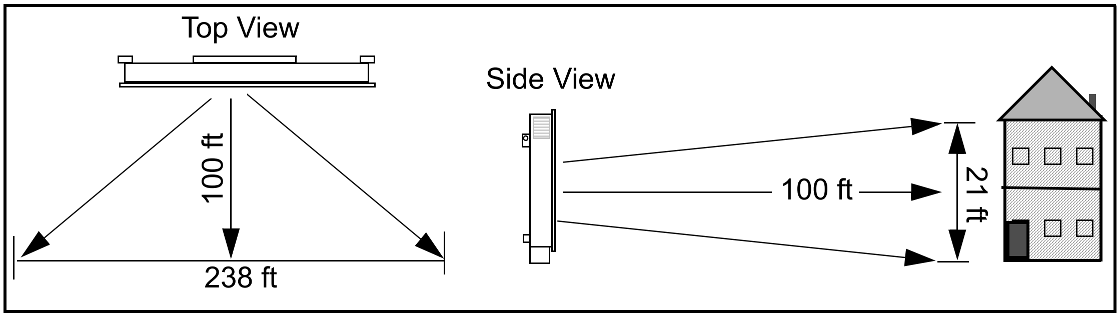
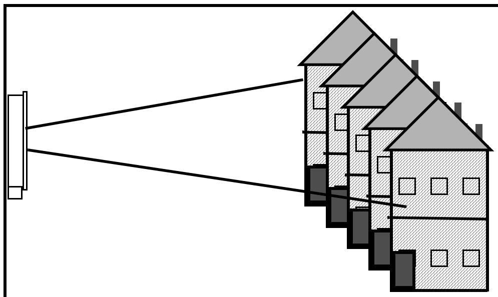
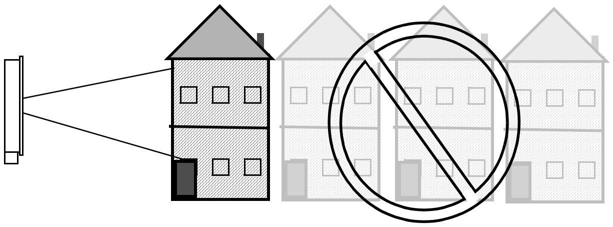


Figure 12—Example Coverage Area 100 Feet From the Wi-Fi Switch (not to scale)

- The Switch should be at least 16 feet from the outside of the structure where Wi-Fi is being provided.
- For a single building, or a horizontal row of buildings, center the Wi-Fi Switch in relation to the coverage area height and width to provide line of sight to each building. Do not position the Wi-Fi Switch where areas requiring Wi-Fi operation are directly blocked by another building (see below).



Position the Wi-Fi so that each building has line of sight access.



Do not position the Wi-Fi Switch where buildings requiring Wi-Fi coverage are blocked by other buildings.

- Where coverage is required in an area with structures of varying heights or were clients are widely dispersed, position the Wi-Fi Switch high enough so that all of the intended coverage area has line of sight clearance to the Wi-Fi Switch (see below). Keep in mind that you should not position the Wi-Fi Switch farther away from the clients than is required to have the clients inside the Switch’s antenna pattern.

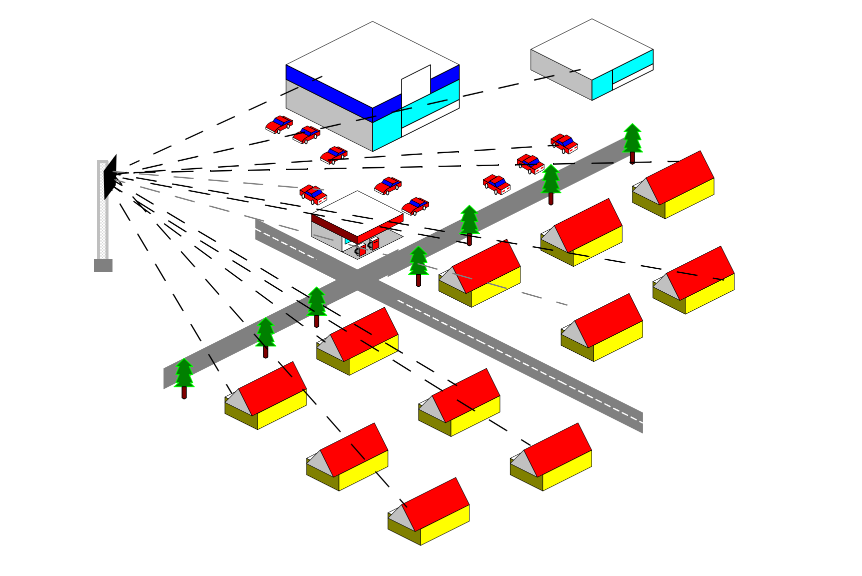


Figure 13—**Positioning The Wi-Fi Switch to Cover Widely Dispersed Clients**

Minimizing Obstructions

All materials provide some resistance to the wireless signal. However, very dense materials, such as metals, windows, and concrete, degrade the signal more than less dense materials, such as cloth cubicle panels or vinyl window awnings. As mentioned before, trees and other plants can greatly weaken the Wi-Fi Switch’s signal when placed near line of sight between the Wi-Fi Switch and intended clients.

Metallized surfaces, such as reflective window coatings, metal siding, metal window blinds, and foil-backed insulation, can significantly reduce penetration by Wi-Fi signals.

Some outdoor coatings, such as stucco, use a screen mesh to support it. Depending on the type of screen used, the screen can also significantly weaken the Wi-Fi signal.

The Wi-Fi Switch'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 the full 11 Mbps.

Important ❗ The Wi-Fi Switch'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 Wi-Fi Switch. To provide maximum coverage, it is important that objects are not placed closer than this distance directly in front of the Wi-Fi Switch. For example, do not position the Wi-Fi Switch facing directly against a wall, window, or other surface to try to provide coverage on the other side of that object.

Interfering Signal Sources

IEEE 802.11b devices share the same unlicensed frequency band as other common devices, such as some radio frequency identification (RFID) systems, some cordless telephones, and microwave ovens. These devices produce radio frequency (RF) energy that can interfere with the Wi-Fi Switch'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 Wi-Fi Switch 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 **"Rogue Access Point Detection (RAPD) and Notification"** on page 83.

Environmental Considerations For Outdoor Use

The following environmental specifications must be adhered to when mounting the Vivato 2.4 GHz Outdoor Wi-Fi Switch:

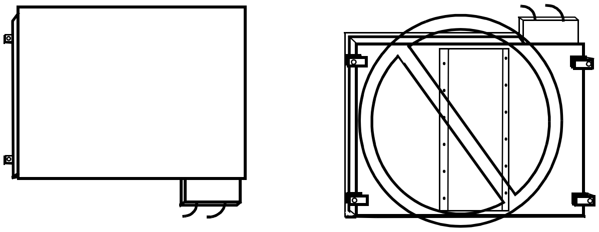
- Operating temperature range: -40° to 114.8° F (-40° to +46° C)
- Humidity: Product must be mounted vertically to assure protection from accumulated moisture.
- Wind loading: 100 MPH on any surface

Mounting the Outdoor Wi-Fi Switch

The Vivato 2.4 GHz Outdoor Wi-Fi Switch has four mounting points designed to allow for a variety of mounting scenarios.

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

Caution ⚠ The Outdoor Wi-Fi Switch is specifically designed to be operated with the power and data connector junction box facing down. Do not mount the Wi-Fi Switch upside down to re-orient the connectors.



Mounting Weight Considerations

The Vivato Outdoor Wi-Fi Switch weighs 80 lbs. (36.3 kg). The four supplied mounting clamps together weigh an additional 3.5 lbs (1.6 kg).

Outdoor Wi-Fi Switch Dimensions

The Vivato 2.4 GHz Outdoor Wi-Fi Switch has four mounting pads with 0.5" holes for attachment. The upper mounting pads also have lifting eyes for raising the Wi-Fi Switch into position. Use the following dimensions for mounting considerations:

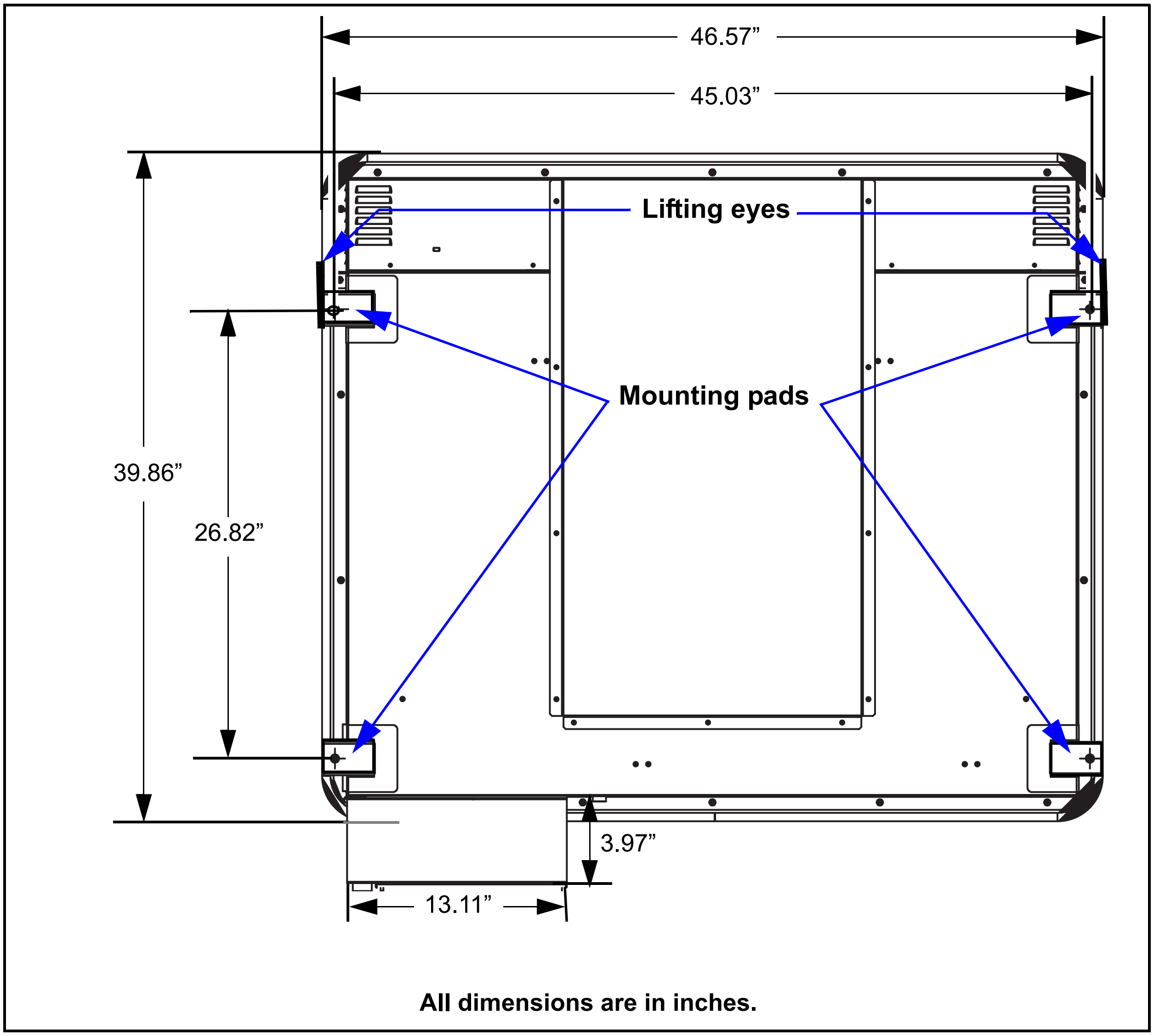


Figure 14—Outdoor Wi-Fi Switch Dimensions - Rear View

Mounting Hardware

The Vivato Outdoor Wi-Fi Switch is supplied with four (4) 2.5” pipe clamp mount assemblies that allow the Wi-Fi Switch to be mounted using a variety of commercially available mounting systems.

The pipe clamp mounts are fastened to the Wi-Fi Switch’s mounting pads using 3/8” bolts, flat washers, and split lock washers. The clamps use 5/16” U-bolts to secure two sections of 2.5” pipe (pipe is not included with the Wi-Fi Switch).

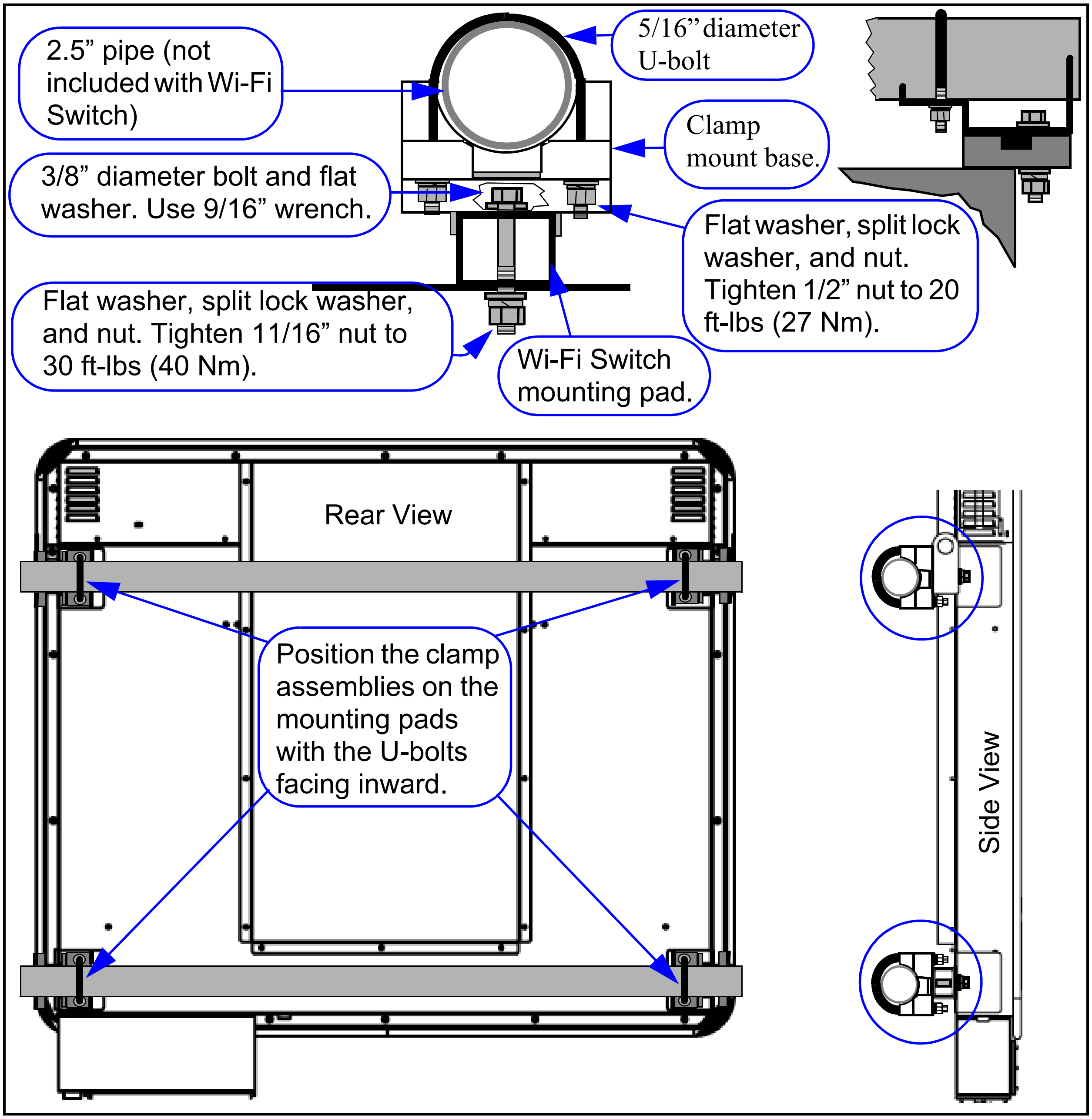

2.5” pipe (not included with Wi-Fi Switch)
5/16” diameter U-bolt
Clamp mount base.
3/8” diameter bolt and flat washer. Use 9/16” wrench.
Flat washer, split lock washer, and nut. Tighten 1/2” nut to 20 ft-lbs (27 Nm).
Flat washer, split lock washer, and nut. Tighten 11/16” nut to 30 ft-lbs (40 Nm).
Wi-Fi Switch mounting pad.
Rear View
Position the clamp assemblies on the mounting pads with the U-bolts facing inward.
Side View

Figure 15—Attaching the Supplied Pipe Clamp Mounting Brackets

Tower Mount Example

The figure below illustrates a possible tower mount installation using cross-over style mounting plates.

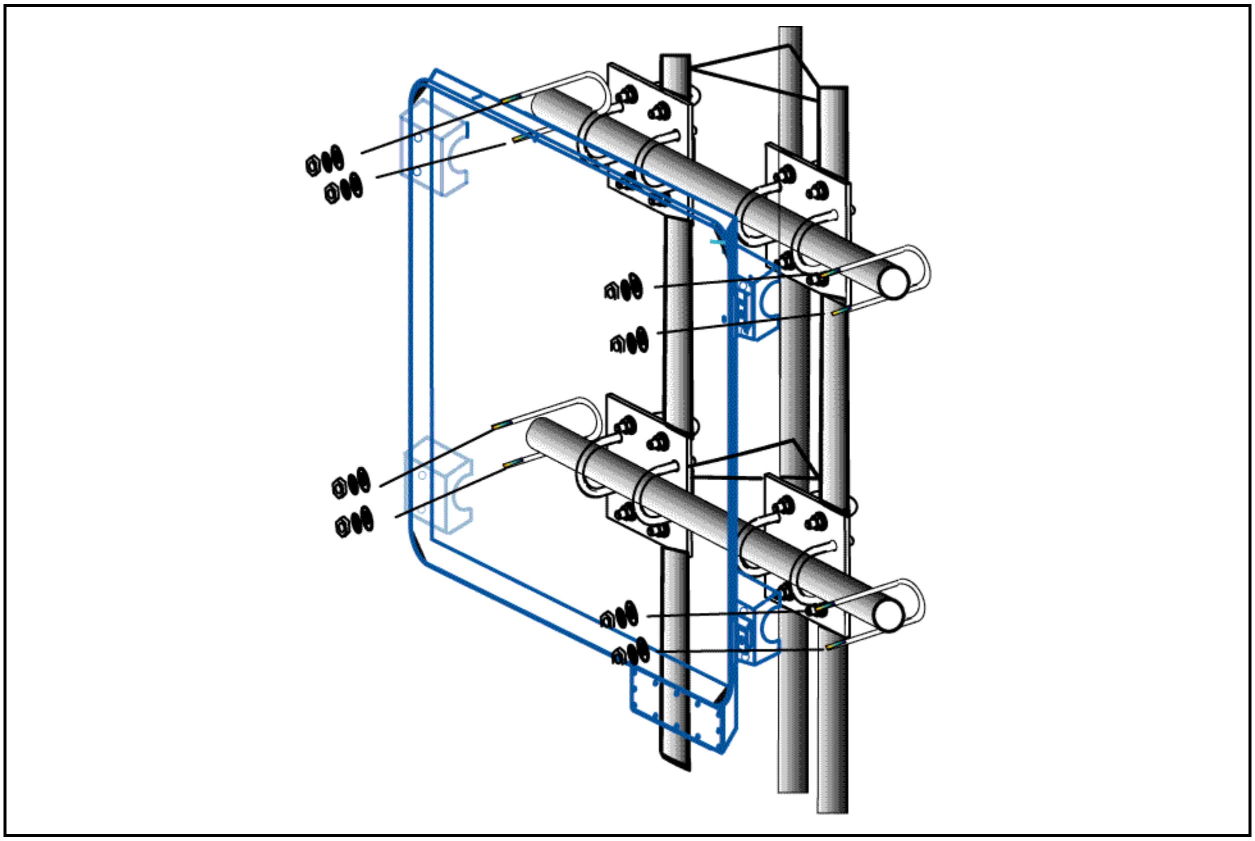


Figure 16—Outdoor Wi-Fi Switch Tower Mount Example

Building Face Mount Example

The figure illustrates a simple method for mounting the Vivato Outdoor Wi-Fi Switch on the exterior of a building.

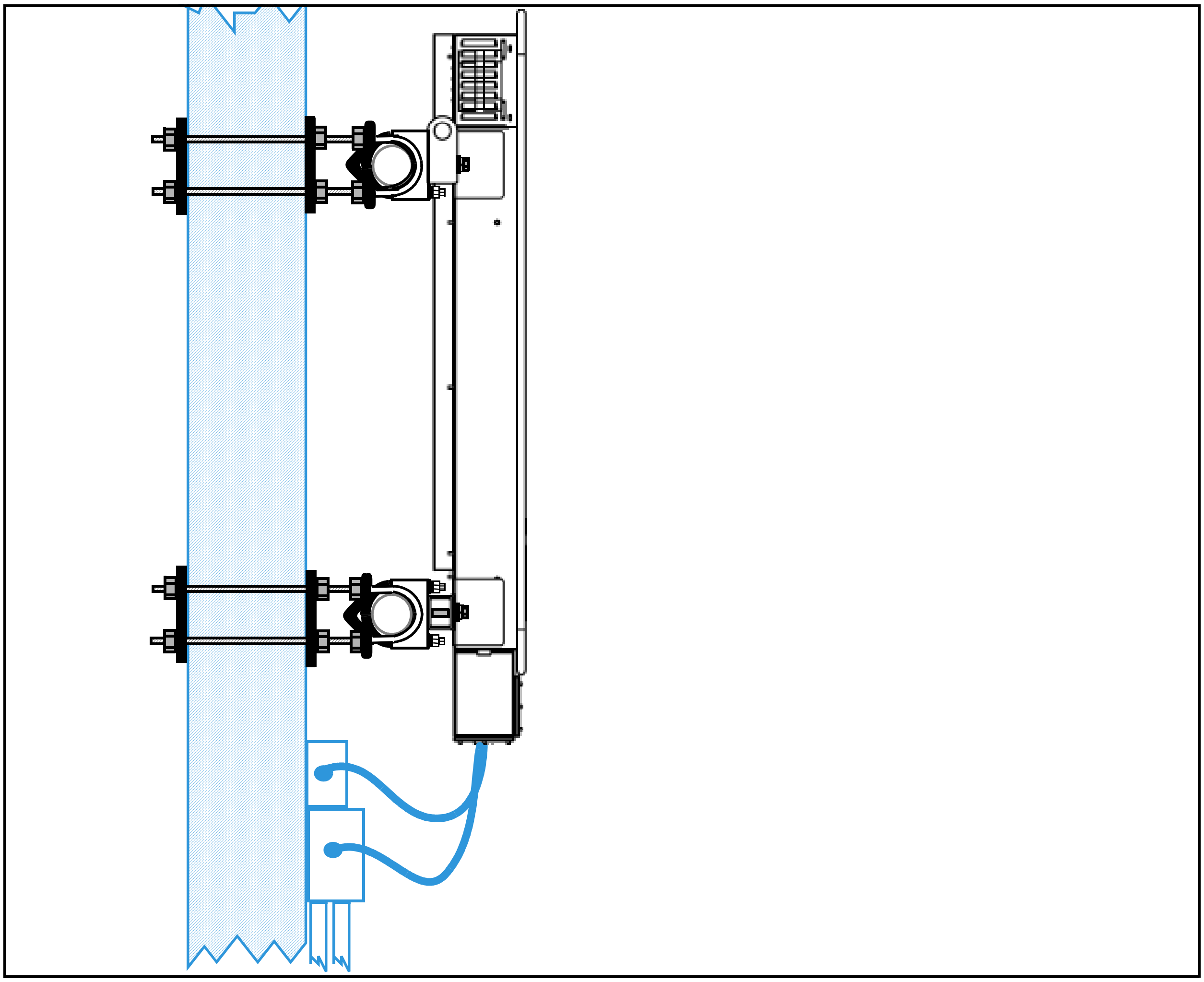
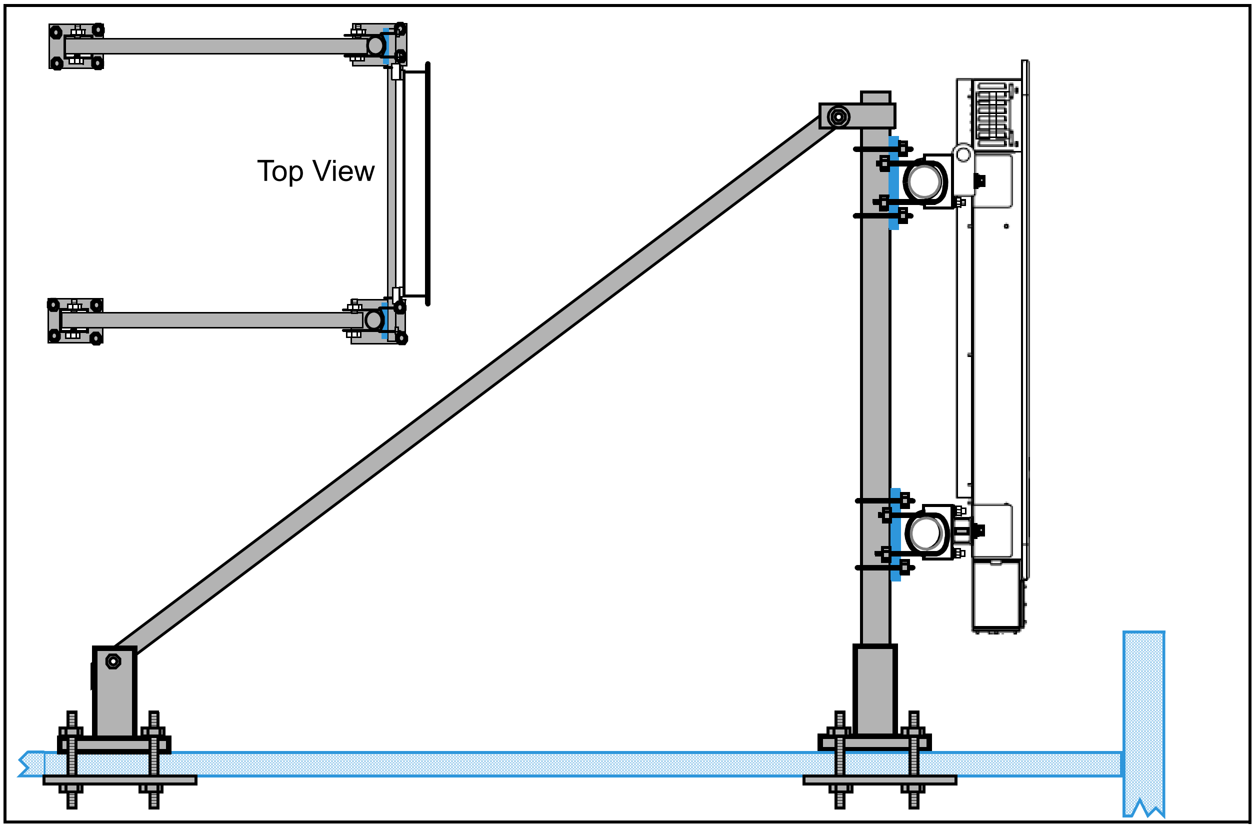


Figure 17—Outdoor Wi-Fi Switch Building Face Mount Example

Roof Top Mount Example

When mounting the Vivato Outdoor Wi-Fi Switch on a roof, the mounting structure must be strongly secured to the roof to prevent damage due to high wind loading against the Wi-Fi Switch.



Mains (AC) Power Requirements and Connections

The Vivato 2.4 GHz Outdoor Wi-Fi Switch has the following power requirements:

- Line (mains) voltage: 110 VAC ±10%, 50 - 60 Hz.
- Fuse: Buss® Class-G, Type SC, 15 Ampere, Time Delay

Power Consumption:

- Without cooling fans or optional heater operating: 200 Watts (maximum)
- With cooling fans operating: 332 Watts (maximum)
- With optional heater operating: 1200 Watts (maximum)

Warning *The Vivato Wi-Fi Switch uses a protective earth ground that must be furnished by the installer prior to powering on the Wi-Fi Switch, and must remain connected at all times.*

Surge Protection

Protection from power surges for the mains power and network connections must be provided during installation. Damage to the Wi-Fi Switch caused by power surges, including lightning, is not covered under the product warranty. The protection device(s) should be located as close as possible to the Wi-Fi Switch; typically within two feet (61cm). **Figure 18—Surge Protection Mounting Example**, shows typical power and network cabling when mounting the Wi-Fi Switch on a tower.

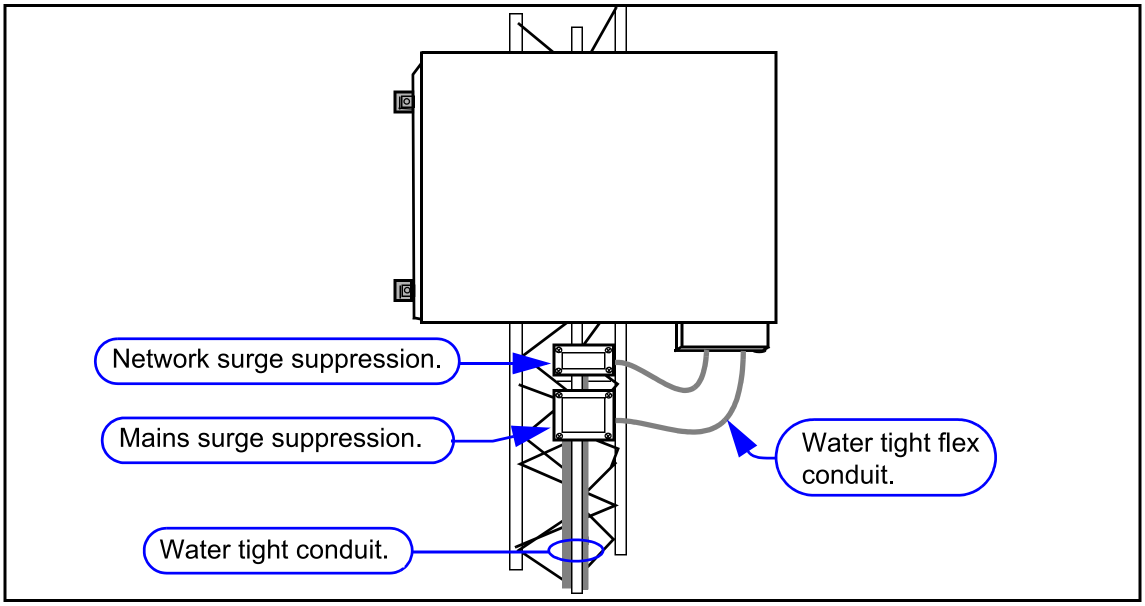


Figure 18—Surge Protection Mounting Example

Accessing Power and Data Connections in the Wi-Fi Switch

The junction box at the bottom of the Wi-Fi Switch provides access to power and data connections. A front and a bottom cover are used to maximize access to the junction box. Data connections are accessed by reaching through the junction box into the enclosure (see below). A chassis grounding bolt and nuts are provided on one of the mounting pads for grounding the enclosure, but this connection must not be used as a substitute for the power ground connection inside the junction box.

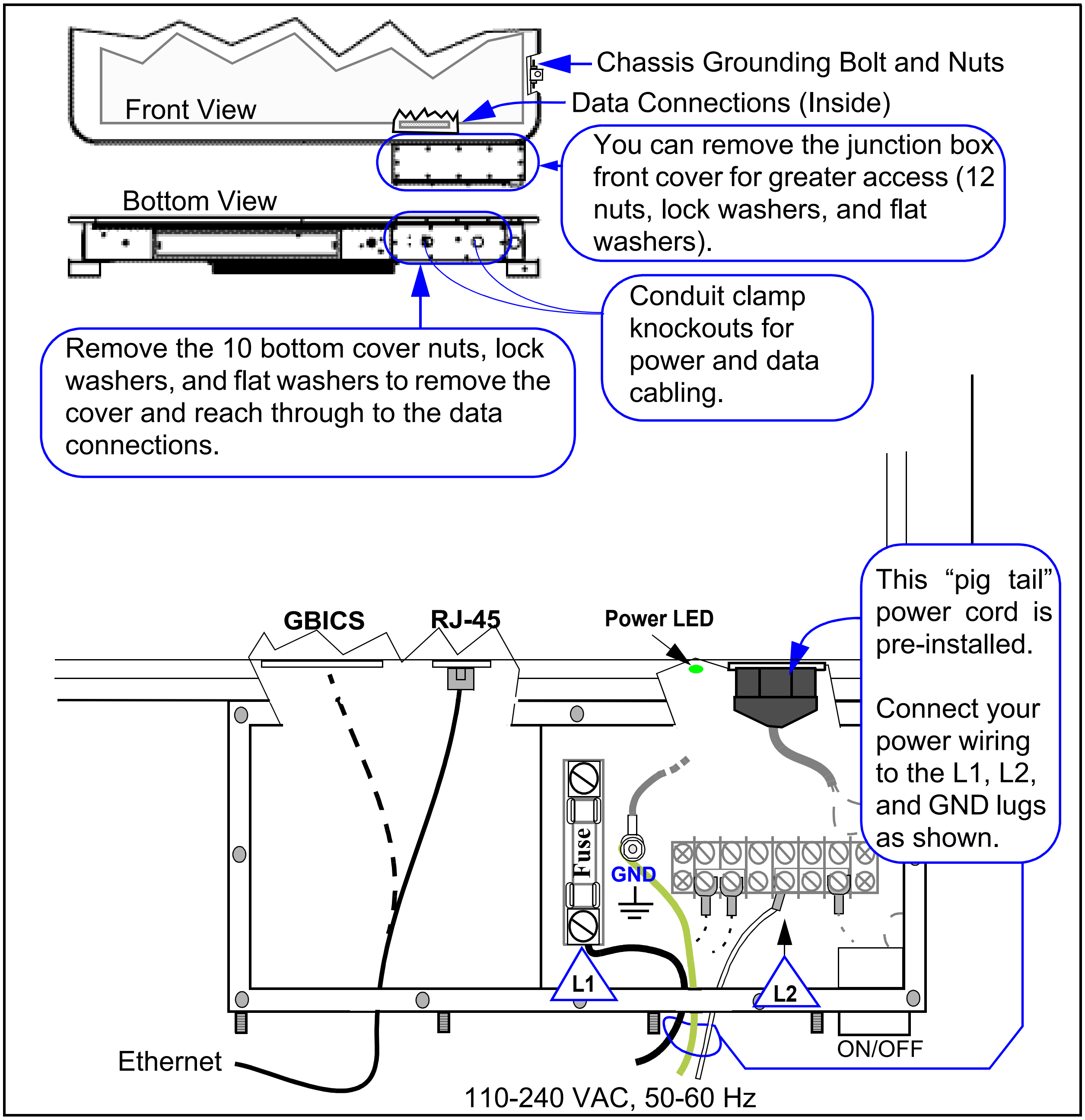

Front View
Chassis Grounding Bolt and Nuts
Data Connections (Inside)
You can remove the junction box front cover for greater access (12 nuts, lock washers, and flat washers).
Bottom View
Conduit clamp knockouts for power and data cabling.
Remove the 10 bottom cover nuts, lock washers, and flat washers to remove the cover and reach through to the data connections.
GBICS
RJ-45
Power LED
This "pig tail" power cord is pre-installed.
Connect your power wiring to the L1, L2, and GND lugs as shown.
Fuse
GND
L1
L2
ON/OFF
Ethernet
110-240 VAC, 50-60 Hz

Figure 19—Accessing Data and Mains Power Connections

Warning ⚠	*It is the responsibility of the person installing the Vivato Wi-Fi Switch to comply with all applicable wiring and building regulations and codes.*

Data Connections

Connections to the outdoor Wi-Fi Switch are accessible after removing the bottom junction box cover and looking through the junction box opening (as shown in **"Accessing Data and Mains Power Connections"** on page 32). With the exception of the power connections and power on/off switch, all other connections are identical to the indoor Wi-Fi Switch. See **"Connections to the Vivato Wi-Fi Switch"** on page 17.

Media Access Control (MAC) Addresses in the Wi-Fi Switch

The product label on the Wi-Fi Switch lists the MAC address of that Switch. See **"Interface MAC Address Assignments"** on page 18 for information on how MAC addresses are assigned in the Wi-Fi Switch.

Initial Configuration Using the Built-In Web Pages

The Vivato Wi-Fi Switch can be quickly configured using its built-in web page. Using the factory-supplied RJ-45 crossover cable and a computer with a network interface card that is set up for TCP/IP communication, you can quickly connect the Wi-Fi Switch to the computer and display the web pages to start configuration. If your computer has an IEEE 802.11b wireless client interface card installed and configured, you can access the configuration web page over the wireless connection.

Note: The web interface does not support all configurable settings at this time. Use the **Command Line Interface** (CLI) to make additional configuration changes.

The CLI is accessed through the RS-232 port using a terminal program or by using a secure shell program connected through an Ethernet connection. This is provided for users who are experienced at using a CLI. See **"Command Line Interface"** on page 97.

Caution ⚠ Security settings are initially disabled to allow your computer to access the web pages and configure the Wi-Fi Switch. To ensure Wi-Fi security before putting the switch into service, make the necessary changes to the security settings during the initial configuration. See **"Configuring Security"** on page 67.

Steps to Configuring the Vivato Wi-Fi Switch

Step 1. Connect a computer to the Wi-Fi Switch and access the Vivato Vision web pages. See **"Configuration Connections"** on page 37.

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

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

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

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

Step 6. Edit the security settings as needed to secure your network. See **"Configuring Security"** on page 67.

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

Step 8. Connect a cable from your LAN to the Wi-Fi Switch’s LAN port. See **"Connections to the Vivato Wi-Fi Switch"** on page 17.

Step 9. With your 802.11b clients properly configured, you should now have secure Wi-Fi operation between your clients and your LAN. See **"Verifying Wi-Fi Operation"** on page 151 to see how you can make sure that everything is working as expected.

Summary of Configuration Web Page Features

The configuration settings are organized under these headings:

- **Quick Setup** - Several setup pages are used to initially enter all of the critical settings to begin Wi-Fi operation. After entering these settings, you can start using the Wi-Fi Switch after rebooting it and connecting it to your wired network. Many of the settings on the initial setup screens are also available on other configuration screens.
- **Home** - Displays information about functions and interfaces enable in the Wi-Fi Switch's hardware and software. You can also access the VivatoVision Setup page from here to initially configure the Wi-Fi Switch or to change these settings at a later date.
- **Network** - Configures the wired and wireless interfaces, VLANs, bridges, and static routes.
- **Security** - Configures settings for WEP, PPTP, and EAP security operations.
- **Monitoring** - Displays system messages, rogue access point detection (RAPD) information, and a list of associated clients. Simple network management protocol (SNMP) is also configured from this screen.
- **System** - Configures functions such as secure shell and http operation, password changes, saving and retrieving configuration files, and accessing the Quick Setup page. This is also where you go to reboot the Wi-Fi Switch.
- **Diagnostics** - Provides ping and traceroute tools to see how packets are being handled.
- **Help** - Accesses the Vivato support website. For initial product shipments, you need to enter your user name and password to access this site. If necessary, contact your Vivato sales person for your user name and password.

Default Configuration

The Wi-Fi Switch is delivered with the following settings pre-configured. Until you change *and save* the configuration, these settings are used anytime the Wi-Fi Switch is rebooted:

- **All client security features are disabled**. *Unless your network is intended to be open to anyone who wants to access it, you should enable security in the Wi-Fi Switch before putting it into service.* This can be done by selecting **Security Options** on the Quick Setup web pages. You can also select the **Security** tab from the Vivato Vision Home page.
- **A default bridge (called br0) connects the RJ-45 Ethernet interfaces to all of the wireless interfaces**. This allows either a 10/100 Ethernet port or a wireless interface to be used for configuration, and provides immediate Wi-Fi operation with 802.11b clients. However, until you have configured your preferred method of security, you should not connect the Wi-Fi Switch to your wired network.
- **The GBIC ports (eth2 and eth3) are shut down.**
- **A static IP address of 169.254.20.1 and a net mask of 255.255.0.0 are assigned to the default bridge (br0).** *You usually need to change the IP address and net mask to operate with your*

network. This is one of the settings you can change on the Quick Setup web pages.

- **The default ESSID, the name that appears on wireless clients to identify the Wi-Fi Switch, is set to "Vivato"**. You do not have to change this entry, but you would typically set it to a name that would identify your system. This is one of the settings you can change on the Quick Setup web pages.
- **Wi-Fi channels 1 and 11 are distributed throughout the 100° pattern in front of the Wi-Fi Switch.** If necessary, channel assignments can be changed using the Quick Setup pages by selecting **Wireless Options**, or by using the **Network>Wireless** web page. For more information, see **"Wireless Interfaces"** on page 56.
- **A secure shell key has been generated, and secure shell operation is enabled, to allow configuration using a secure shell program.**
- **Hyper-text transfer protocol (HTTP) operation is enabled to allow access to the built-in configuration web pages.**
- **Traffic shaping is enabled to maximize 802.11b traffic.**

Configuration Connections

You can configure the Vivato Wi-Fi Switch using the built-in web page over either a wired or a wireless connection. Once the connection has been established, the procedure to configure the Wi-Fi Switch is the same for both methods.

The Wi-Fi Switch must be powered on for at least one minute before configuration.

For indoor Wi-Fi Switches, use the factory-supplied power cable to furnish power to the Wi-Fi Switch and turn the Wi-Fi Switch on (the power switch is built into the power connector module). The power LED lights continuously when the Wi-Fi Switch is powered on.

For outdoor Wi-Fi Switches, provide power as shown in **"Accessing Data and Mains Power Connections"** on page 32. The power LED is only visible by removing the bottom junction box cover and looking up into the enclosure. However, the enclosure's power on/off button lights when the Wi-Fi Switch is turned on.

Enabling Your Network Adapter to Access the Wi-Fi Switch

The IP address of the Wi-Fi Switch is within the range of 169.254.0.1 to 169.254.255.254. Your computer's network interface must be assigned an IP address within this range to initially access the configuration web pages or to access the command line interface using a secure shell. You can set your interface's IP address manually by accessing the network settings for the interface, disabling DHCP operation, and specifying an IP address in this range. You can also use automatic private IP addressing (APIPA) to set the network interface's IP address.

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

Note: If a DHCP server is configured on your network, be careful to not connect to your network until after APIPA has assigned an IP address to your interface; otherwise your DHCP server will assign an address to your interface that will prevent it from accessing the Wi-Fi Switch at the default IP address.

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

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

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

Using APIPA to Assign a Usable IP Address For Your Client

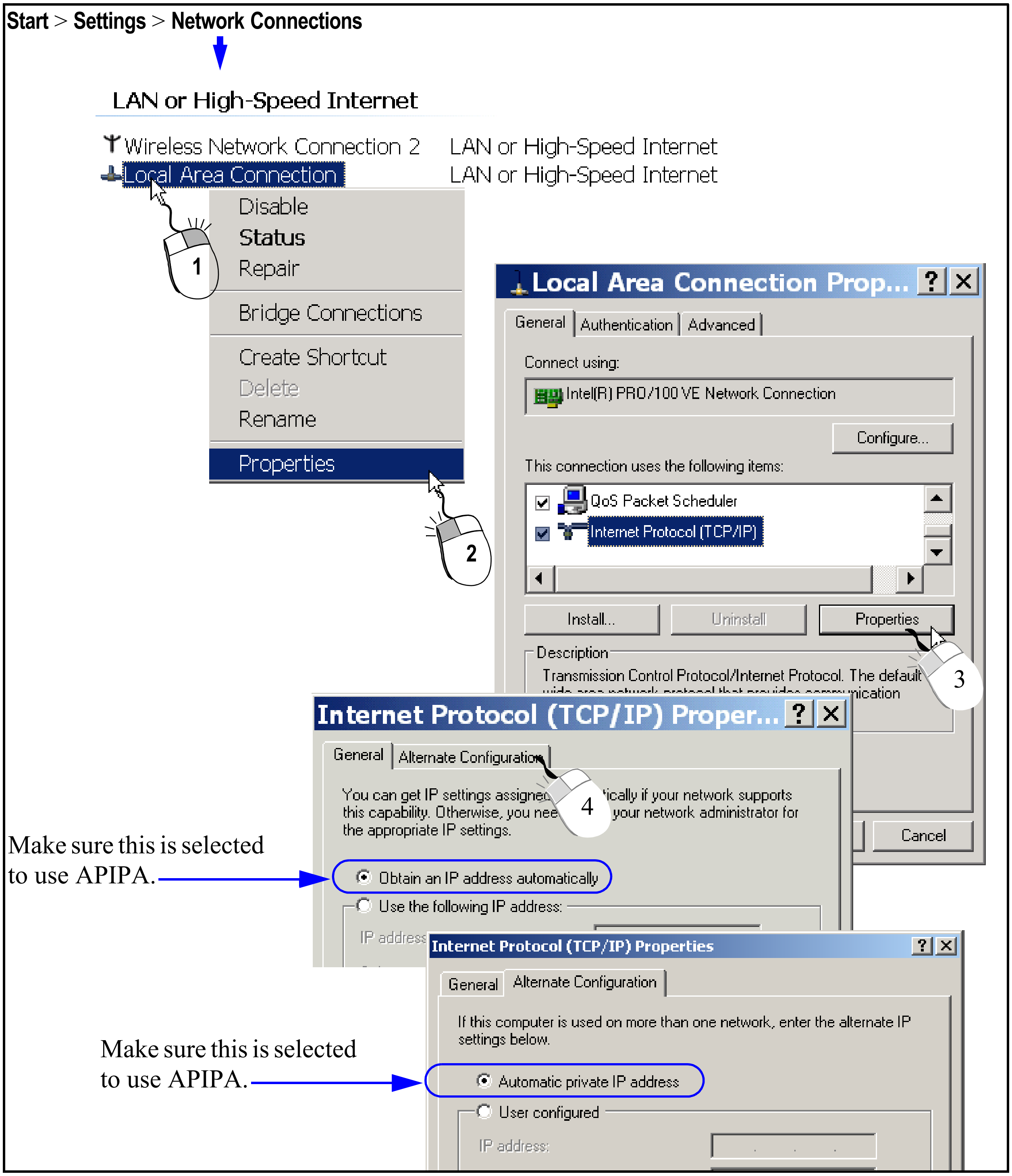
To get APIPA to assign an IP address to your interface that is accessible by the Wi-Fi Switch, use the following steps and refer to **Figure 20—Enabling Automatic IP Address Assignment on Your Wireless Client**:

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

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

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

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



Start > Settings > Network Connections
LAN or High-Speed Internet
Wireless Network Connection 2 | LAN or High-Speed Internet
Local Area Connection | LAN or High-Speed Internet
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties
1
2
3
4
Local Area Connection Prop...
General
Authentication
Advanced
Configure...
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Cancel
Internet Protocol (TCP/IP) Proper...
General
Alternate Configuration
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication

You can get IP settings assigne ...ically if your network supports this capability. Otherwise, you nee ... your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Make sure this is selected to use APIPA.

If this computer is used on more than one network, enter the alternate IP settings below.

● Automatic private IP address

○ User configured

IP address:

Make sure this is selected to use APIPA.

Figure 20—Enabling Automatic IP Address Assignment on Your Wireless Client

Step 5. Shut down your computer.

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

Wired Connection to Access the Configuration Web Page

After the Wi-Fi Switch has been powered on for at least one minute, connect the supplied RJ-45 crossover cable between your computer's network interface card (NIC) and the Wi-Fi Switch's eth0 port (see below).

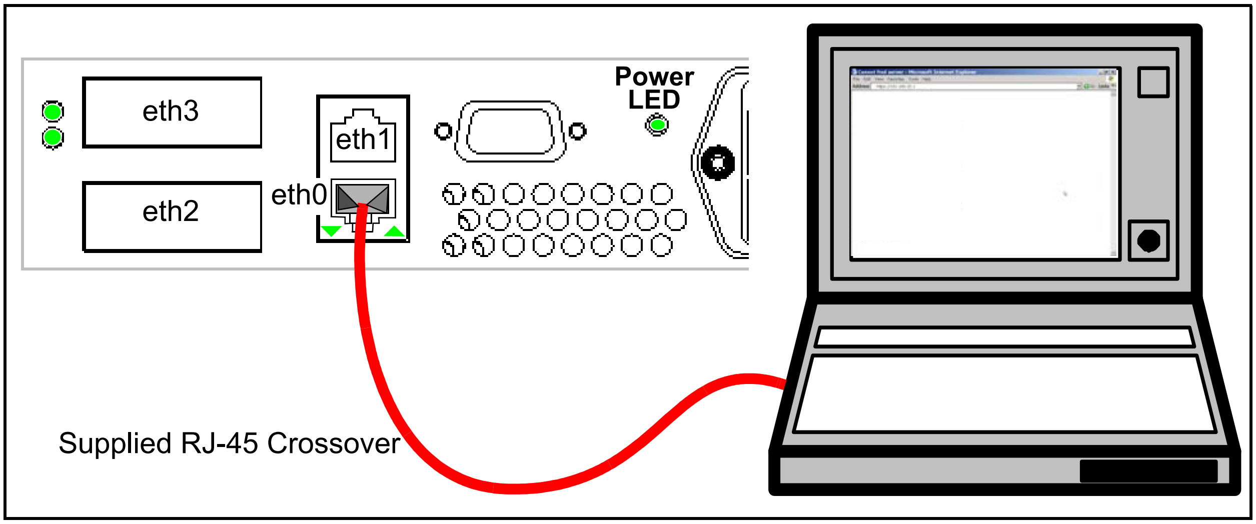
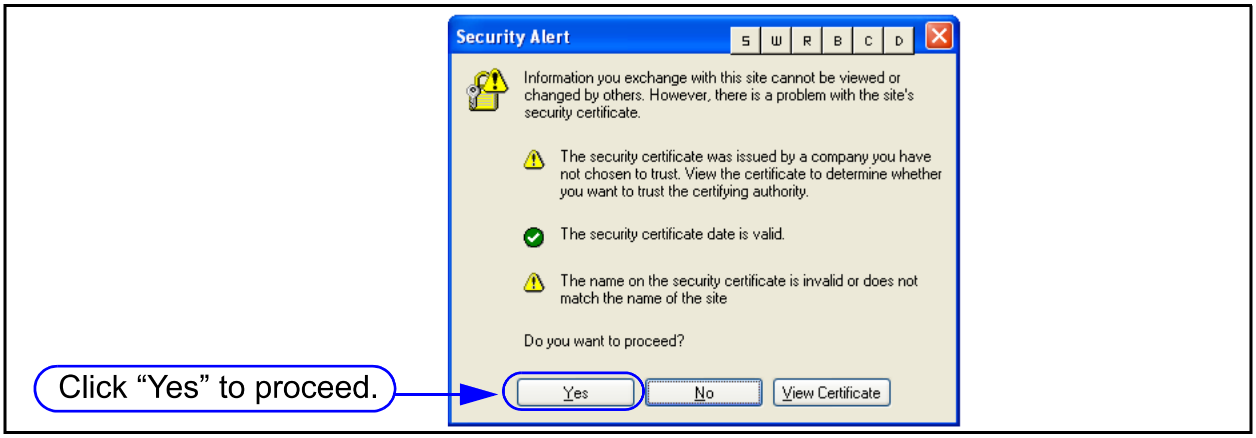


Figure 21—Wired Connection To Access The Configuration Web Page

Step 1. Turn on your computer. If APIPA is being used to assign an IP address for the NIC, wait for the DHCP server search to time-out and issue an address to the interface (about one minute).

Step 2. Launch a web browser in your computer. All popular browsers are supported. The minimum recommended display resolution is 800 x 600 pixels. The webpages are configured using a secure socket layer (SSL) connection.

Step 3. Enter the following Wi-Fi Switch IP address in the Address/Location field in your browser: **https://169.254.20.1**. A "Security Alert" may be displayed (shown below), asking if you want to proceed with connecting to the Wi-Fi Switch. Select "Yes".


Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

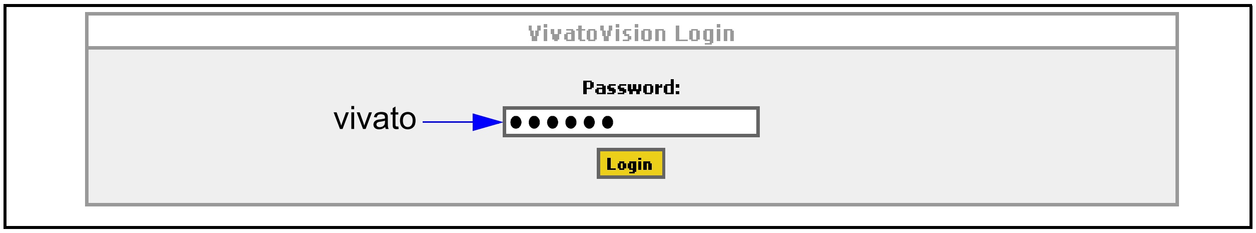
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Step 4. The Wi-Fi Switch's login prompt appears on your browser. Enter the default password: **vivato**



Important	Only the "Read" level password is needed *the first time* you access the Quick Setup web pages to configure and reboot the Wi-Fi Switch. However, the next time you access the Quick Setup pages you will need to enter the Enable password you specified during the initial configuration before you are allowed to make any changes to the configuration.

Step 5. Click on **Login** to display the initial Quick Setup page. See **"Entering the Initial Configuration Information in the Quick Setup Pages"** on page 43.

Wireless Configuration Connection

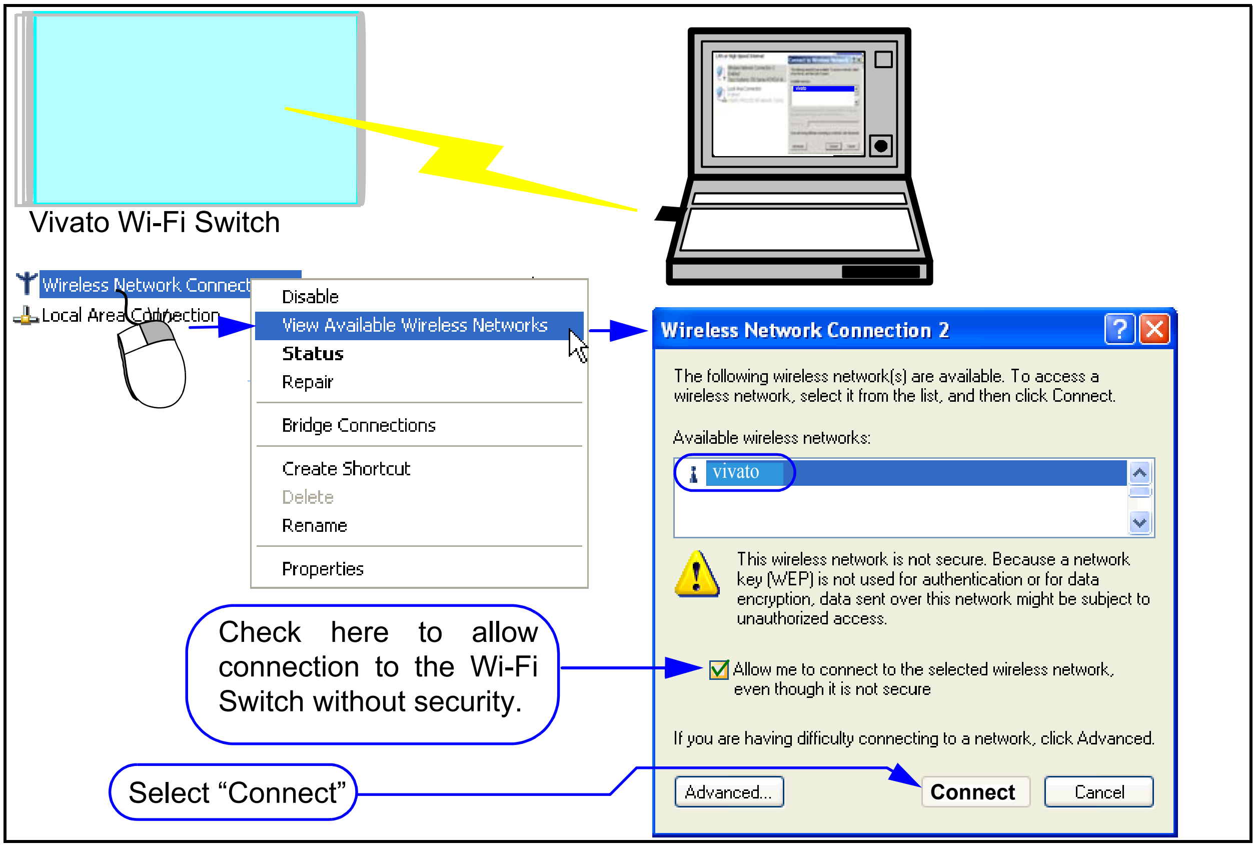
Turn your computer on and enable the wireless client. In the Microsoft Windows environment, this is typically done by selecting **Start** > **Settings** >**Network Connections** > **Wireless Network Connection**.

Step 1. Using the "Available Networks" or other search function, select the "**Vivato**" entry (see below).

Step 2. Because the Wi-Fi Switch is delivered with wireless security disabled to allow configuration through a wireless connection, you may need to confirm using an unsecured connection.

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

Step 3. Select "**Connect**" to begin associating with the Wi-Fi Switch.



The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.

Available wireless networks:

This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.

☑ Allow me to connect to the selected wireless network, even though it is not secure

If you are having difficulty connecting to a network, click Advanced.

Check here to allow connection to the Wi-Fi Switch without security.

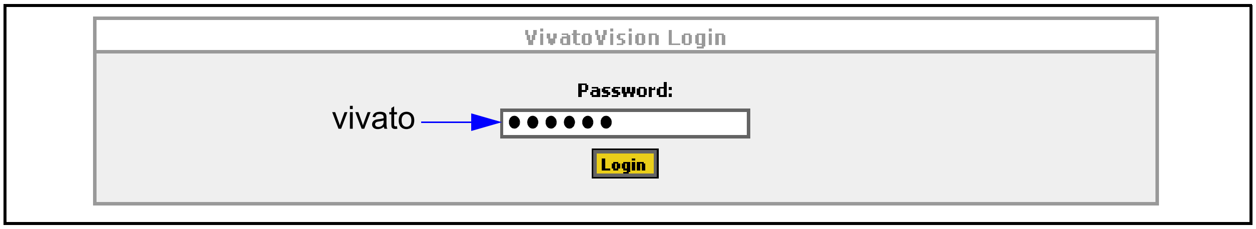
Select "Connect"

Figure 22—Wireless Connection to Access the Configuration Web Pages

Step 4. Launch a web browser in your computer. All popular browsers are supported. The minimum recommended display resolution is 800 x 600 pixels. The webpages are configured using a secure socket layer (SSL) connection.

Step 5. Enter the following Wi-Fi Switch IP address in the Address/Location field in your browser: **https://169.254.20.1**. The Wi-Fi Switch's login prompt appears on your browser.

Step 6. Enter the default password: **vivato**



Password: ●●●●●●

Important

Only the "Read" level password is needed *the first time* you access the Quick Setup web pages to configure and reboot the Wi-Fi Switch. However, the next time you access the Quick Setup pages you will need to enter the Enable password you specified during the initial configuration before you are allowed to make any changes to the configuration.

Step 7. Click on **Login** to display the initial Quick Setup page.

Entering the Initial Configuration Information in the Quick Setup Pages

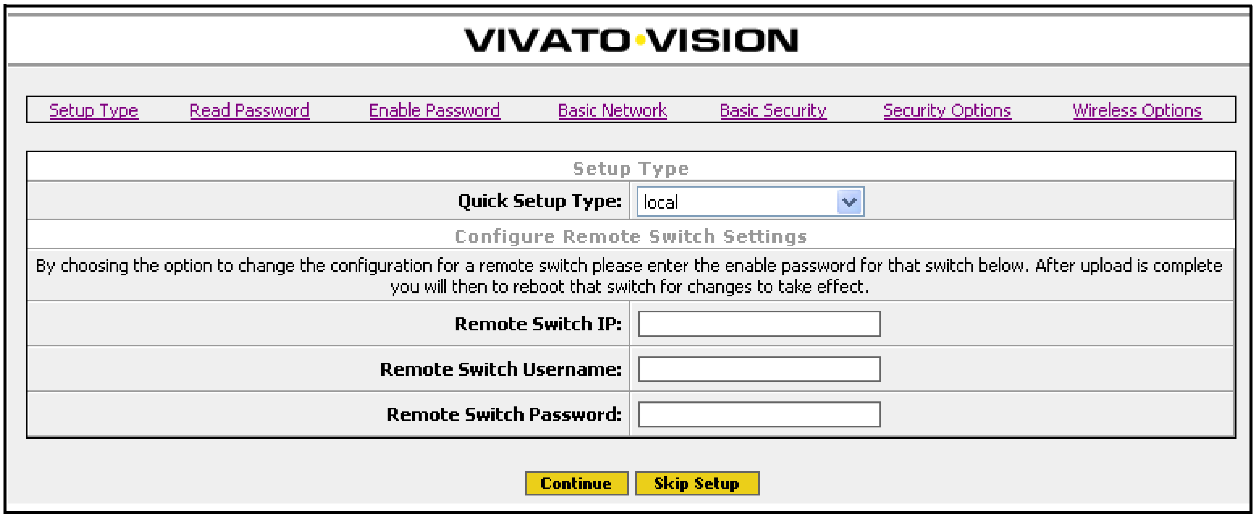
Enter the information in the **Setup Type** screen (shown below) and select **Continue** to continue to the **Read Password** settings. Continue to fill in the requested information on each screen until all of the Quick Setup screens have been configured and the Wi-Fi Switch is rebooted using the new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

The titles for each of the Quick Setup screens are highlighted as settings are completed on those screens.

The Quick Setup screens are displayed automatically the first time you access the configuration web pages, and each time after that until your configuration has been saved at least once. To access the Quick Setup screens at a later time, select **Quick Setup** on the Home configuration page.

Switch Selection

The settings made on the Quick Setup screens can be used to configure a local Wi-Fi Switch or a remote Wi-Fi Switch. This can reduce the need to log into other Switch's configuration web pages when configuring more than one Wi-Fi Switch.



Setup Type

Quick Setup Type: local

Configure Remote Switch Settings

By choosing the option to change the configuration for a remote switch please enter the enable password for that switch below. After upload is complete you will then to reboot that switch for changes to take effect.

Remote Switch IP:

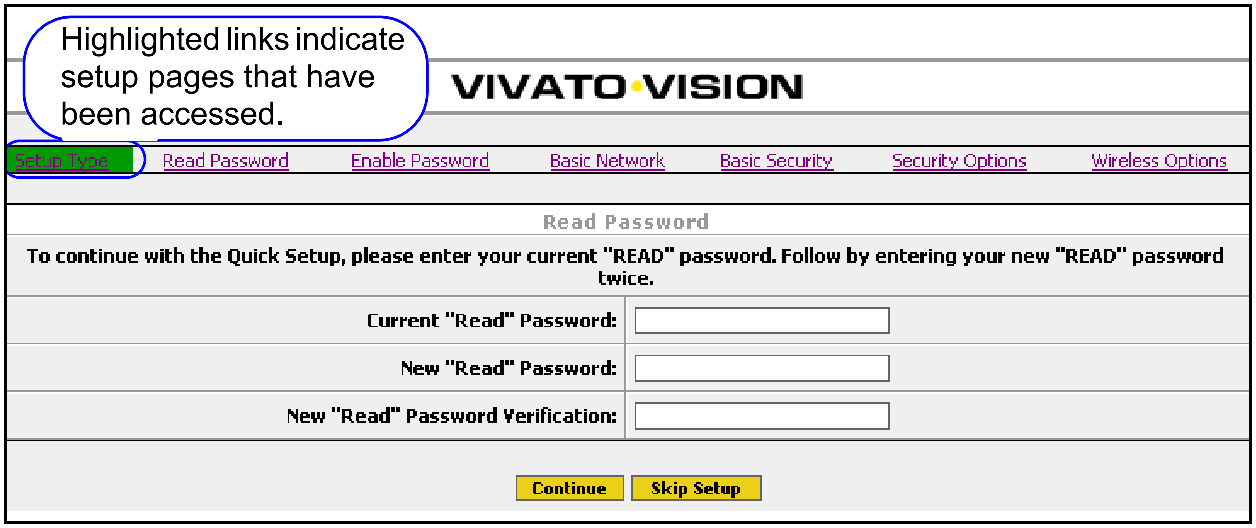
Remote Switch Username:

Remote Switch Password:

- **Quick Setup Type**: Select "**local**" to send the Quick Setup settings to the Wi-Fi Switch you are currently connected to. Select "**remote**" to configure another Wi-Fi Switch. Remote configuration requires you to enter the enable password of the other Wi-Fi Switch.
- **Configure Remote Switch Settings** : When configuring a remote Wi-Fi Switch, enter the IP address, the user name, and the enable password of that Switch. All configuration settings made using the Quick Setup pages will be sent to the specified Wi-Fi Switch when it is rebooted at the end of the quick setup process.

Read Password Setup

The read password protects unauthorized viewing of configuration settings.



Highlighted links indicate setup pages that have been accessed.

Read Password

To continue with the Quick Setup, please enter your current "READ" password. Follow by entering your new "READ" password twice.

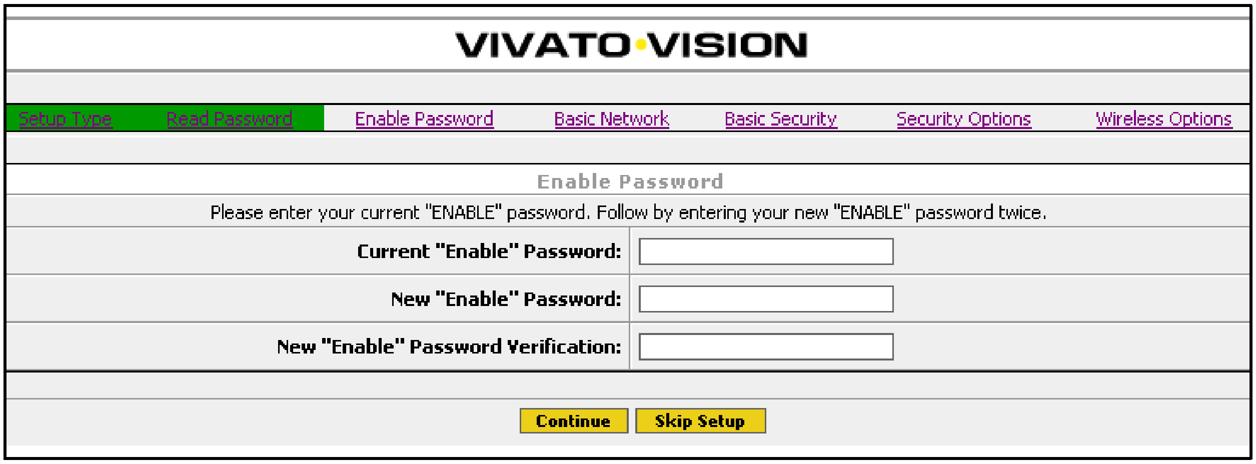
Current "Read" Password:	
New "Read" Password:	
New "Read" Password Verification:	

Figure 23—Read Password Setup Page

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

Enable Password Setup

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



Enable Password

Please enter your current "ENABLE" password. Follow by entering your new "ENABLE" password twice.

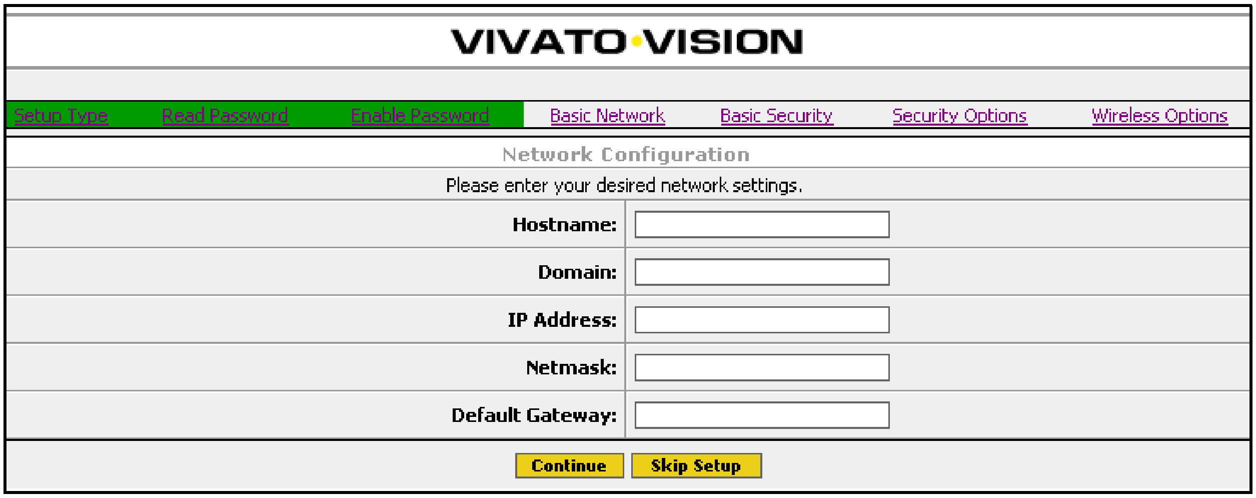
Current "Enable" Password:	
New "Enable" Password:	
New "Enable" Password Verification:	

Figure 24—Enable Password Setup Page

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

Basic Network Setup

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



Network Configuration

Please enter your desired network settings.

Hostname:	
Domain:	
IP Address:	
Netmask:	
Default Gateway:	

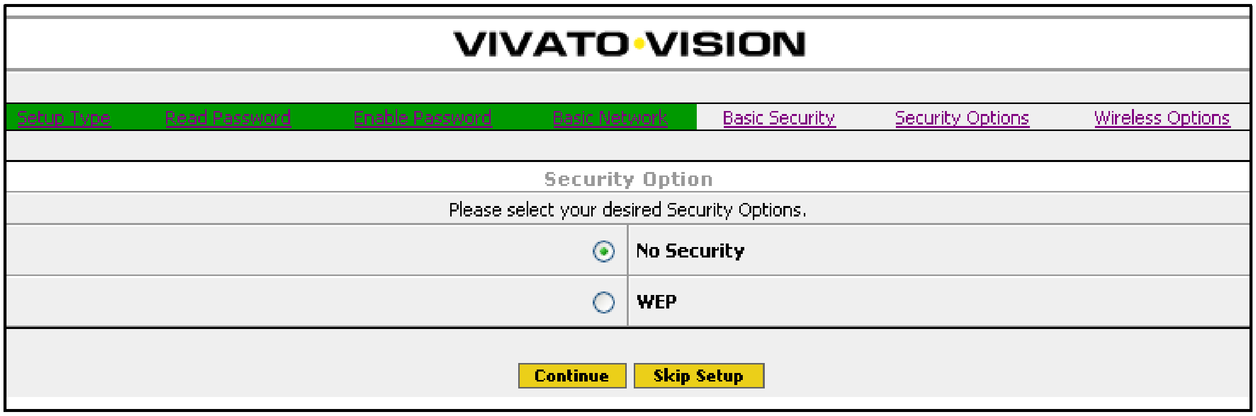
Figure 25—**Basic Network Setup Page**

- **Hostname**: Enter a name to be used to refer to the Wi-Fi Switch in your *wired* network. For your network to be able to identify the Wi-Fi Switch using this name it typically needs a domain name service (DNS) server.
- **Note**: This entry is NOT the name that *wireless* users see when searching for the wireless network; that name is specified for the extended service set identifier (ESSID).
- **Domain**: Enter the name of the domain where the Wi-Fi Switch will be used.
- **IP Address**: Enter an IP address for the Wi-Fi Switch. *Note: The IP address and Netmask are assigned to the default bridge (br0) during the Quick Setup process. If you need to delete the default bridge for your desired configuration, enter the standard information in the Quick Setup pages and reboot the Wi-Fi Switch, then access the configuration pages again and select the* **Network** *tab. Assign the IP address to the desired interface (logical or physical) before deleting the bridge.*
- **Netmask**: Enter an IP net mask for the Wi-Fi Switch.
- **Default Gateway**: Enter the IP address of the default gateway for your wired network.

Basic Security Setup

The Basic Security settings are used to select the type of security to use. Unless your network is intended to be totally open for use by any 802.11b client, you should always configure some type of security.

Note: To use EAP or PPTP security. For this pre-production release, select **No Security** and proceed to the **Wireless Options** setup page and reboot the Wi-Fi Switch when prompted. Access the configuration web pages using your new IP address and select the **Security** tab to enable and configure the desired type of security.



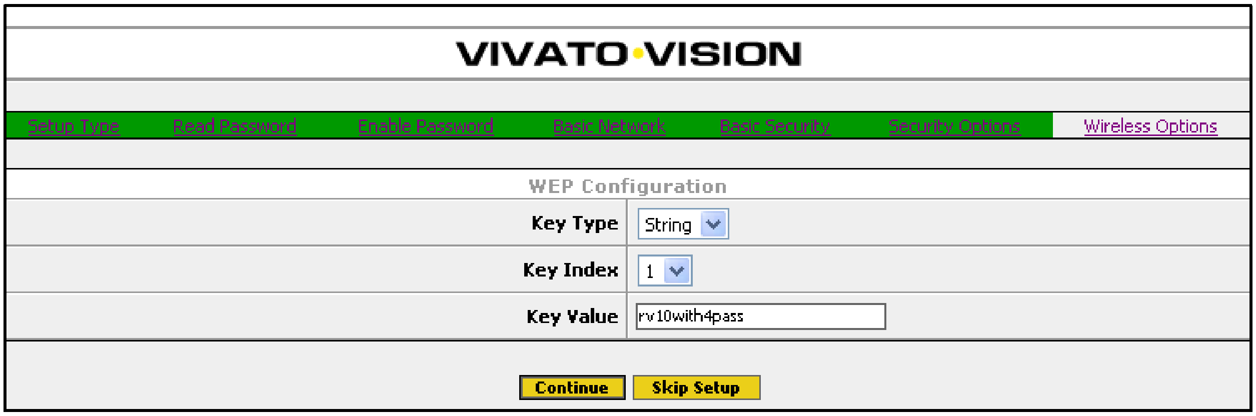
Please select your desired Security Options.

● No Security

○ WEP

Figure 26—Basic Security Setup Page

- **No Security**: This setting allows any wireless client to associate with the Wi-Fi Switch without using passwords, data encryption, or authentication. Unless you are providing open Wi-Fi operation to anyone who desires it, this setting is not recommended.
- **WEP**: Use wired equivalent privacy. When WEP is selected, clicking on **Continue** causes a WEP setup screen to be displayed (see below). Select the **Key Type** (String or Hex), the **Key Index** (up to four WEP keys can be defined), and enter the **Key Value** (valid entries are 5 or 13 String characters or 10 or 26 hex digits).



Key Type: String

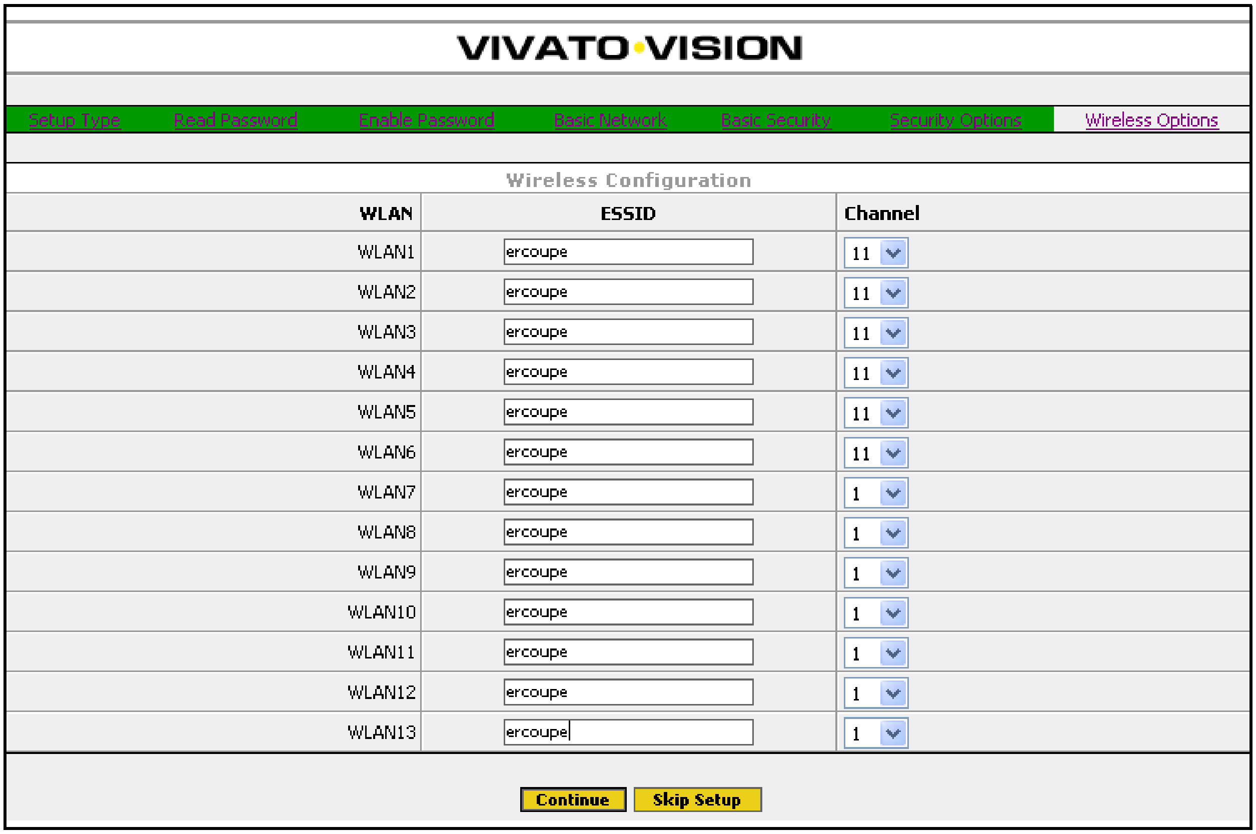
Key Index: 1

Key Value: rv10with4pass

Figure 27—WEP Security Configuration During Quick Setup

Wireless Options Setup

Wireless options specify the extended service set identifier (ESSID) that the Wi-Fi Switch uses to identify itself to 802.11b clients and the channel number for each of the 13 wireless interfaces.



Wireless Configuration

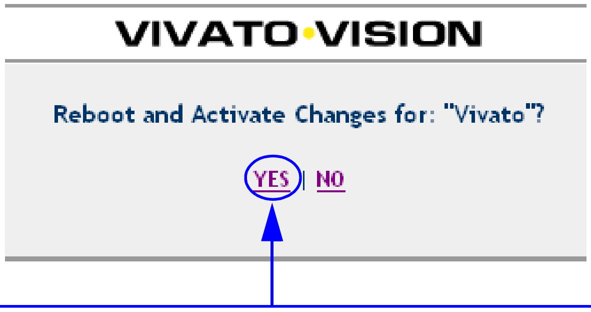
WLAN	ESSID	Channel
WLAN1	ercoupe	11
WLAN2	ercoupe	11
WLAN3	ercoupe	11
WLAN4	ercoupe	11
WLAN5	ercoupe	11
WLAN6	ercoupe	11
WLAN7	ercoupe	1
WLAN8	ercoupe	1
WLAN9	ercoupe	1
WLAN10	ercoupe	1
WLAN11	ercoupe	1
WLAN12	ercoupe	1
WLAN13	ercoupe	1

- **ESSID**: Enter the service set identifier for each of the 13 wireless interfaces. You can use the same ESSID for all interfaces, or use groups of interfaces with the same ESSID, depending on your needs. Keep in mind that each client typically has a list of preferred SSIDs, and that each of the Wi-Fi Switch's ESSIDs must be added to that list to be able to move from the area serviced by one ESSID to the an area serviced by a different ESSID without losing service indefinitely.
- **Channel**: Select the channel number to use for each wireless interface (wlan). See **"Wireless Interfaces"** on page 56 for information on assigning channel numbers.

Rebooting the Wi-Fi Switch

After entering your configuration information on all of the Quick Setup screens, you are prompted to reboot the Wi-Fi Switch. You must select “**Yes**” for your configuration to take effect. If you select “No”, your configuration is not saved.

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



Reboot and Activate Changes for: "Vivato"?

Select “Yes” to save your configuration and reboot the Wi-Fi Switch.

Where Do I Go From Here?

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

Using the Main Configuration Web Pages

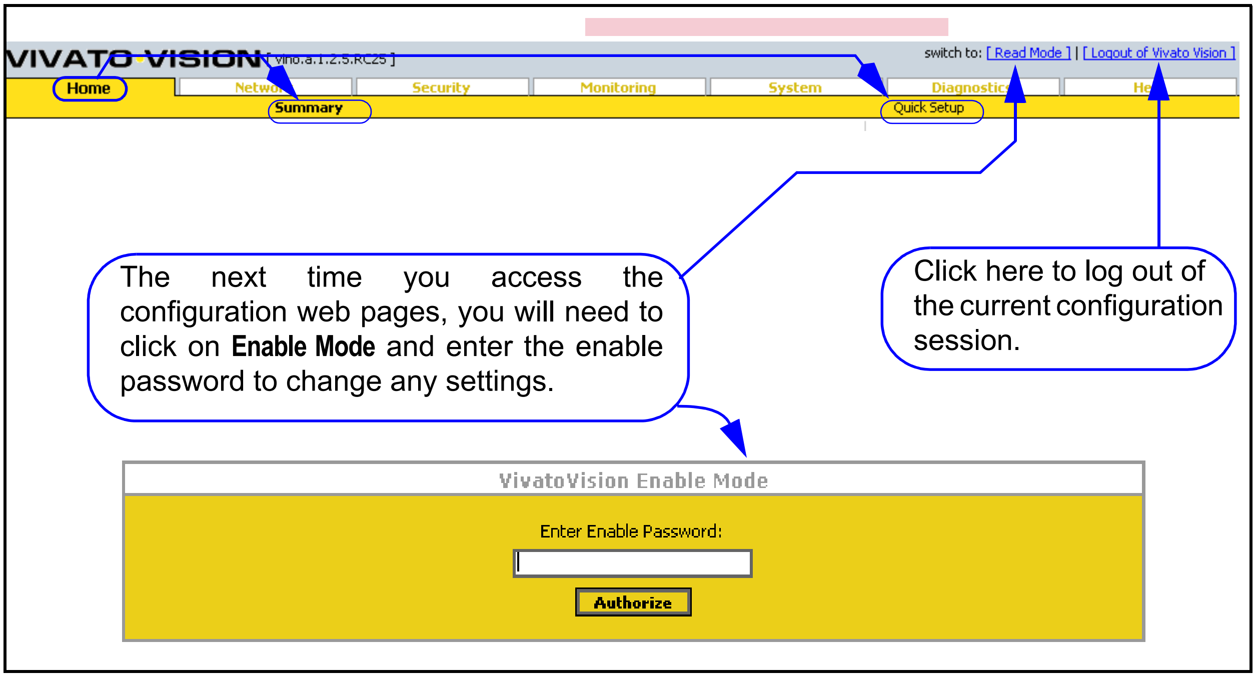
The Quick Setup screens are used to configure the Wi-Fi Switch for basic, secured Wi-Fi operation. All of the settings on the Quick Setup screens are also available on one of the main configuration pages.

Navigating the Main Web Page Configuration Screens

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

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

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



The next time you access the configuration web pages, you will need to click on **Enable Mode** and enter the enable password to change any settings.

Click here to log out of the current configuration session.

Figure 28—**Accessing Sub-Menus on the Home Configuration Screen**

Status Indicators

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

❗ indicates that the function is disabled.

✓ indicates that the function is enabled.

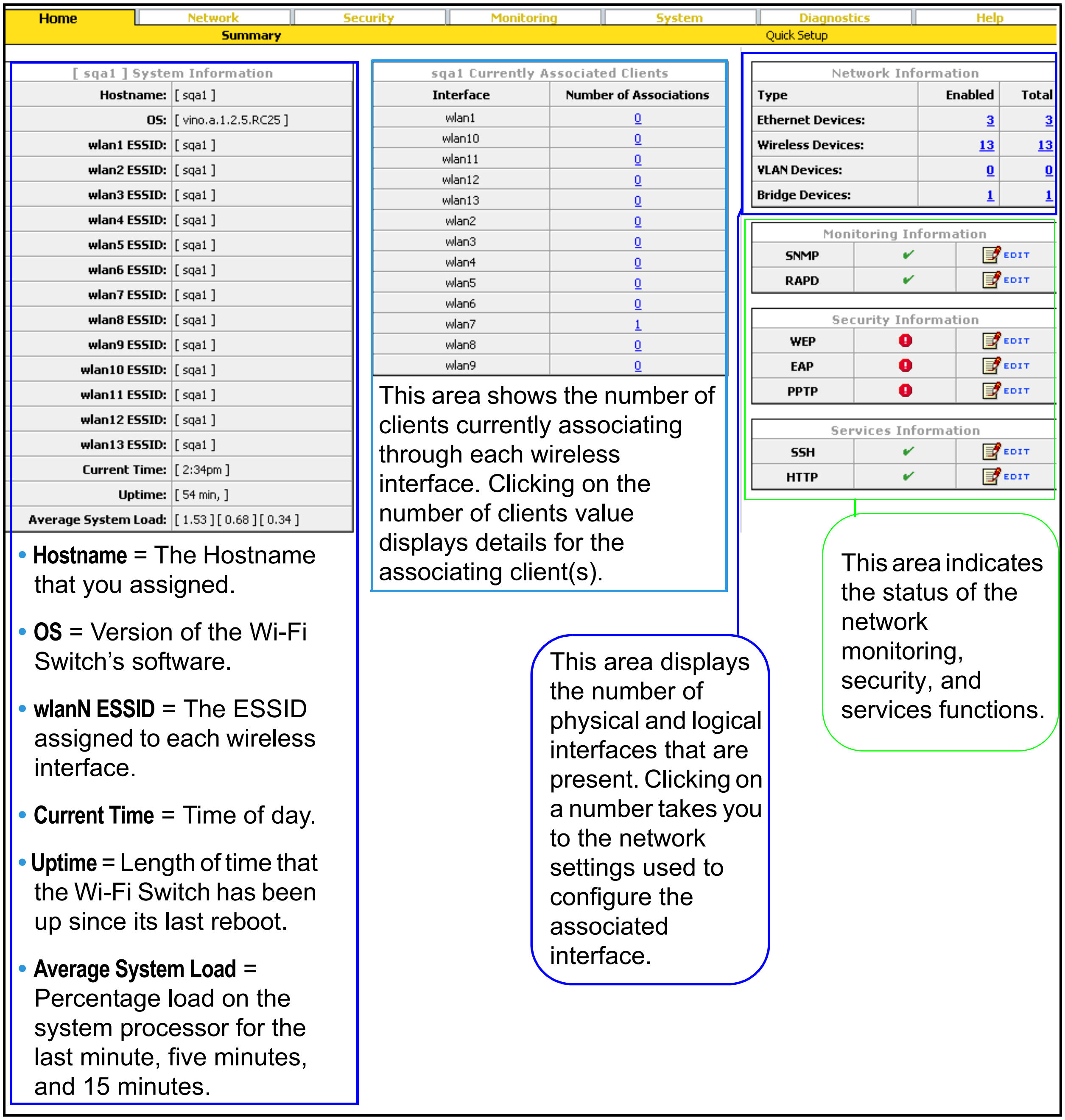
EDIT click to edit this setting.

Home

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

Summary

The Summary page displays an overview of Wi-Fi Switch hardware and system configuration.



[sqa1] System Information

Hostname:	[sqa1]
OS:	[vino.a.1.2.5.RC25]
wlan1 ESSID:	[sqa1]
wlan2 ESSID:	[sqa1]
wlan3 ESSID:	[sqa1]
wlan4 ESSID:	[sqa1]
wlan5 ESSID:	[sqa1]
wlan6 ESSID:	[sqa1]
wlan7 ESSID:	[sqa1]
wlan8 ESSID:	[sqa1]
wlan9 ESSID:	[sqa1]
wlan10 ESSID:	[sqa1]
wlan11 ESSID:	[sqa1]
wlan12 ESSID:	[sqa1]
wlan13 ESSID:	[sqa1]
Current Time:	[2:34pm]
Uptime:	[54 min,]
Average System Load:	[1.53] [0.68] [0.34]

sqa1 Currently Associated Clients

Interface	Number of Associations
wlan1	0
wlan10	0
wlan11	0
wlan12	0
wlan13	0
wlan2	0
wlan3	0
wlan4	0
wlan5	0
wlan6	0
wlan7	1
wlan8	0
wlan9	0

Network Information

Type	Enabled	Total
Ethernet Devices:	3	3
Wireless Devices:	13	13
VLAN Devices:	0	0
Bridge Devices:	1	1

Monitoring Information

SNMP	✓	EDIT
RAPD	✓	EDIT

Security Information

WEP	❗	EDIT
EAP	❗	EDIT
PPTP	❗	EDIT

Services Information

SSH	✓	EDIT
HTTP	✓	EDIT

- **Hostname** = The Hostname that you assigned.
- **OS** = Version of the Wi-Fi Switch's software.
- **wlanN ESSID** = The ESSID assigned to each wireless interface.
- **Current Time** = Time of day.
- **Uptime** = Length of time that the Wi-Fi Switch has been up since its last reboot.
- **Average System Load** = Percentage load on the system processor for the last minute, five minutes, and 15 minutes.

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

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

This area indicates the status of the network monitoring, security, and services functions.

Quick Setup

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

Network Configuration Web Pages

The **Network** tab accesses screens for configuring all of the physical and logical interfaces within the Wi-Fi Switch. Operations such as changing IP addresses and wireless interface channel numbers are easily accessed and changed.

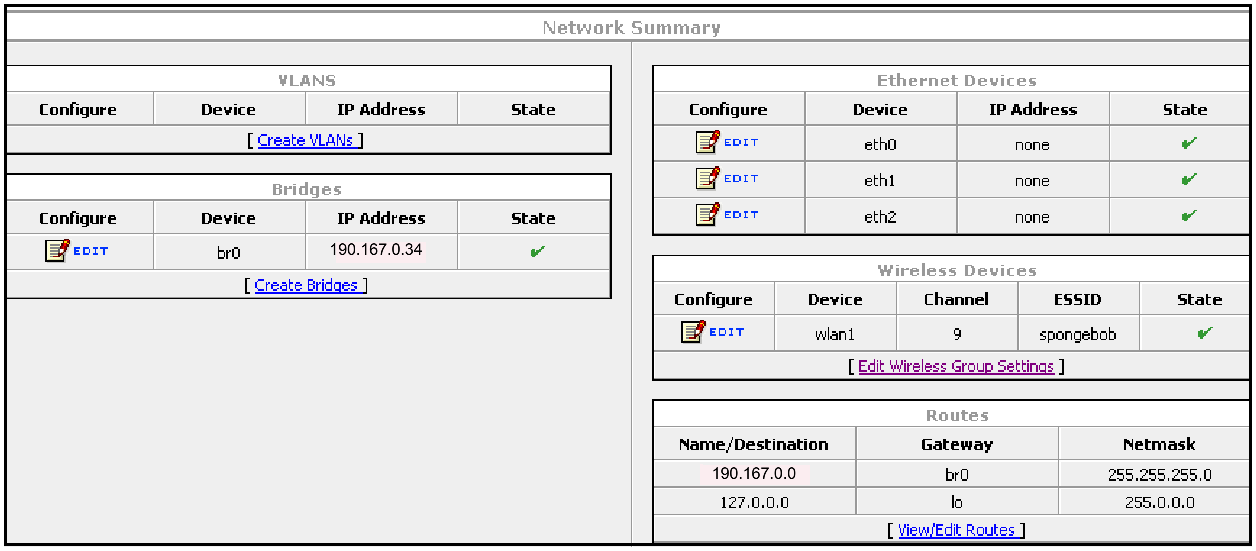
Network Settings

Network settings include the following physical and logical interfaces within the Wi-Fi Switch:

- **Ethernet Interfaces**
- **Wireless Interfaces**
- **Bridges**
- **VLANs**
- **Routes**

Summary

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



Network Summary

VLANS

Configure	Device	IP Address	State

[Create VLANs]

Bridges

Configure	Device	IP Address	State
EDIT	br0	190.167.0.34	✓

[Create Bridges]

Ethernet Devices

Configure	Device	IP Address	State
EDIT	eth0	none	✓
EDIT	eth1	none	✓
EDIT	eth2	none	✓

Wireless Devices

Configure	Device	Channel	ESSID	State
EDIT	wlan1	9	spongebob	✓

[Edit Wireless Group Settings]

Routes

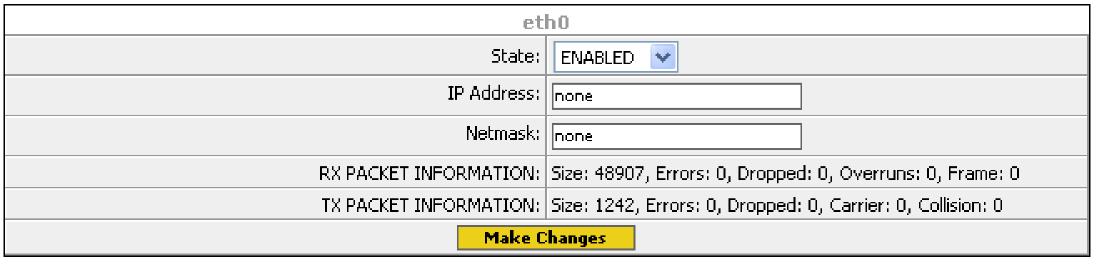
Name/Destination	Gateway	Netmask
190.167.0.0	br0	255.255.255.0
127.0.0.0	lo	255.0.0.0

[View/Edit Routes]

Ethernet Interfaces

The following settings are available for each wired Ethernet interface:

- **State**: Enable or Disable the interface.
- **IP Address**: Enter the IP address for that interface.
- **Netmask**: Enter the subnet mask for that interface.



eth0

State:	ENABLED
IP Address:	none
Netmask:	none
RX PACKET INFORMATION:	Size: 48907, Errors: 0, Dropped: 0, Overruns: 0, Frame: 0
TX PACKET INFORMATION:	Size: 1242, Errors: 0, Dropped: 0, Carrier: 0, Collision: 0

Figure 29—**Editing The Wired Interface Settings (Only eth0 is Shown)**

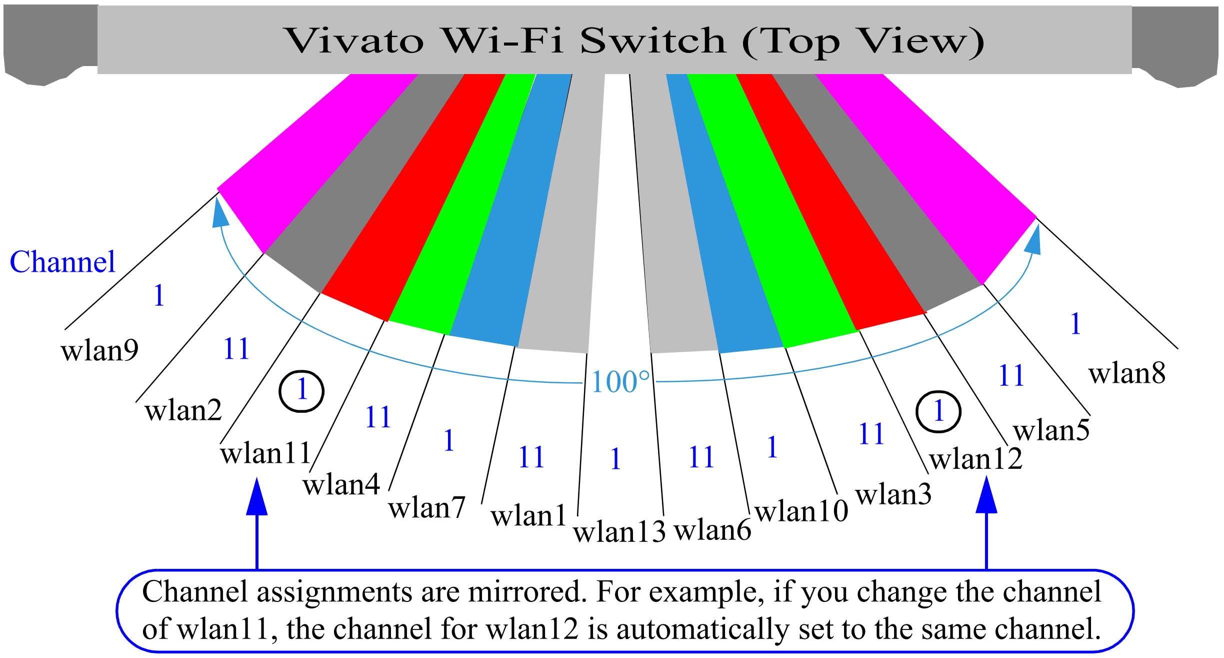
After editing settings, select **Make Changes** to put the changes into effect.

Wireless Interfaces

Unlike previous wireless LAN broadcasting, Vivato's Wi-Fi Switch uses a focused antenna pattern to point precisely at the desired client device. These narrow patterns of Wi-Fi enable up to three simultaneous Wi-Fi transmissions on three channels pointed in different directions. These narrow patterns also reduce co-channel interference, since they are powered only when needed.

The Wi-Fi Switch contains 13 signal processing wireless interfaces (wlan1 to wlan13) that can be individually configured or configured in groups to direct the antenna pattern. Each wireless interface transmits and receives signals within a specific area of the Wi-Fi Switch's pattern (see **Figure 30— Example Wi-Fi Switch Wireless Interface Assignments**). To provide simultaneous operation on two or three channels, the same ESSID is typically used for each wireless interface and the channel setting for each interface is configured as shown in **Figure 30— Example Wi-Fi Switch Wireless Interface Assignments**.

Important	Under most circumstances, the default channel assignments shown below should be used, especially when using the Wi-Fi Switch in areas of heavy Wi-Fi traffic. Channel 6 can be used to provide three channel operation (along with channels 1 and 11) when Wi-Fi traffic is light.



Channel assignments are mirrored. For example, if you change the channel of wlan11, the channel for wlan12 is automatically set to the same channel.

Table 1—Example Wireless Interface Configuration

Wireless Interface	ESSID	Channel
wlan1, wlan2, wlan3, wlan4, wlan5, wlan6	wifi_switch	11
wlan7, wlan8, wlan9, wlan10, wlan11, wlan12, wlan13	wifi_switch	1

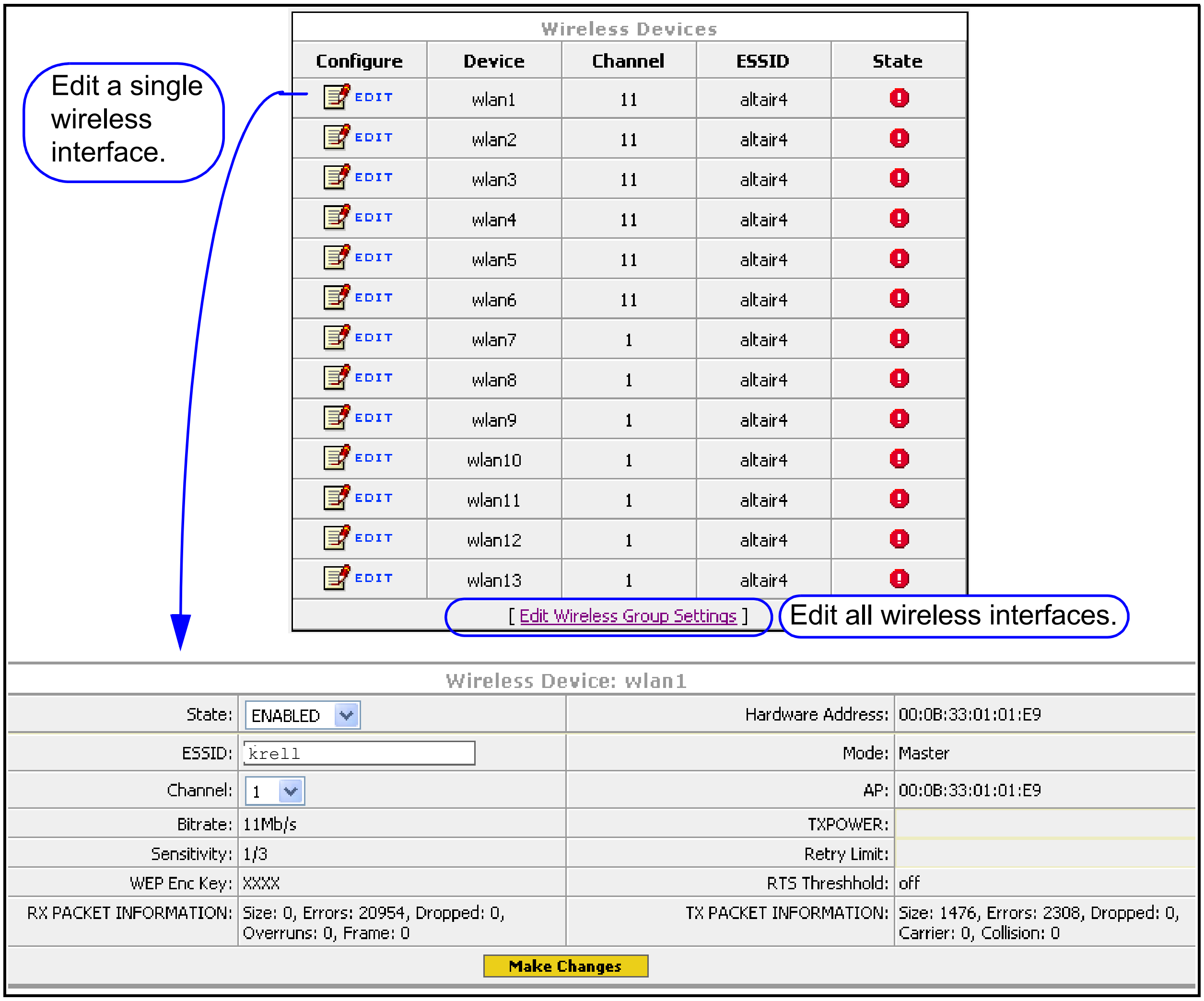
Figure 30—Example Wi-Fi Switch Wireless Interface Assignments

Using this configuration, a client moving within the area of the Wi-Fi Switch's antenna pattern will continue to see the same network name in its "Available Networks" window. At the same time, another client could be communicating simultaneously with the Wi-Fi Switch under the same network name but on a different channel.

Note: Wireless signals are reflected by solid objects, causing the focused antenna patterns to "bounce around" in enclosed areas. This is especially true in an office environment, where many objects tend to reflect the Wi-Fi Switch's signals in many directions. Therefore, the signal from a particular wireless interface that is not pointing directly at a client may still provide very good data rates to that client.

Configuring the Wireless Interfaces

You can configure each interface separately or configure all interfaces at one time. To edit a single interface's settings, click on the EDIT symbol next to that interface. To edit all wireless interfaces, select "**Edit Wireless Group Settings**".



Edit a single wireless interface.

Wireless Devices

Configure	Device	Channel	ESSID	State
EDIT	wlan1	11	altair4	●
EDIT	wlan2	11	altair4	●
EDIT	wlan3	11	altair4	●
EDIT	wlan4	11	altair4	●
EDIT	wlan5	11	altair4	●
EDIT	wlan6	11	altair4	●
EDIT	wlan7	1	altair4	●
EDIT	wlan8	1	altair4	●
EDIT	wlan9	1	altair4	●
EDIT	wlan10	1	altair4	●
EDIT	wlan11	1	altair4	●
EDIT	wlan12	1	altair4	●
EDIT	wlan13	1	altair4	●

[Edit Wireless Group Settings]

Edit all wireless interfaces.

Wireless Device: wlan1

State:	ENABLED	Hardware Address:	00:0B:33:01:01:E9
ESSID:	krell	Mode:	Master
Channel:	1	AP:	00:0B:33:01:01:E9
Bitrate:	11Mb/s	TXPOWER:	
Sensitivity:	1/3	Retry Limit:	
WEP Enc Key:	XXXX	RTS Threshhold:	off
RX PACKET INFORMATION:	Size: 0, Errors: 20954, Dropped: 0, Overruns: 0, Frame: 0	TX PACKET INFORMATION:	Size: 1476, Errors: 2308, Dropped: 0, Carrier: 0, Collision: 0

Figure 31—Wireless Interface’s Settings

Configuring a Single Interface

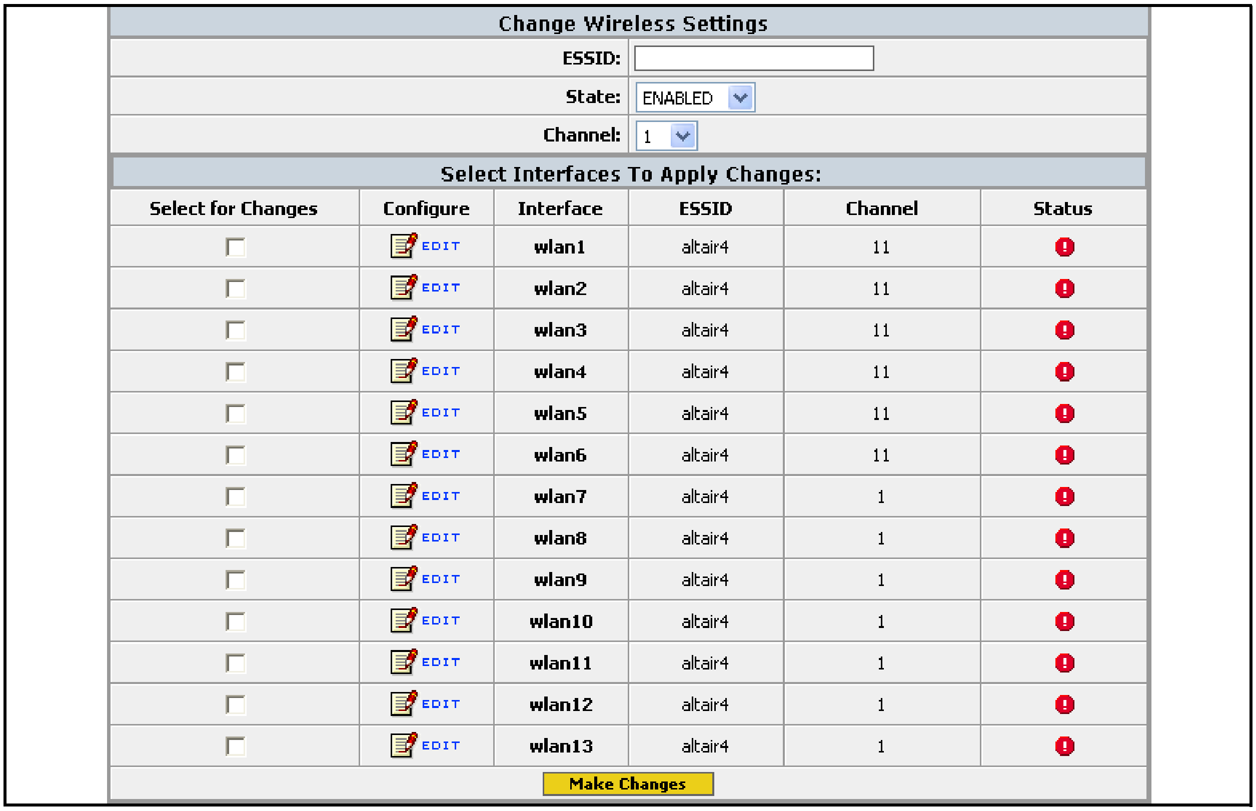
Each wireless interface contains the following configurable settings, as well as the hardware (MAC) address of that interface and some transmit and receive statistics (see Figure 31—Wireless Interface’s Settings):

- **State**: Enable or Disable the interface.
- **ESSID**: Enter the name that clients will see from this interface when searching for wireless networks.
- **Channel**: Select the channel to use for this wireless interface. Refer to "Example Wi-Fi Switch Wireless Interface Assignments" on page 57.

Configuring the Wireless Interfaces as a Group

The following settings are available when you choose to configure the wireless interfaces as a group:

- **ESSID**: The extended service set identifier is the name that the wireless interface uses to identify itself, and should usually be configured to the same value for all wireless interfaces. This is the name you see when your client lists available wireless networks. *This is NOT the same as the host name; the identifier for the Wi-Fi Switch that is used in your wired network.*
- **State**: Enable or Disable the interface.
- **Channel**: This is the channel number to use for that interface. For two channel operation, channels 1 and 11 should be used to prevent overlapping channels. Corresponding wireless interfaces are automatically "mirrored" when the channel for any wireless interface (other than 13) is changed. Refer to **"Example Wi-Fi Switch Wireless Interface Assignments"** on page 57.



Change Wireless Settings

ESSID:	
State:	ENABLED
Channel:	1

Select Interfaces To Apply Changes:

Select for Changes	Configure	Interface	ESSID	Channel	Status
□	EDIT	wlan1	altair4	11	●
□	EDIT	wlan2	altair4	11	●
□	EDIT	wlan3	altair4	11	●
□	EDIT	wlan4	altair4	11	●
□	EDIT	wlan5	altair4	11	●
□	EDIT	wlan6	altair4	11	●
□	EDIT	wlan7	altair4	1	●
□	EDIT	wlan8	altair4	1	●
□	EDIT	wlan9	altair4	1	●
□	EDIT	wlan10	altair4	1	●
□	EDIT	wlan11	altair4	1	●
□	EDIT	wlan12	altair4	1	●
□	EDIT	wlan13	altair4	1	●

Figure 32—Editing Wireless Interface Settings as a Group

Use the following steps to change a setting for one or more wireless interfaces.

1. Enter the changes for the ESSID, State, and Channel.
2. Click on the **Select for Changes** box for the interface(s) to configure using these changes.
3. Select **Make Changes**.

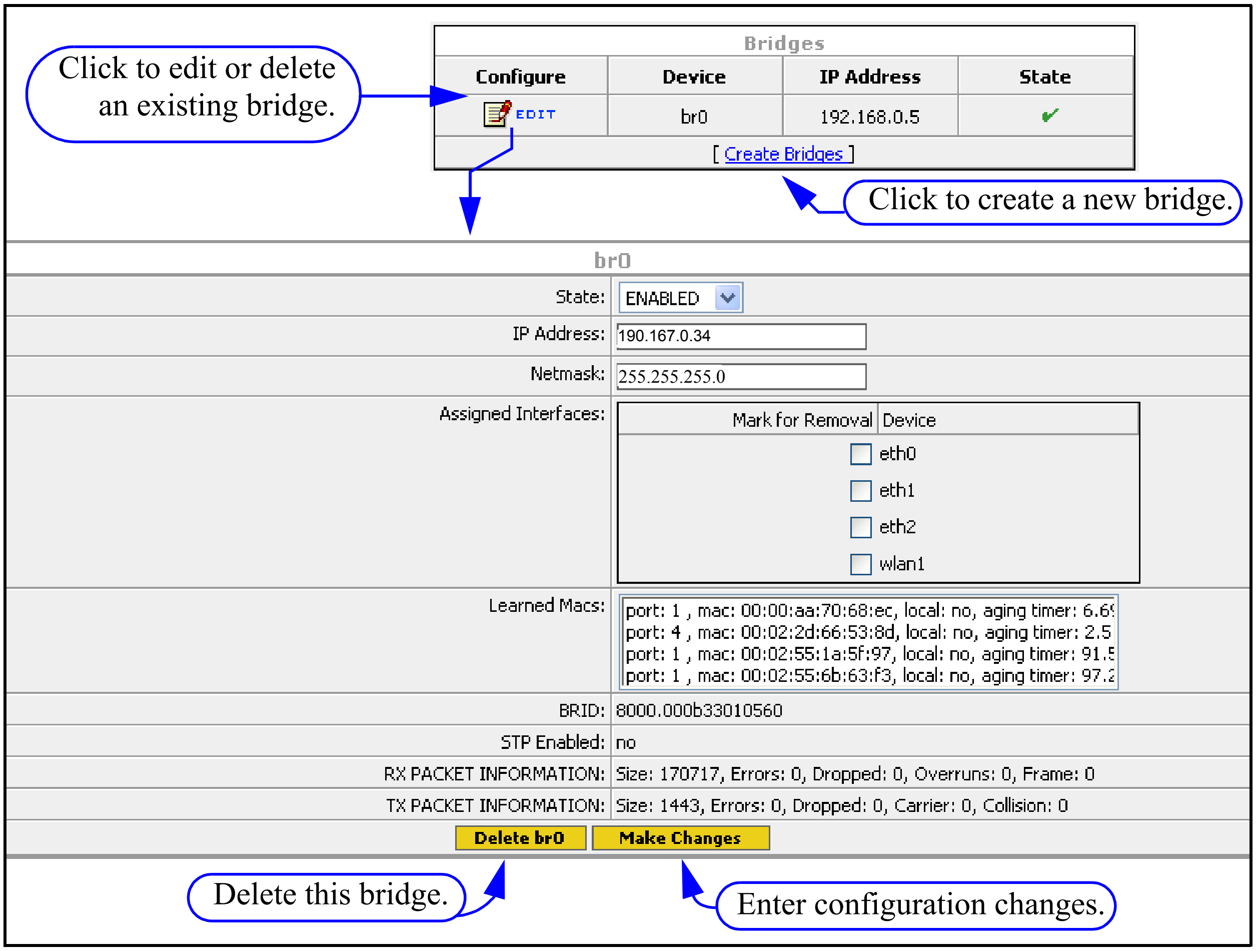
Bridges

Bridges create pathways for data packets to travel freely between two or more interfaces within the Wi-Fi Switch. Bridges differ from VLANs in that you do not have to specify the media access control (MAC) addresses of each client before it can use the bridge.

A default bridge, called “br0”, is configured to provide communications between the wired Ethernet interfaces (eth0-eth1) and the wireless interfaces (wlan1-wlan13). The default IP address of the Wi-Fi Switch is applied to this bridge for immediate access to these interfaces.

Editing an Existing Bridge

Clicking on EDIT displays a window to enable/disable the bridge, set the IP address and net mask, and remove existing interfaces on that bridge. The media access control (MAC) addresses of devices forwarding packets to that bridge are shown, as well as received and transmitted packet information.



Click to edit or delete an existing bridge.

Bridges

Configure	Device	IP Address	State
EDIT	br0	192.168.0.5	✓

[Create Bridges]

Click to create a new bridge.

br0

State:	ENABLED
IP Address:	190.167.0.34
Netmask:	255.255.255.0
Assigned Interfaces:	Mark for Removal / Device □ eth0 □ eth1 □ eth2 □ wlan1
Learned Macs:	port: 1 , mac: 00:00:aa:70:68:ec, local: no, aging timer: 6.6 port: 4 , mac: 00:02:2d:66:53:8d, local: no, aging timer: 2.5 port: 1 , mac: 00:02:55:1a:5f:97, local: no, aging timer: 91.5 port: 1 , mac: 00:02:55:6b:63:f3, local: no, aging timer: 97.2
BRID:	8000.000b33010560
STP Enabled:	no
RX PACKET INFORMATION:	Size: 170717, Errors: 0, Dropped: 0, Overruns: 0, Frame: 0
TX PACKET INFORMATION:	Size: 1443, Errors: 0, Dropped: 0, Carrier: 0, Collision: 0

Delete this bridge.

Enter configuration changes.

- **State**: Enable or Disable the bridge. Under normal operating conditions, you should always have bridge br0 enabled.

- **IP Address**: Enter the IP address of the bridge.
- **Netmask**: Enter the subnet mask for the bridge.
  - **Mark for Removal Device**: Click in the box corresponding to any interface that you want to remove from this bridge.
  - **Make Changes**: Configuration changes are not put into effect until you select this button.

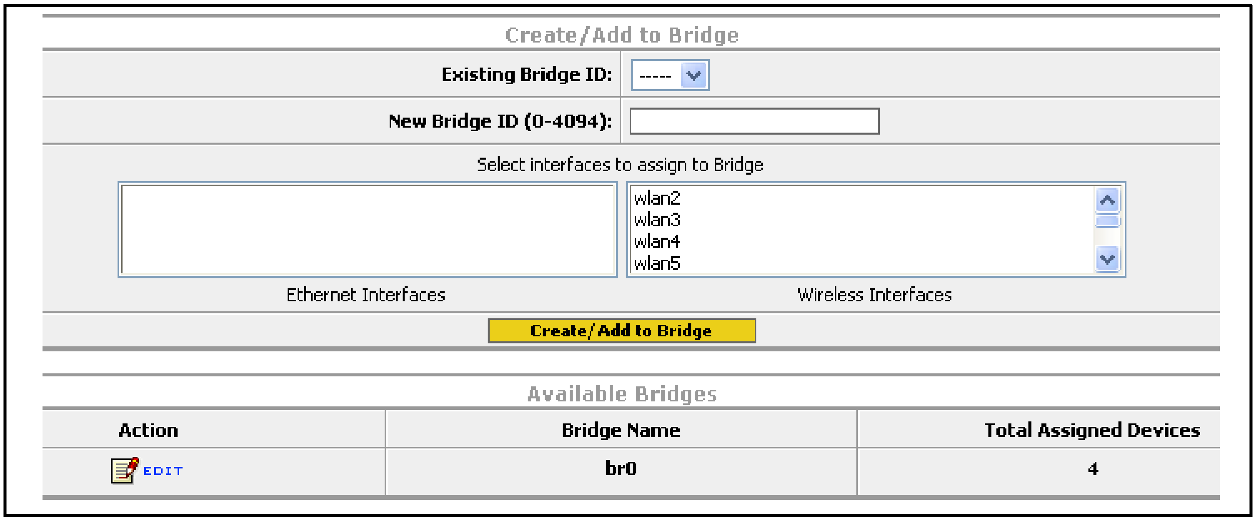
Caution ⚠ The IP address of the default bridge (br0) is used to access the Wi-Fi Switch for initial configuration. If you delete this bridge before assigning an IP address to a different bridge, VLAN, or Ethernet interface, you will lose connection to the Wi-Fi Switch when the bridge is deleted and you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

Creating a New Bridge

You can create a new bridge, or add interfaces to an existing bridge, by selecting **Create Bridges** from the **Network**>**Summary** page.

To create a new bridge, enter the **New Bridge ID** value and select the desired interfaces to include on that bridge. To add an interface to an existing bridge, select the **Existing Bridge ID** and the desired interface(s) to add. To select more than one interface at a time, hold down the **Ctrl** key while selecting the interfaces. Select **Create/Add to Bridge** to put the changes into effect.

Important ❗ An interface can only be used on one bridge; it cannot be "shared" by another bridge. Therefore, any interfaces that are already assigned to an existing bridge are not displayed when you try to create a new bridge. Since the default bridge, br0, includes all of the interfaces, you must delete two or more interfaces from the default bridge before another bridge can be created.



Create/Add to Bridge

Existing Bridge ID:	-----
New Bridge ID (0-4094):	

Select interfaces to assign to Bridge

Ethernet Interfaces	Wireless Interfaces
	wlan2 wlan3 wlan4 wlan5

Available Bridges

Action	Bridge Name	Total Assigned Devices
EDIT	br0	4

VLANs

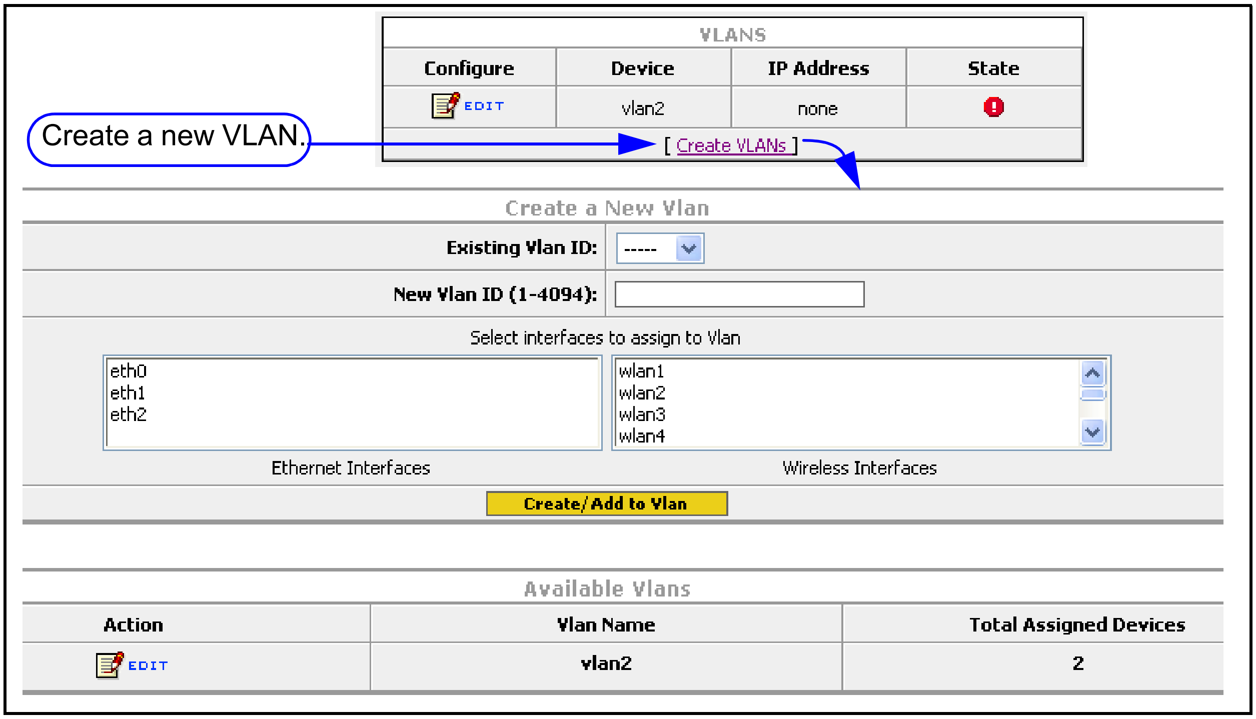
Virtual local area networks (VLANs) are groups of devices configured to work efficiently with each other. The device may be a client, server, or any device with a MAC address that needs to send and receive packets with other devices on a VLAN.

Special tags are added to the packets of devices assigned to a VLAN to indicate its association with that VLAN. Each device on the VLAN is also identified by its media access control (MAC) address, and only packets containing a MAC address that has been assigned to that VLAN are forwarded through the VLAN to their destination.

Creating a New VLAN

To create a new VLAN, or add interfaces to an existing VLAN, go to the **Network**>**Summary** page and select **Create VLANs**. The following selections are displayed:

- **Existing Vlan ID**: Select an existing VLAN to add interfaces to it.
- **New Vlan ID (1-4094)**: Enter a number in the displayed range to create a new VLAN.
- **Select interfaces to assign to Vlan**: Hold the **Cntrl** key down and select the interfaces to add to the VLAN.
- **Create/Add to Vlan**: Put your changes into effect.



VLANS

Configure	Device	IP Address	State
EDIT	vlan2	none	●

Create a New Vlan

Existing Vlan ID:	-----
New Vlan ID (1-4094):	

Select interfaces to assign to Vlan

Ethernet Interfaces	Wireless Interfaces
eth0 eth1 eth2	wlan1 wlan2 wlan3 wlan4

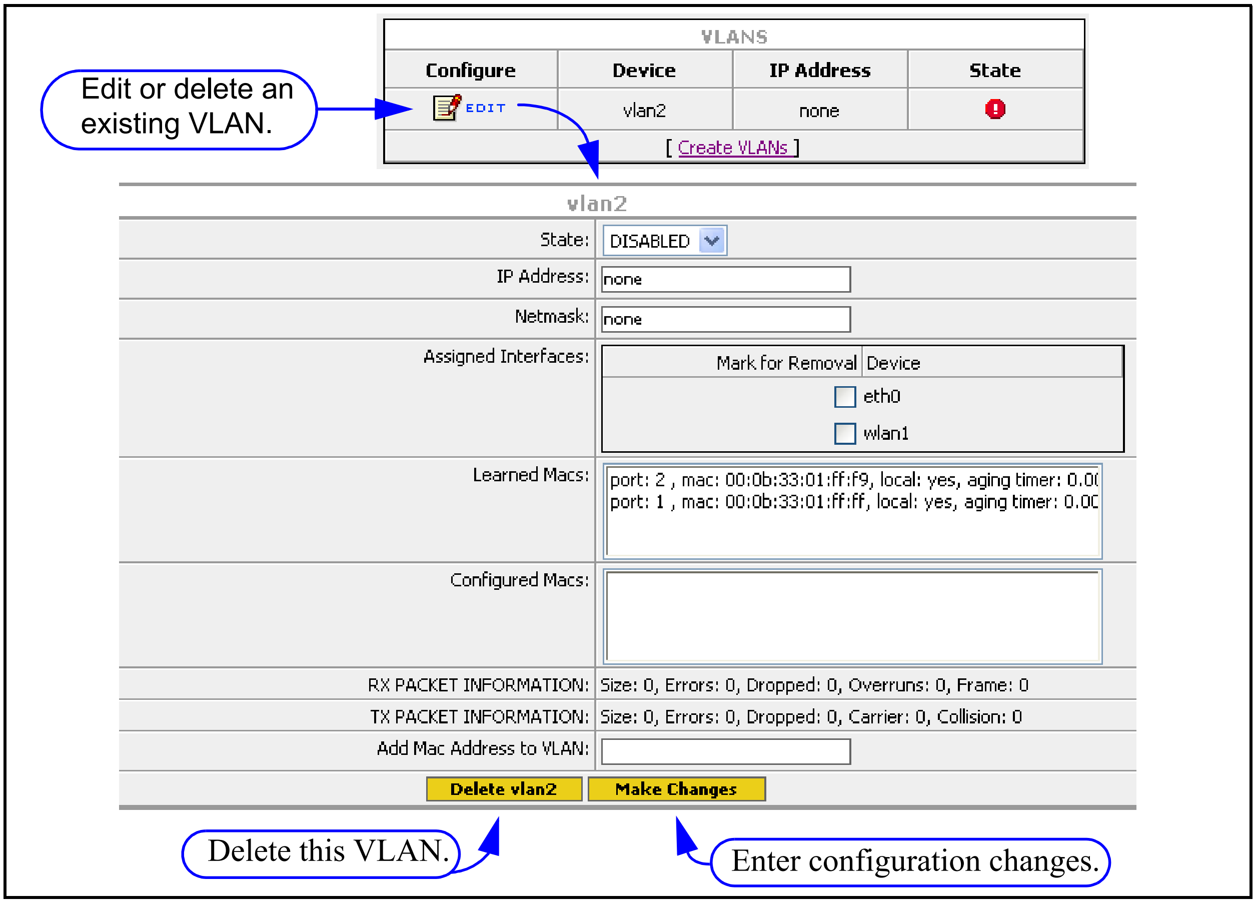
Available Vlans

Action	Vlan Name	Total Assigned Devices
EDIT	vlan2	2

Editing an Existing VLAN

To delete a VLAN or edit an existing VLAN configuration, or add a MAC address to a VLAN, go to the **Network**>**Summary** page and select EDIT for the desired VLAN. The following selections are displayed:

- **State**: Enable or disable this VLAN.
- **IP Address**: If desired, enter the IP address for the VLAN.
- **Netmask**: Enter a subnet mask for the VLAN (if an IP address was specified).
- **Mark for Removal**: Select interface(s) to remove from an existing VLAN.
- **Learned Macs**: This area lists the MAC addresses of Wi-Fi Switch's interfaces that are part of the VLAN, and the MAC address of any device that a client/device assigned to the VLAN used to access the VLAN. The "local: yes/no" entry specifies whether that MAC address is for an interface inside the Wi-Fi Switch (local) or is for another device outside the Wi-Fi Switch (remote).
- **Configured Macs**: This area lists the MAC addresses of clients/devices that have been individually added to the VLAN.
- **Add Mac Address to VLAN**: Enter the MAC address of a device to enter it into the VLAN's list of configured MAC addresses. This allows packets from that device to travel through this VLAN. The MAC is added to the list when you select **Make Changes**.
- **Delete Vlan**: Delete the specified VLAN.
- **Make Changes**: Put your changes into effect.



Edit or delete an existing VLAN.

VLANS

Configure	Device	IP Address	State
EDIT	vlan2	none	●

[Create VLANs]

vlan2

State:	DISABLED
IP Address:	none
Netmask:	none
Assigned Interfaces:	Mark for Removal / Device □ eth0 □ wlan1
Learned Macs:	port: 2 , mac: 00:0b:33:01:ff:f9, local: yes, aging timer: 0.0(port: 1 , mac: 00:0b:33:01:ff:ff, local: yes, aging timer: 0.0C
Configured Macs:	
RX PACKET INFORMATION:	Size: 0, Errors: 0, Dropped: 0, Overruns: 0, Frame: 0
TX PACKET INFORMATION:	Size: 0, Errors: 0, Dropped: 0, Carrier: 0, Collision: 0
Add Mac Address to VLAN:	

Delete this VLAN.

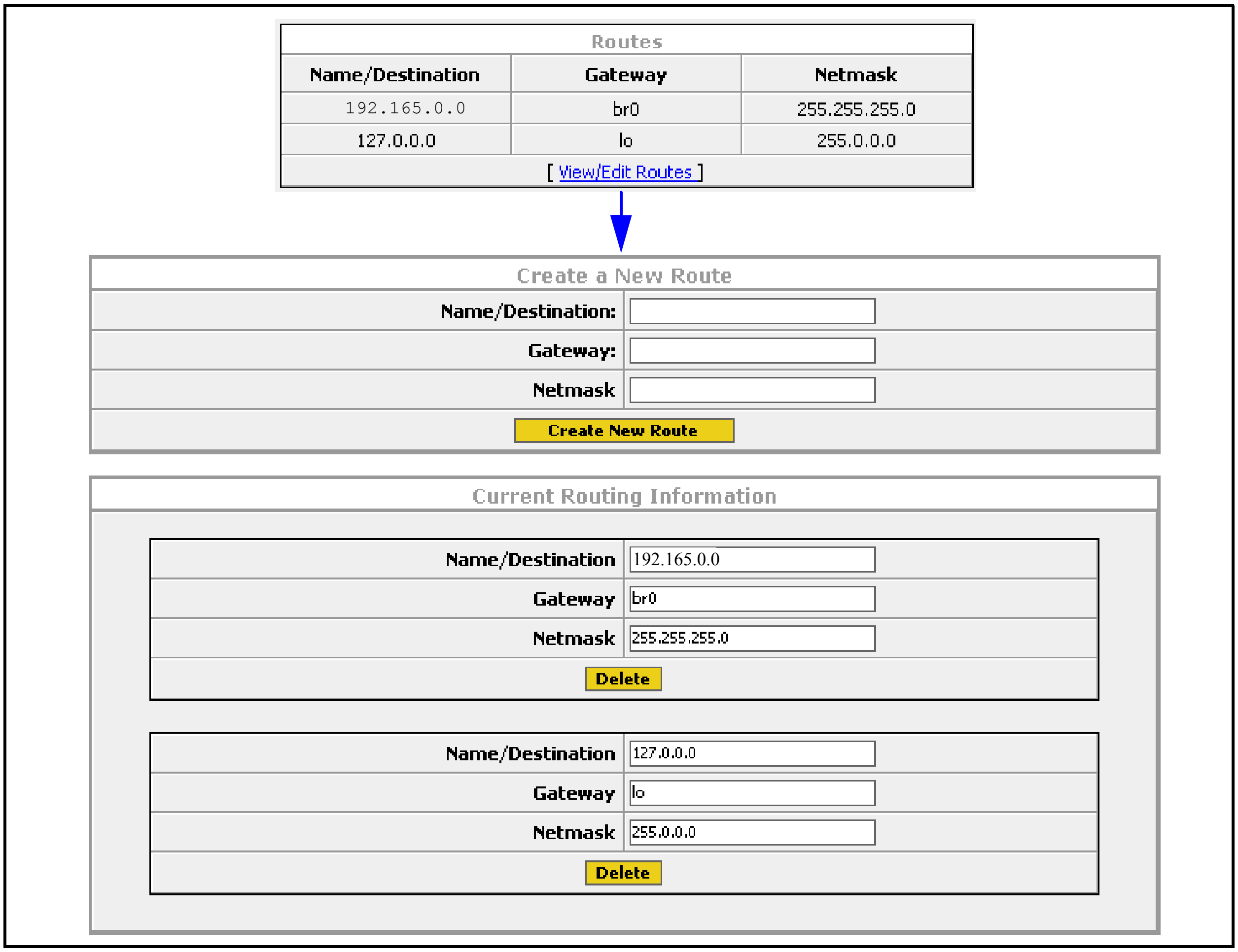
Enter configuration changes.

Routes

The **Network>Routes** settings indicate how packets within a specified IP address range are directed (routed).

- **Name/Destination**: Enter the host name or base IP address of the destination to which you are trying to connect.
- **Gateway**: Enter the IP address of the gateway used to access addresses on the destination subnet.
- **Netmask**: Enter the subnet mask that defines the range of IP addresses allowed to use this route.

In the Current Routing Information example below, all packets addressed to the 192.165.0.0 base IP address that are within the Netmask of 255.255.255.0 are routed through the specified Gateway - br0. *The 127.0.0.0 route is a loopback path used by the Wi-Fi Switch's host, and should not be modified.*



Routes

Name/Destination	Gateway	Netmask
192.165.0.0	br0	255.255.255.0
127.0.0.0	lo	255.0.0.0

[View/Edit Routes]

Create a New Route

Name/Destination:	
Gateway:	
Netmask	

Current Routing Information

Name/Destination	192.165.0.0
Gateway	br0
Netmask	255.255.255.0

Name/Destination	127.0.0.0
Gateway	lo
Netmask	255.0.0.0

Security Configuration Web Pages

The **Security** tab accesses screens for configuring the various security features in the Wi-Fi Switch, such as WEP, EAP, and PPTP.

Configuring Security

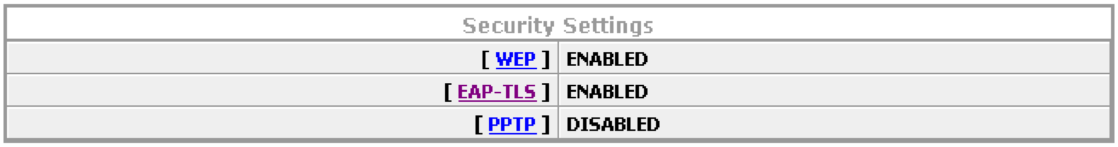
Security settings determine who is allowed network access through the Vivato Wi-Fi Switch. Security is initially turned off in the Wi-Fi Switch to allow access for configuration. Security should be configured when you access the configuration web pages for the first time and select the security method in the Quick Setup screens.

For more information on configuring Microsoft® Windows® XP clients and a Windows 2000® Internet Access Server (Win2K IAS) for EAP or PEAP security, see ***Windows XP Win2kIAS Deployment.pdf*** on the Vivato 2.4 GHz Wi-Fi Switch CD-ROM.

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

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

To view and edit the security settings at another time click on the **Security** tab.



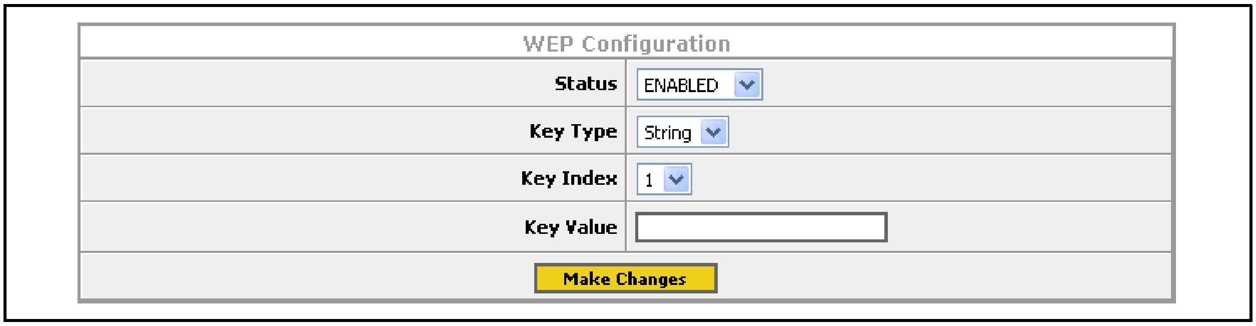
Security Settings	
[WEP]	ENABLED
[EAP-TLS]	ENABLED
[PPTP]	DISABLED

Settings are arranged in the following sub-menus:

- **Wired Equivalent Privacy (WEP)**
- **EAP** (802.1x)
- **Point to Point Tunneling Protocol (PPTP)**

Wired Equivalent Privacy (WEP)

WEP is a method of data encryption for wireless networks, originally developed to provide approximately the same level of security provided by wired networks. Data encryption keys are shared between the Wi-Fi Switch and the wireless clients to try to provide a secure link between them.



WEP Configuration

Status	ENABLED
Key Type	String
Key Index	1
Key Value	

WEP has been shown to be somewhat susceptible to wireless interception and fraud by those skilled at breaking into networks. Where needed, use EAP or PPTP to provide greater levels of security. See **"EAP"** on page 69 and **"Point to Point Tunneling Protocol (PPTP)"** on page 72.

WEP configuration includes the following settings:

- **Status**: Select enabled or disabled to turn WEP on or off, respectively.
- **Key Type**: Select the character type for the WEP key: String (ASCII) or HEX.
- **Key Index**: Up to four WEP keys can be configured. The key index represents which key value you are using. The key indexes and the key values for clients must match those of the Wi-Fi Switch.

  Note: In most client's configuration settings, the WEP key index ranges from 1 to 4; just like the Wi-Fi Switch. However, some clients use indexes from 0 to 3 instead. In this case, use the key index of the same relative order when configuring your client. For example; if the Wi-Fi Switch is set to use a key index of 1, set your client to use a key index of 0, and so on.

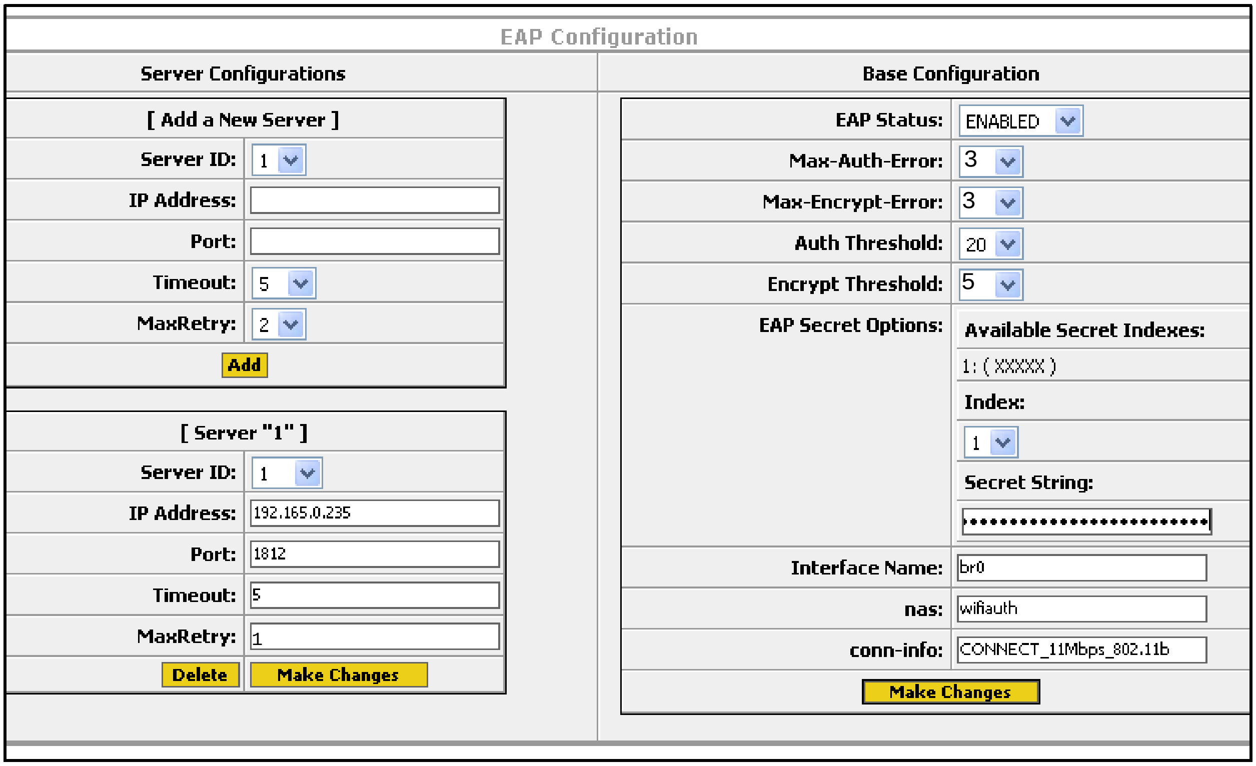
- **Key Value**: Enter the WEP key value. Valid entries are 5 or 13 String (ASCII) characters or 10 or 26 hex digits.
- **Make Changes**: Change the Wi-Fi Switch's configuration to use the specified key value on the specified interface.

EAP

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

For information on configuring the Windows 2000 Internet Access Server to work with the Vivato Wi-Fi Switch's EAP configuration, see **"Configure EAP Commands"** on page 120.

Caution When EAP is enabled, WEP is automatically enabled because it is used by EAP. Therefore, do not disable WEP when using EAP.



EAP Configuration

Server Configurations

[Add a New Server]	
Server ID:	1
IP Address:	
Port:	
Timeout:	5
MaxRetry:	2

[Server "1"]	
Server ID:	1
IP Address:	192.165.0.235
Port:	1812
Timeout:	5
MaxRetry:	1

Base Configuration

EAP Status:	ENABLED
Max-Auth-Error:	3
Max-Encrypt-Error:	3
Auth Threshold:	20
Encrypt Threshold:	5
EAP Secret Options:	Available Secret Indexes: 1: (XXXXX) Index: 1 Secret String: ••••••••••••••••••••••••••
Interface Name:	br0
nas:	wifiauth
conn-info:	CONNECT_11Mbps_802.11b

Adding a New Authentication Server

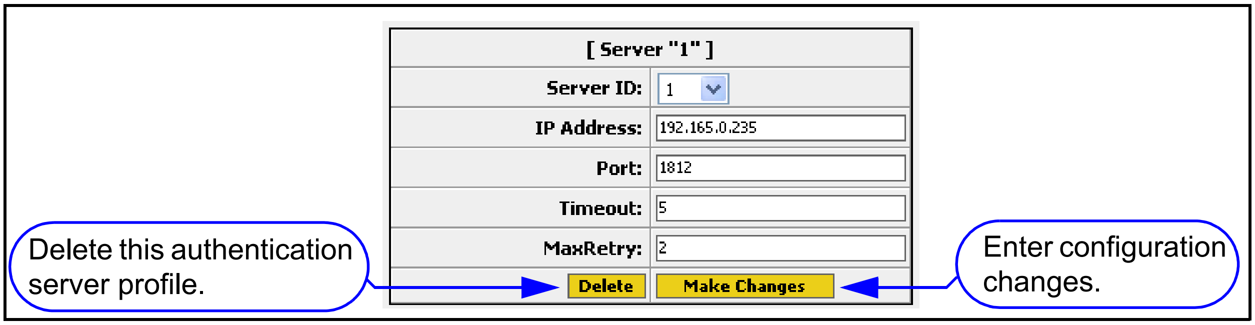
These settings are used to add available authentication servers:

- **Server ID**: Enter an identifier to assign to this RADIUS server. Up to four (4) authentication servers can be specified, in order of preference, with "1" being the preferred available server.
- **IP Address**: Enter the IP address of the RADIUS server.
- **Port**: Enter the port number for the RADIUS server.

- **Timeout**: Enter the maximum number of seconds to wait for a reply from the RADIUS server after an authentication request is sent.
- **MaxRetry**: 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. The default is 1.
- **Add**: Click to add this server to the list of available servers.

Editing or Deleting an Authentication Server

After an authentication server has been configured, you can change its settings and click on **Make Changes** to put those changes into effect. You can also click on **Delete** to remove that authentication server's configuration.



[Server "1"]

Server ID:	1
IP Address:	192.165.0.235
Port:	1812
Timeout:	5
MaxRetry:	2

Delete this authentication server profile.

Enter configuration changes.

Base Configuration

These settings are used to specify EAP operating conditions and devices:

- **EAP Status**: Select **Enabled** or **Disabled** to turn EAP on or off when you select **Make Changes**.
- **Max-Auth-Error**: 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. A typical value is 3.
- **Max-Encrypt-Error**: Enter the maximum number of encryption errors from the client that are allowed during the time specified in **Auth Threshold** before an authentication failure is reported. A typical value is 3.
- **Auth Threshold**: The amount of time, in minutes, used to measure client authentication errors for the **Max-Encrypt-Error** command. The value must be in the range of 1 to 60; a typical value is 20.
- **Encrypt Threshold**: Enter the length of time, in minutes, that the **Max-Encrypt-Error** command uses to measure encryption errors in packets before disassociating the client from the Wi-Fi Switch. The value must be in the range of 1 to 10; a typical value is 5.

- **Index**: Up to four (4) authentication servers can be specified, in order of preference, with “1” being the preferred server if available. Enter the index corresponding to the **Server ID** value entered for the desired server.
- **Secret String**: Enter the secret string value the range of 22 to 255 bytes. At this time, the Secret can only be entered using the command line interface (CLI).
- **Interface Name**: Enter the name of the interface used to access the RADIUS authentication server, such as br0 or eth0.
- **nas**: Enter the network access device name. This is the name of the switch defined as the RADIUS server client for authentication.
- **conn-info**: 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.

Important Considerations When Using EAP

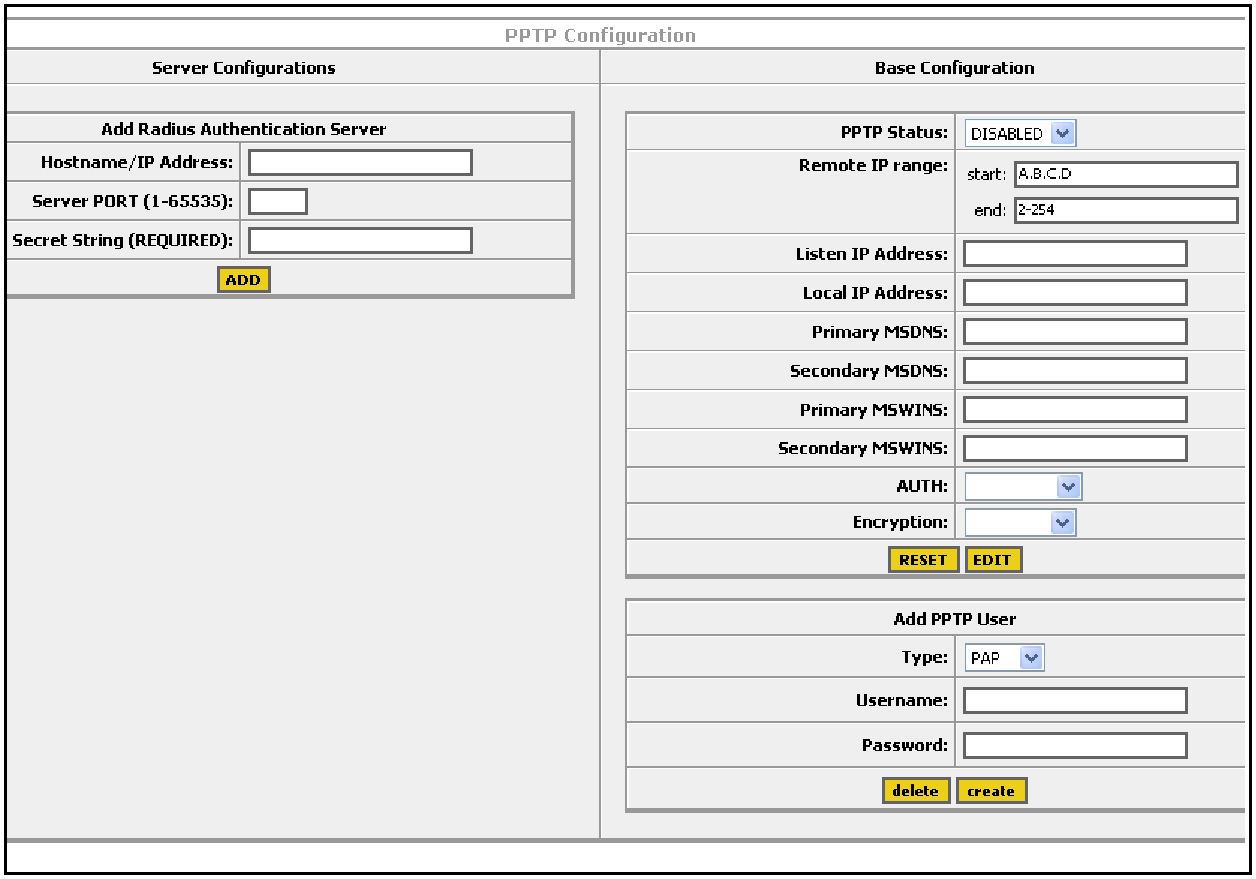
The following conditions must be considered when configuring EAP in the Wi-Fi Switch, clients, and the services supporting EAP.

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

Point to Point Tunneling Protocol (PPTP)

PPTP is used to provide security between a wireless client and the Wi-Fi Switch. The Wi-Fi Switch supports challenge handshake authentication protocol (CHAPv2, MS-CHAP, MS-CHAPV2) and password authentication protocol (PAP) encryption formats.

For a description of PPTP operation, see **"Point to Point Tunneling Protocol (PPTP) Operation"** on page 165.



PPTP Configuration

Server Configurations

Add Radius Authentication Server

Hostname/IP Address:

Server PORT (1-65535):

Secret String (REQUIRED):

Base Configuration

PPTP Status: DISABLED

Remote IP range: start: A.B.C.D end: 2-254

Listen IP Address:

Local IP Address:

Primary MSDNS:

Secondary MSDNS:

Primary MSWINS:

Secondary MSWINS:

AUTH:

Encryption:

Add PPTP User

Type: PAP

Username:

Password:

Base Configuration

The following settings are used with all PPTP connections:

- **PPTP Status**: Select enable or disable to turn PPTP on or off.
- **Remote IP range**: Using a start and a stop IP address, define the range of IP addresses to assign to wireless clients using PPTP .
- **Listen IP address**: This is the address that the PPTP daemon process listens on for new client connections. This address can either be associated with a bridge or with a VLAN. However, to use the default bridge (br0), you must assign a secondary IP address to that bridge and use that IP address as the listen address.

- **Local IP address**: Enter the IP address within the Wi-Fi switch that wireless clients will connect to for backhaul access. This is the same IP address that devices on the Wi-Fi Switch's backhaul use to access the Wi-Fi Switch. Unless a VLAN or another bridge is created for PPTP operation and given an IP address, this is the IP address that is associated with the default bridge, br0.
- **Primary MSDNS**: Enter the IP address for the primary Microsoft® domain name service (DNS) server.
- **Secondary MSDNS**: Enter the IP address for a secondary Microsoft® domain name service (DNS) server
- **Primary MSWINS**: Enter the IP address of the primary Microsoft Windows Internet Naming Service (MS-WINS) server to use when a server name is used when specifying a radius authentication server.
- **Secondary MSWINS**: Enter the IP address of the secondary Microsoft Windows Internet Naming Service (MS-WINS) server to use when a server name is used when specifying a radius authentication server.
- **AUTH**: Select the type of authentication to use from the drop down menu: PAP, CHAP, RADIUS, MS-CHAP, MS-CHAPv2.
- **Encryption**: Select the encryption format to use from the drop down menu: mppe-40, mppe-128.

Add a PPTP User

These settings are used to add a user when PAP or CHAP authentication is used.

- **Password**: Enter the password for the specified user name.
- **Type**: Select the type of authentication to use for the specified user name: PAP or CHAP.
- **Username**: Enter the user name to add to allow access using PPTP.

Add A RADIUS Authentication Server

These settings are used to specify a RADIUS server to use for authenticating clients using PPTP:

- **Hostname/IP Address**: Enter the host name or IP address of the RADIUS server.
- **Server Port (1-65535)**: Enter the port number on the RADIUS server used for PPTP client authentication.
- **Secret String**: Enter the secret string used to authenticate users through the RADIUS server.

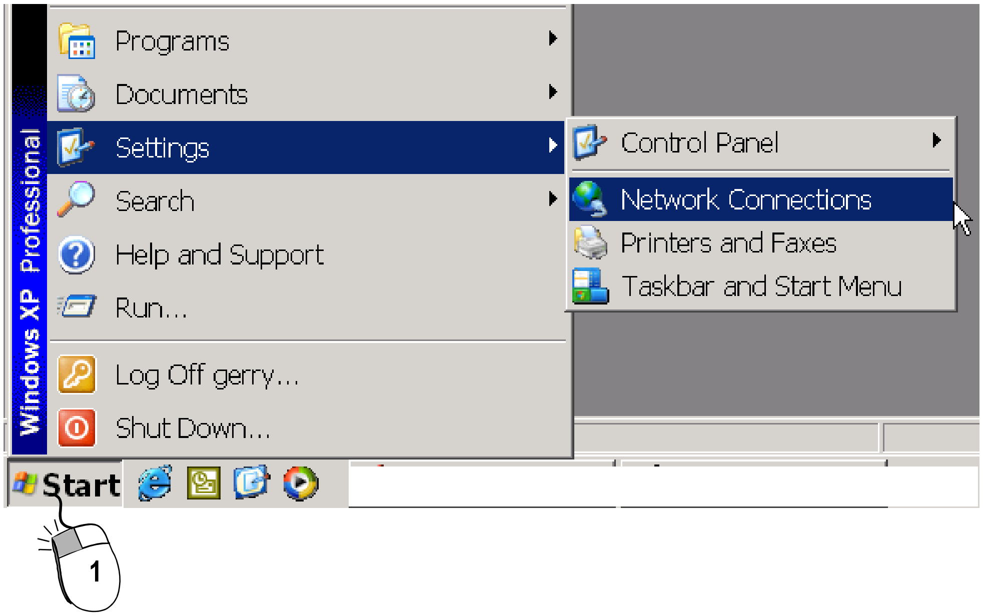
Optimizing Your Wireless Client For Secure Communications

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

For information on using PPTP to provide a virtual private network (VPN) tunnel, see **"Point to Point Tunneling Protocol (PPTP) Operation"** on page 165.

The examples below use the Microsoft Windows XP® Network Connections feature to access and change the client configuration. *The client interface must be enabled, and the Wi-Fi Switch's Wireless interface must be enabled, to be able to access the client's security settings.*

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



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

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

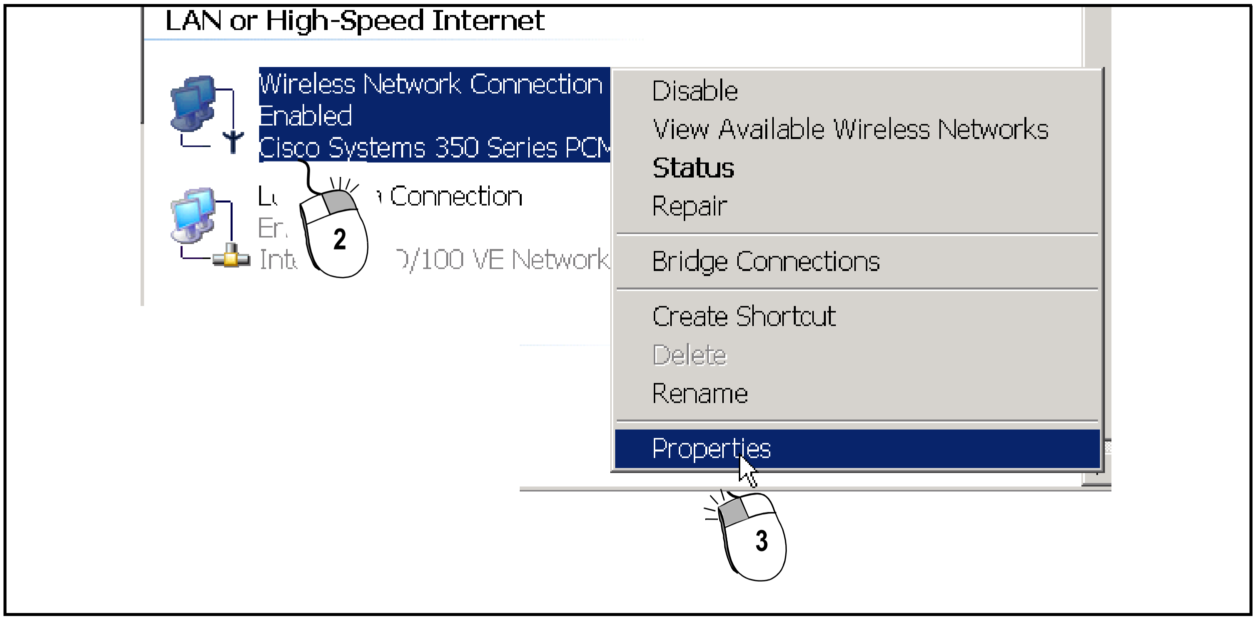
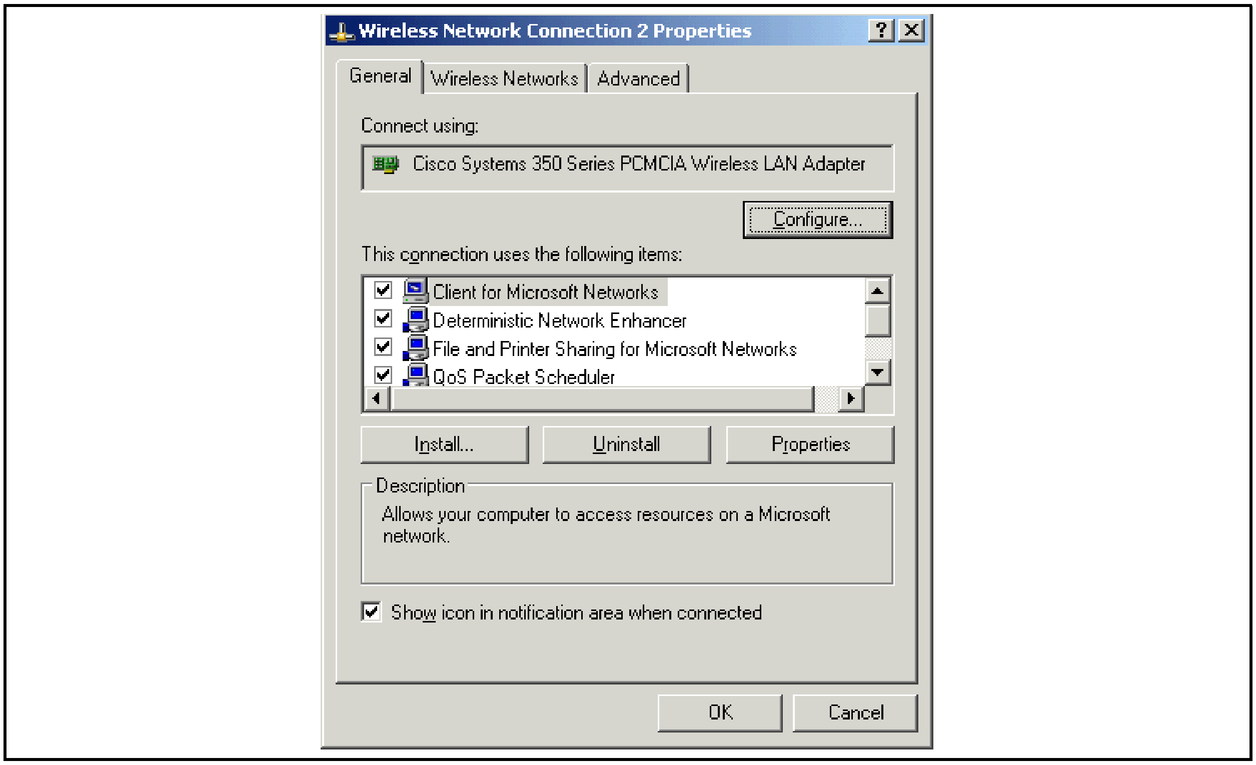


Figure 33—Accessing the Wireless Network Connections Configuration



Wireless Network Connection 2 Properties

General | Wireless Networks | Advanced

Connect using:

Cisco Systems 350 Series PCMCIA Wireless LAN Adapter

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ Deterministic Network Enhancer
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler

Install... | Uninstall | Properties

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

OK | Cancel

Figure 34—Windows XP Wireless Network Connections Screen (With the Client Enabled)

Configuring WEP in Your Client

See **"Wired Equivalent Privacy (WEP)"** on page 68 for a description of WEP.

With the *client enabled* and close enough to the Wi-Fi Switch to receive its wireless signal, use the following steps to configure WEP.

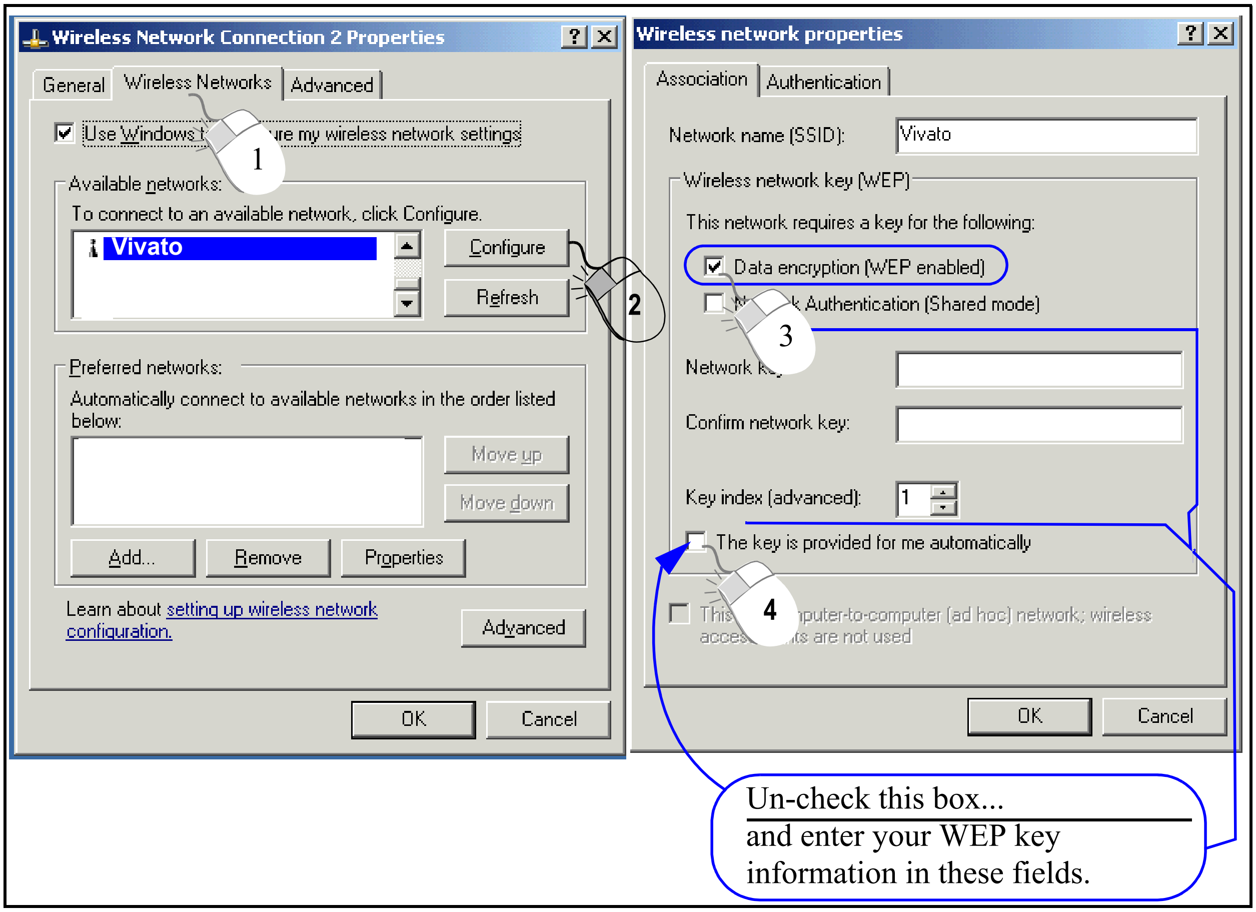
Step 1. Click on the **Wireless Networks** tab in the Wireless Network Connection window and select the **Vivato** entry (see **Figure 35— Configuring WEP in Your Client on page 76**). If the ESSID for the Wi-Fi Switch's wireless interfaces has been changed, use that entry instead.

If you are not receiving the Wi-Fi Switch's signal (no ESSID is shown), verify that a wireless interface has been enabled on the Wi-Fi Switch. See **"Wireless Interfaces"** on page 56.

Step 2. Click **Configure** to display the WEP settings.

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

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



☑ Use Windows t… …re my wireless network settings

Available networks:
To connect to an available network, click Configure.
Vivato

Preferred networks:
Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

Network name (SSID): Vivato

Wireless network key (WEP)
This network requires a key for the following:
☑ Data encryption (WEP enabled)
☐ N…k Authentication (Shared mode)
Network k…:
Confirm network key:
Key index (advanced): 1
☐ The key is provided for me automatically

☐ This … …nputer-to-computer (ad hoc) network; wireless acces… …ts are not used

Un-check this box...
and enter your WEP key information in these fields.

Figure 35—Configuring WEP in Your Client

Configuring EAP in Your Client

Extensible authentication protocol (EAP), or protected EAP (PEAP), should be enabled whenever a RADIUS server is used. Windows 2000 clients can use EAP/PEAP by downloading the free “Microsoft 802.1X Authentication Client” download.

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

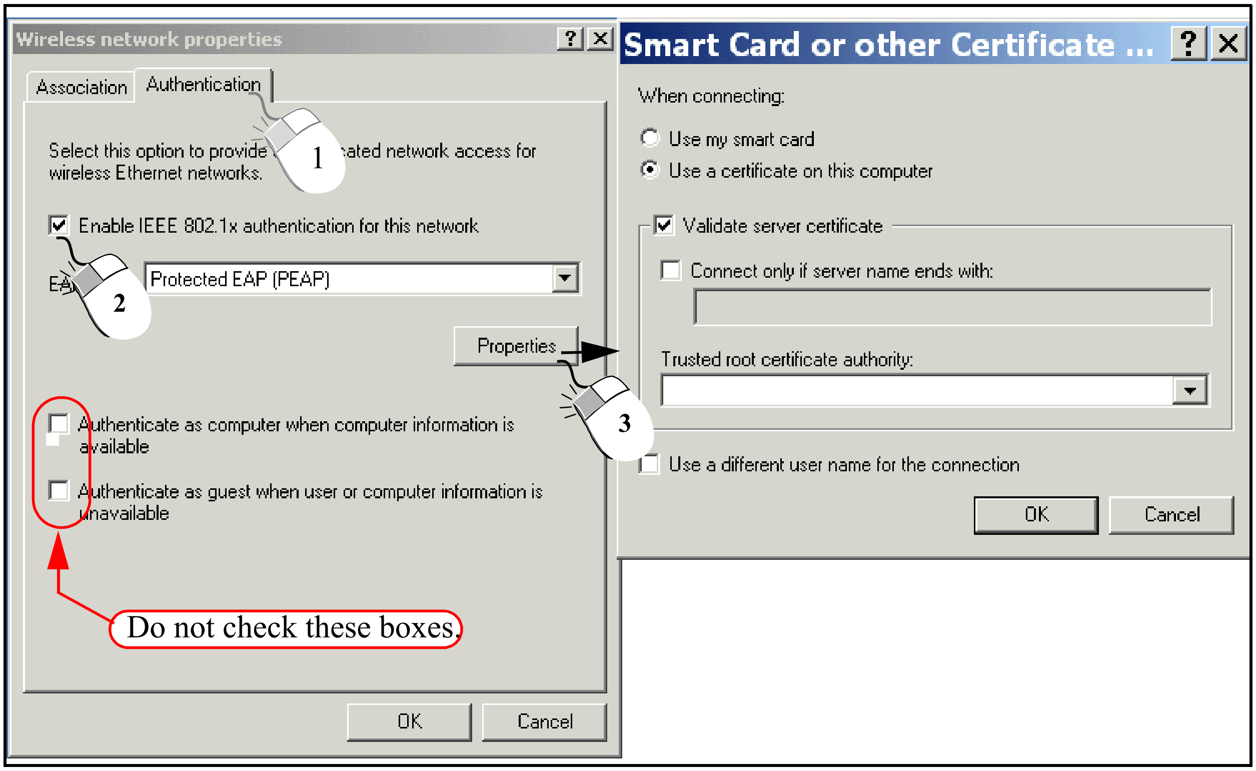
Step 1. Enable WEP, and check the box labeled “The key is provided for me automatically”. See **Configuring WEP in Your Client**. WEP is used with EAP, but the key is provided automatically during the authentication process.

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

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

Step 4. Select **Properties** to specify the method of obtaining authentication certificates that your network uses.

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



Wireless network properties

Association | Authentication

Select this option to provide ...ated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EA... Protected EAP (PEAP)

Properties

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Do not check these boxes.

Smart Card or other Certificate ...

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Validate server certificate

□ Connect only if server name ends with:

Trusted root certificate authority:

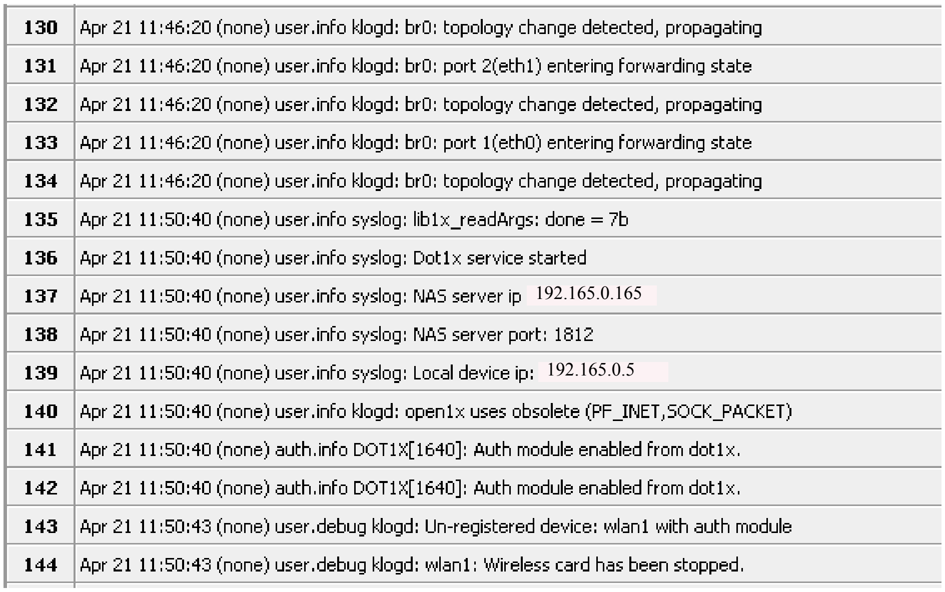
□ Use a different user name for the connection

Monitoring Rogue APs, Clients, and System Operations

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

System Messages

Displays any system messages arising from changes in configuration or from clients associating and disassociating (as shown below).



```
130  Apr 21 11:46:20 (none) user.info klogd: br0: topology change detected, propagating
131  Apr 21 11:46:20 (none) user.info klogd: br0: port 2(eth1) entering forwarding state
132  Apr 21 11:46:20 (none) user.info klogd: br0: topology change detected, propagating
133  Apr 21 11:46:20 (none) user.info klogd: br0: port 1(eth0) entering forwarding state
134  Apr 21 11:46:20 (none) user.info klogd: br0: topology change detected, propagating
135  Apr 21 11:50:40 (none) user.info syslog: lib1x_readArgs: done = 7b
136  Apr 21 11:50:40 (none) user.info syslog: Dot1x service started
137  Apr 21 11:50:40 (none) user.info syslog: NAS server ip 192.165.0.165
138  Apr 21 11:50:40 (none) user.info syslog: NAS server port: 1812
139  Apr 21 11:50:40 (none) user.info syslog: Local device ip: 192.165.0.5
140  Apr 21 11:50:40 (none) user.info klogd: open1x uses obsolete (PF_INET,SOCK_PACKET)
141  Apr 21 11:50:40 (none) auth.info DOT1X[1640]: Auth module enabled from dot1x.
142  Apr 21 11:50:40 (none) auth.info DOT1X[1640]: Auth module enabled from dot1x.
143  Apr 21 11:50:43 (none) user.debug klogd: Un-registered device: wlan1 with auth module
144  Apr 21 11:50:43 (none) user.debug klogd: wlan1: Wireless card has been stopped.
```

SNMP Monitoring

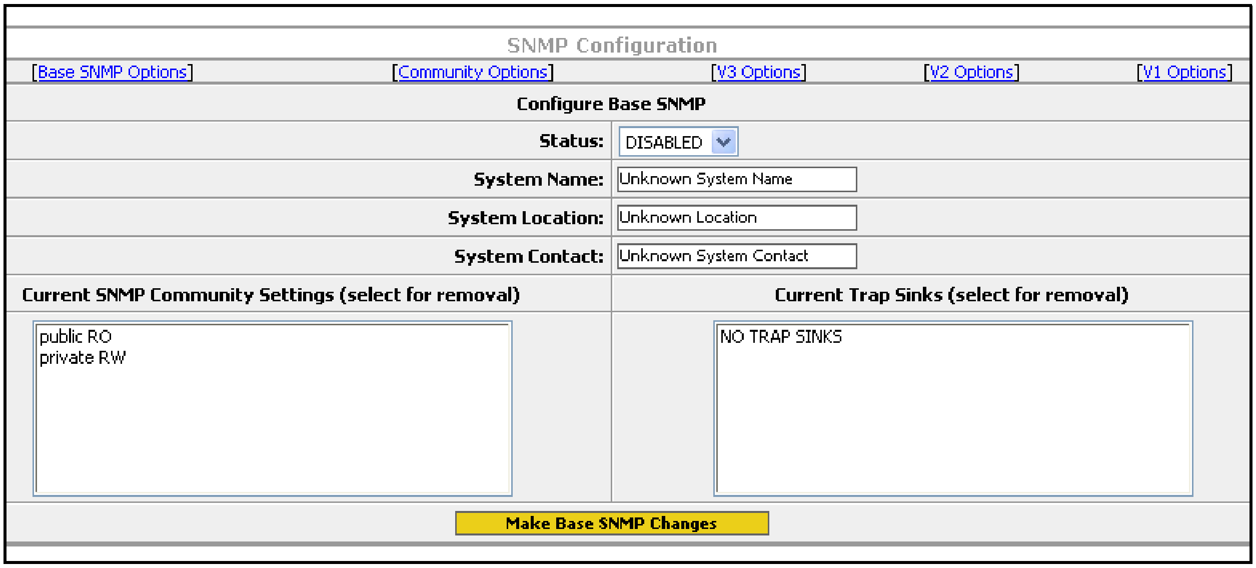
Simple network management protocols (SNMP) use pre-defined sets of data for the Wi-Fi Switch called a management information base (MIB) to monitor network operations. The MIBs are defined in a way that allows third-party developers of network monitoring software to use them with their products. The Vivato Wi-Fi Switch has its own MIB, and also supports several industry standard MIBs. Refer to **"Network Monitoring"** on page 157 for more operation on using SNMP with the Vivato Wi-Fi Switch.

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

Base SNMP Options

These settings do not take effect until Make Base SNMP Changes is selected:

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



Configure Base SNMP

Status:	DISABLED
System Name:	Unknown System Name
System Location:	Unknown Location
System Contact:	Unknown System Contact

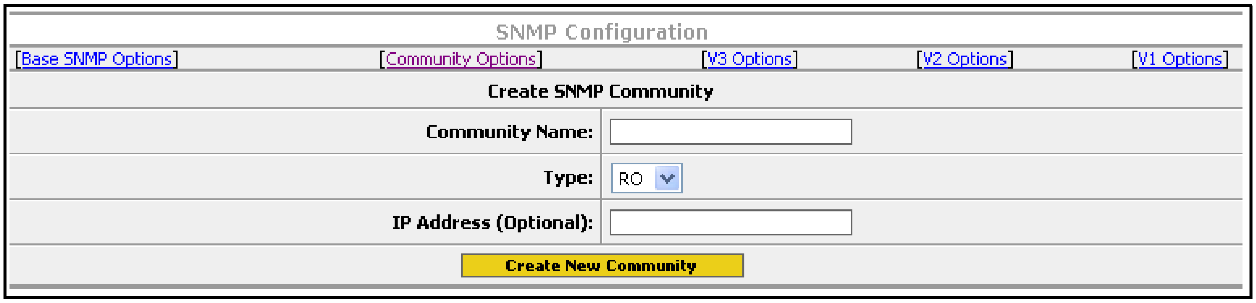
Current SNMP Community Settings (select for removal)	Current Trap Sinks (select for removal)
public RO private RW	NO TRAP SINKS

Figure 36—Base SNMP Options

Create an SNMP Community

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

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



SNMP Configuration

[Base SNMP Options] [Community Options] [V3 Options] [V2 Options] [V1 Options]

Create SNMP Community

Community Name:	
Type:	RO
IP Address (Optional):	

Figure 37—**Create an SNMP Community**

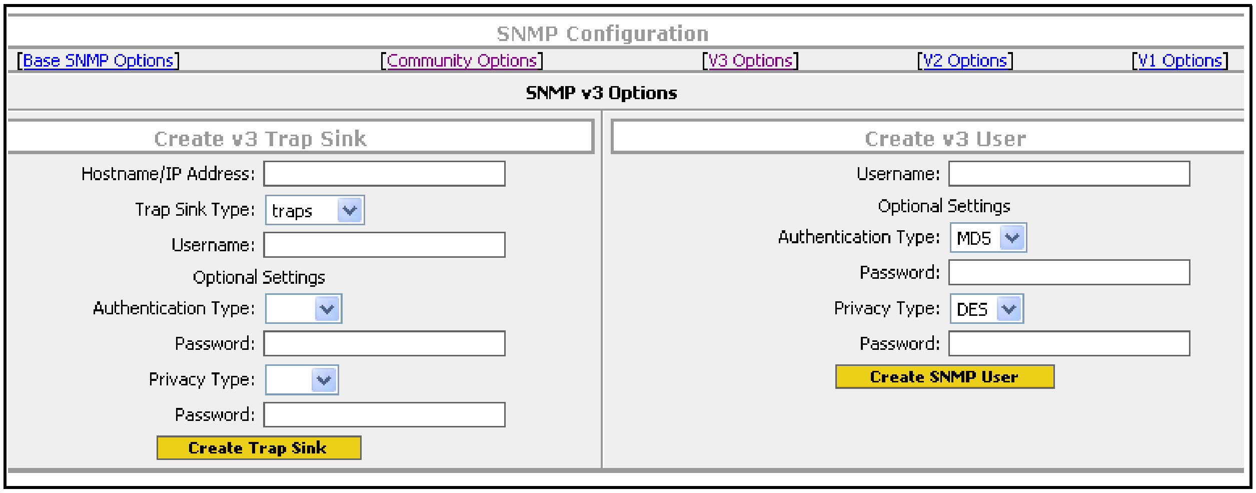
SNMP Version 3 Configuration Settings

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

Create an SNMP Version 3 Trap Sink

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

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



SNMP Configuration

[Base SNMP Options] [Community Options] [V3 Options] [V2 Options] [V1 Options]

SNMP v3 Options

Create v3 Trap Sink

Hostname/IP Address:
Trap Sink Type: traps
Username:
Optional Settings
Authentication Type:
Password:
Privacy Type:
Password:
Create Trap Sink

Create v3 User

Username:
Optional Settings
Authentication Type: MD5
Password:
Privacy Type: DES
Password:
Create SNMP User

Figure 38—SNMP Version 3 Options

Create an SNMP Version 3 User

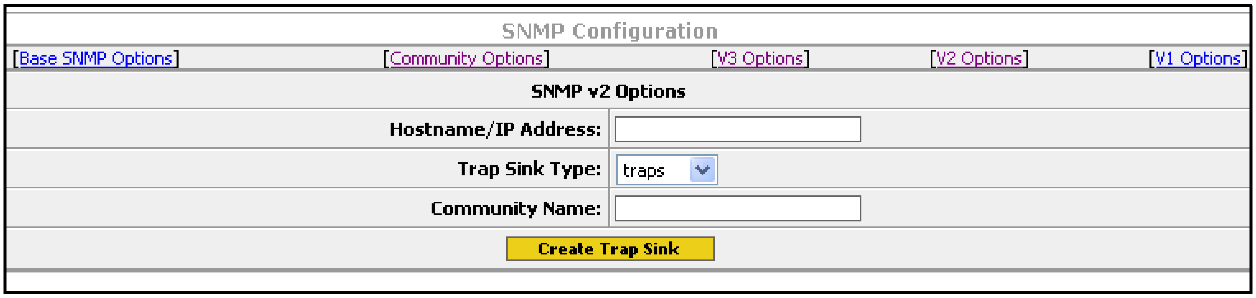
These settings create an SNMP version 3 user. Settings do not take effect until Create SNMP User is selected.

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

SNMP Version 2 Trap Sinks

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

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



SNMP Configuration

[Base SNMP Options] [Community Options] [V3 Options] [V2 Options] [V1 Options]

SNMP v2 Options

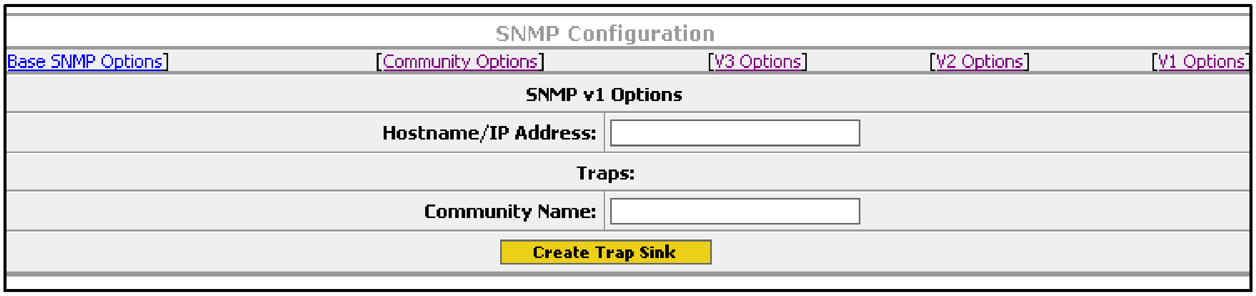
Hostname/IP Address:	
Trap Sink Type:	traps
Community Name:	

Figure 39—Creating an SNMP Version 2 Trap

SNMP Version 1 Traps

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

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



SNMP Configuration

[Base SNMP Options] [Community Options] [V3 Options] [V2 Options] [V1 Options]

SNMP v1 Options

Hostname/IP Address:	
Traps:	
Community Name:	

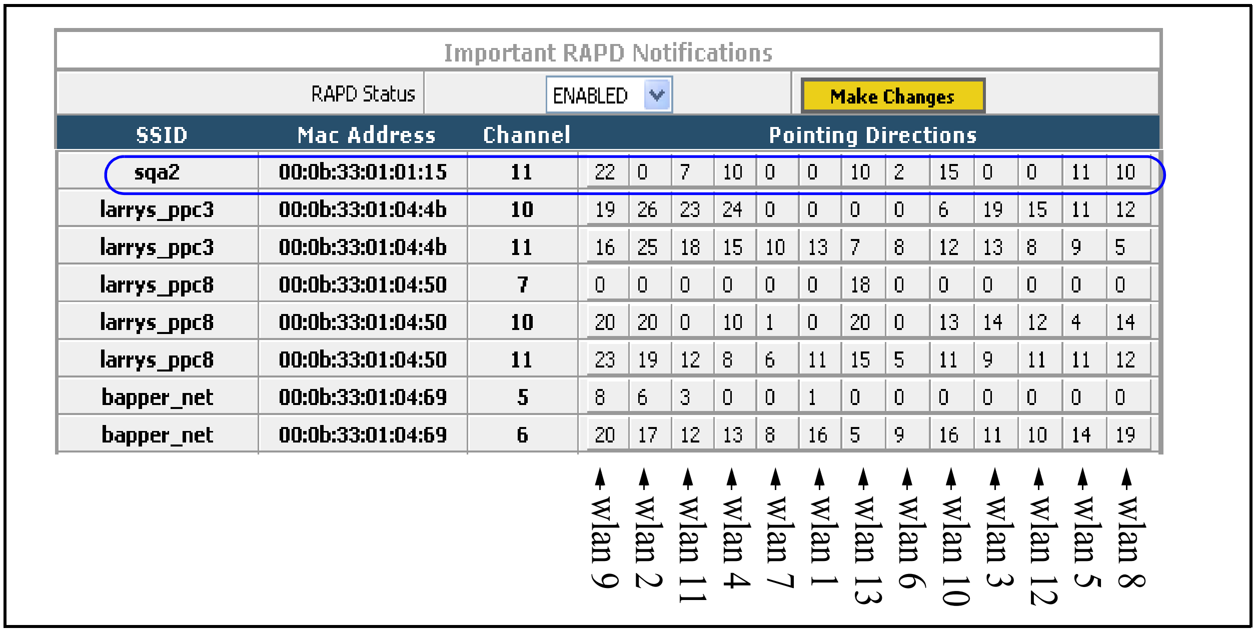
Rogue Access Point Detection (RAPD) and Notification

Access points operating within the coverage area of the Wi-Fi Switch that are not controlled by the Wi-Fi Switch can interfere with Wi-Fi operation. These signals are identified by the Wi-Fi Switch as “rogue APs”.

The rogue AP detector screen displays extensive decoded information from these signals to help you identify and locate their source.

- SSID: The service set identifier (SSID) is similar to the Wi-Fi Switch's ESSID - an identifying name that is broadcast to enable users to select the desired Wi-Fi Switch.
- Mac Address: The media access control number of the device or wireless interface transmitting the received signal.
- Channel: The 802.11b channel for the detected signal.
- Pointing Directions: The signal-to-noise ratio (SNR dB) for this signal as it is received at each of the 13 wireless interfaces in the Wi-Fi Switch. The values are ordered from left to right to correspond to the wireless interface that received that signal (as shown in **"Example Wi-Fi Switch Wireless Interface Assignments"** on page 57).

In the following example, the signal from "sqa2" had a measured SNR of 22 dB on wlan 9, 0 dB SNR was measured on wlan 2 for that signal, 7 dB SNR on wlan 11,... and so forth.



Important RAPD Notifications

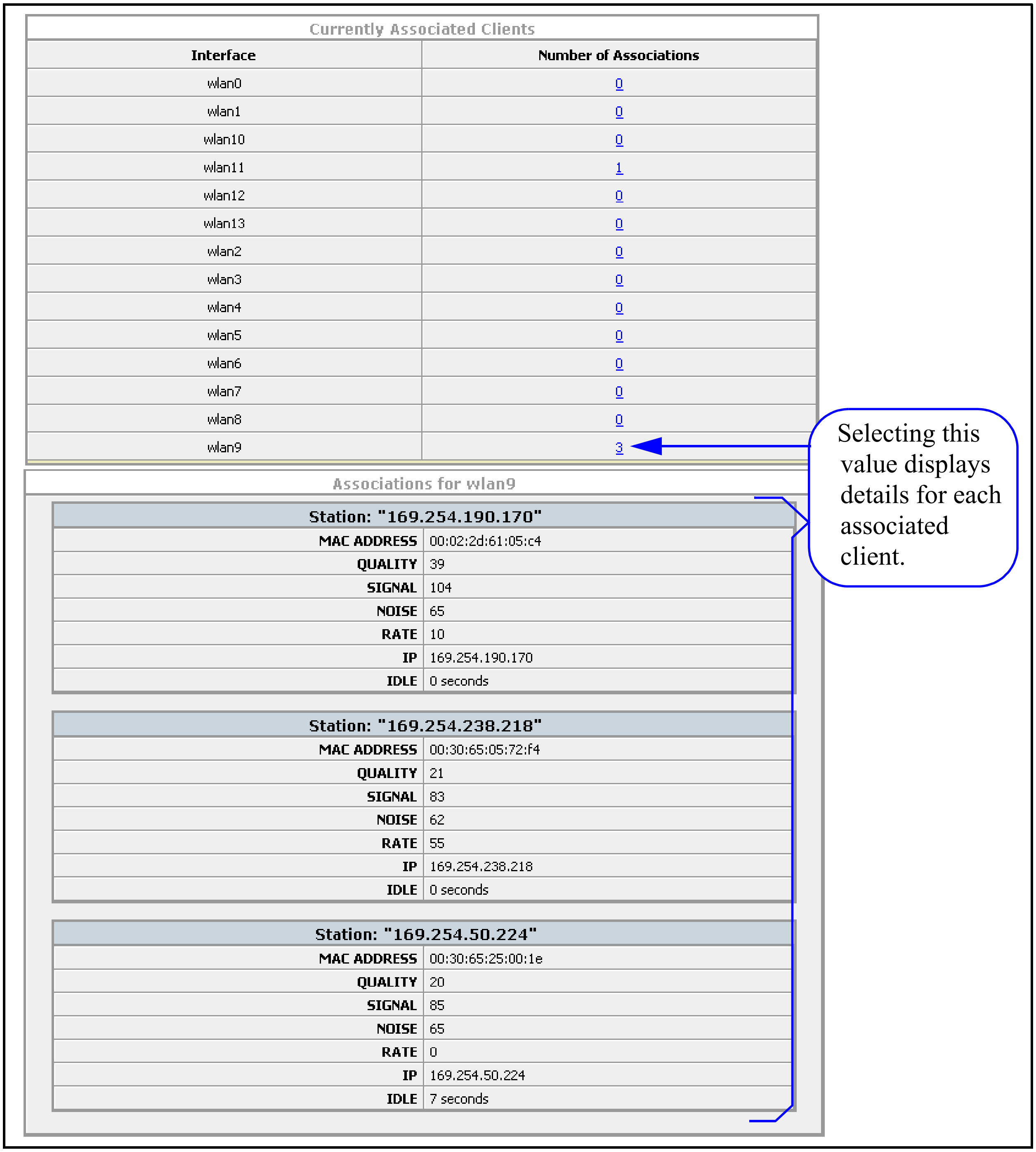
RAPD Status: ENABLED

SSID	Mac Address	Channel	Pointing Directions												
sqa2	00:0b:33:01:01:15	11	22	0	7	10	0	0	10	2	15	0	0	11	10
larrys_ppc3	00:0b:33:01:04:4b	10	19	26	23	24	0	0	0	0	6	19	15	11	12
larrys_ppc3	00:0b:33:01:04:4b	11	16	25	18	15	10	13	7	8	12	13	8	9	5
larrys_ppc8	00:0b:33:01:04:50	7	0	0	0	0	0	0	18	0	0	0	0	0	0
larrys_ppc8	00:0b:33:01:04:50	10	20	20	0	10	1	0	20	0	13	14	12	4	14
larrys_ppc8	00:0b:33:01:04:50	11	23	19	12	8	6	11	15	5	11	9	11	11	12
bapper_net	00:0b:33:01:04:69	5	8	6	3	0	0	1	0	0	0	0	0	0	0
bapper_net	00:0b:33:01:04:69	6	20	17	12	13	8	16	5	9	16	11	10	14	19

Figure 40—Example Rogue Access Point Detection Results

Associated Clients

This table displays information about clients that are currently associating with the Wi-Fi Switch. This information is helpful in understanding the number of clients associating through each wireless interface in the Wi-Fi Switch and who those clients are.



Currently Associated Clients

Interface	Number of Associations
wlan0	0
wlan1	0
wlan10	0
wlan11	1
wlan12	0
wlan13	0
wlan2	0
wlan3	0
wlan4	0
wlan5	0
wlan6	0
wlan7	0
wlan8	0
wlan9	3

Selecting this value displays details for each associated client.

Associations for wlan9

Station: "169.254.190.170"	
MAC ADDRESS	00:02:2d:61:05:c4
QUALITY	39
SIGNAL	104
NOISE	65
RATE	10
IP	169.254.190.170
IDLE	0 seconds

Station: "169.254.238.218"	
MAC ADDRESS	00:30:65:05:72:f4
QUALITY	21
SIGNAL	83
NOISE	62
RATE	55
IP	169.254.238.218
IDLE	0 seconds

Station: "169.254.50.224"	
MAC ADDRESS	00:30:65:25:00:1e
QUALITY	20
SIGNAL	85
NOISE	65
RATE	0
IP	169.254.50.224
IDLE	7 seconds

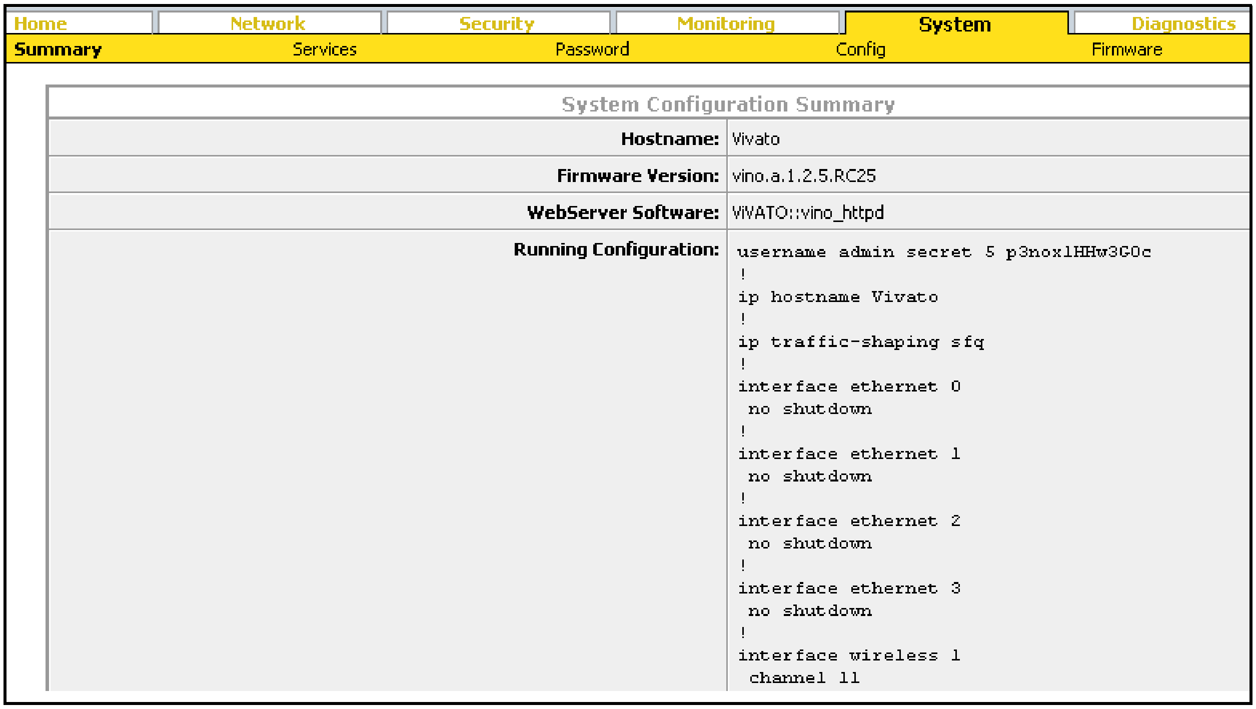
Figure 41—Example Associated Clients Listing

Services, Password, Config, and Firmware Web Pages

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

Summary

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



System Configuration Summary

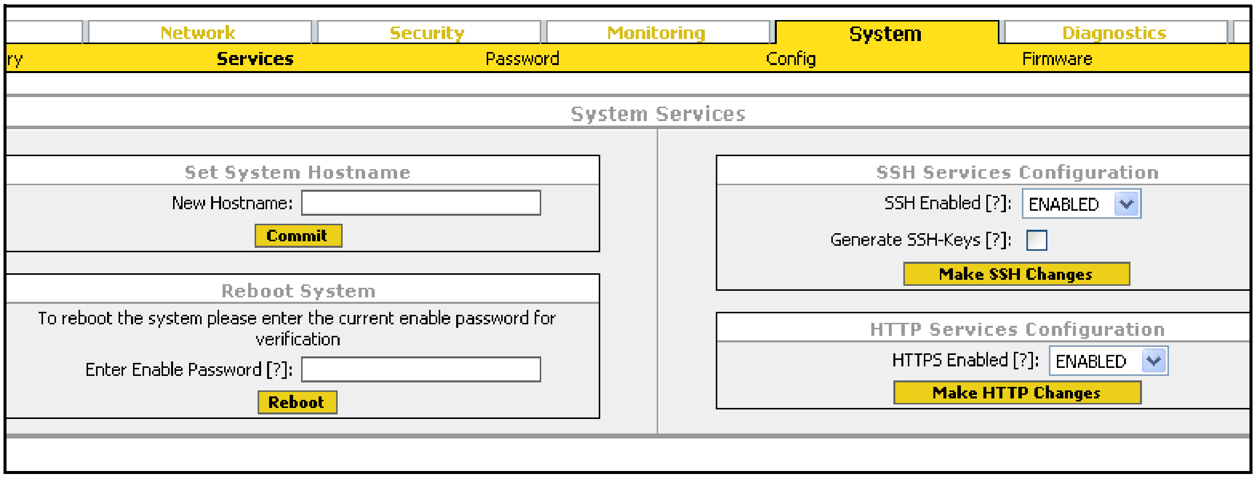
Hostname:	Vivato
Firmware Version:	vino.a.1.2.5.RC25
WebServer Software:	VIVATO::vino_httpd
Running Configuration:	

```
username admin secret 5 p3noxlHHw3G0c
!
ip hostname Vivato
!
ip traffic-shaping sfq
!
interface ethernet 0
 no shutdown
!
interface ethernet 1
 no shutdown
!
interface ethernet 2
 no shutdown
!
interface ethernet 3
 no shutdown
!
interface wireless 1
 channel 11
```

Figure 42—Example System Summary Screen

Services

Services lets you enable and disable communications with outside hosts used for a variety of operations, set or change the host name, and reboot the Wi-Fi Switch.



System Services

Set System Hostname

New Hostname:

Commit

Reboot System

To reboot the system please enter the current enable password for verification

Enter Enable Password [?]:

Reboot

SSH Services Configuration

SSH Enabled [?]: ENABLED

Generate SSH-Keys [?]: □

Make SSH Changes

HTTP Services Configuration

HTTPS Enabled [?]: ENABLED

Make HTTP Changes

Set System Hostname

Enter a host name for the Wi-Fi Switch. The host name can also be set using the Quick Setup web pages. See **"Basic Network Setup"** on page 46.

Reboot System

Entering the enable password and selecting Reboot causes the Wi-Fi Switch to reboot using the last configuration saved as “vivato.conf”.

Rebooting causes any unsaved configuration changes to be discarded. To preserve your current configuration, use Configuration File Options to save your configuration (see **"Config"** on page 89).

SSH Services Configuration

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

- **SSH Enabled**: Enable or disable the use of a secure shell to access the configuration settings.
- **Generate SSH-Keys**: Check this box to generate keys required for secure shell operation when Make SSH Changes is selected.

HTTP Services Configuration

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

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

Password

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

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

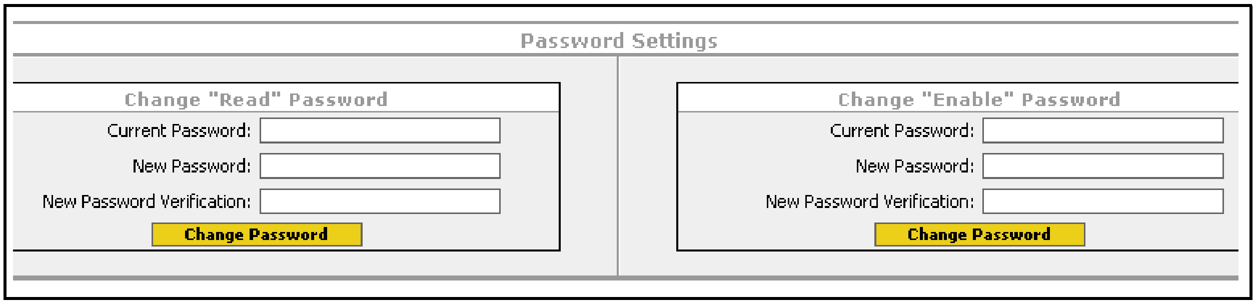


Figure 43—Changing the Read and Enable Passwords

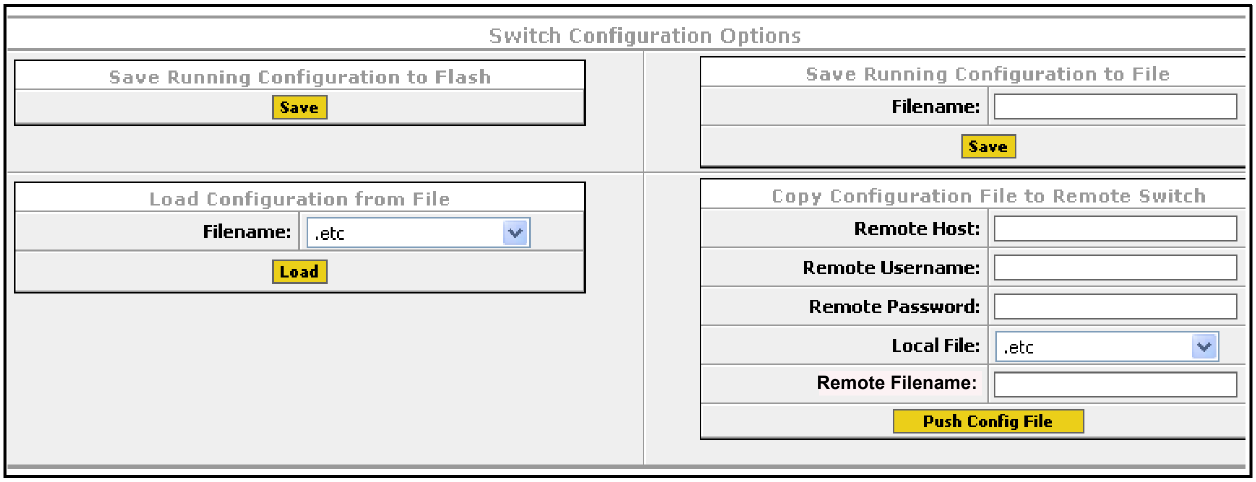
Config

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

Unless you save the current configuration under a new name, the Wi-Fi Switch uses the default configuration file entitled "startup-config".

- **Save Running Configuration to Flash**: Save the current configuration settings as the default "startup-config" file. The next time you reboot the Wi-Fi Switch, these configuration settings are automatically used.
- **Load Configuration From File**: Select the configuration file to load when **Load** is selected. These settings are in effect until you change them, or until the Wi-Fi Switch is rebooted.

- **Save Current Config To File**: Enter a file name to use for saving the configuration when **Save** is selected.
- **Save Running Configuration to File**: Enter a file name for saving the current configuration when Save is selected. These settings can be retrieved at a later date using the **Load Configuration from File** function.
- **Copy Configuration File to Remote Switch**: These settings are used to copy a configuration file on the local Wi-Fi Switch to another Wi-Fi Switch:
- **Remote Host**: Enter the host name or IP address of the remote Wi-Fi Switch.
- **Remote Username**: Enter the user name specified for the remote Wi-Fi Switch.
- **Remote Password**: Enter the read level password for the remote Switch.
- **Local File**: Select the file to transfer to the remote Switch.
- **Remote Filename**: Enter the name to use for storing the configuration file on the remote Switch.
- **Push Config File**: Send the configuration file to the remote Switch.



Switch Configuration Options

Save Running Configuration to Flash

Save

Save Running Configuration to File

Filename:

Save

Load Configuration from File

Filename: .etc

Load

Copy Configuration File to Remote Switch

Remote Host:

Remote Username:

Remote Password:

Local File: .etc

Remote Filename:

Push Config File

Returning to Factory Configuration Defaults

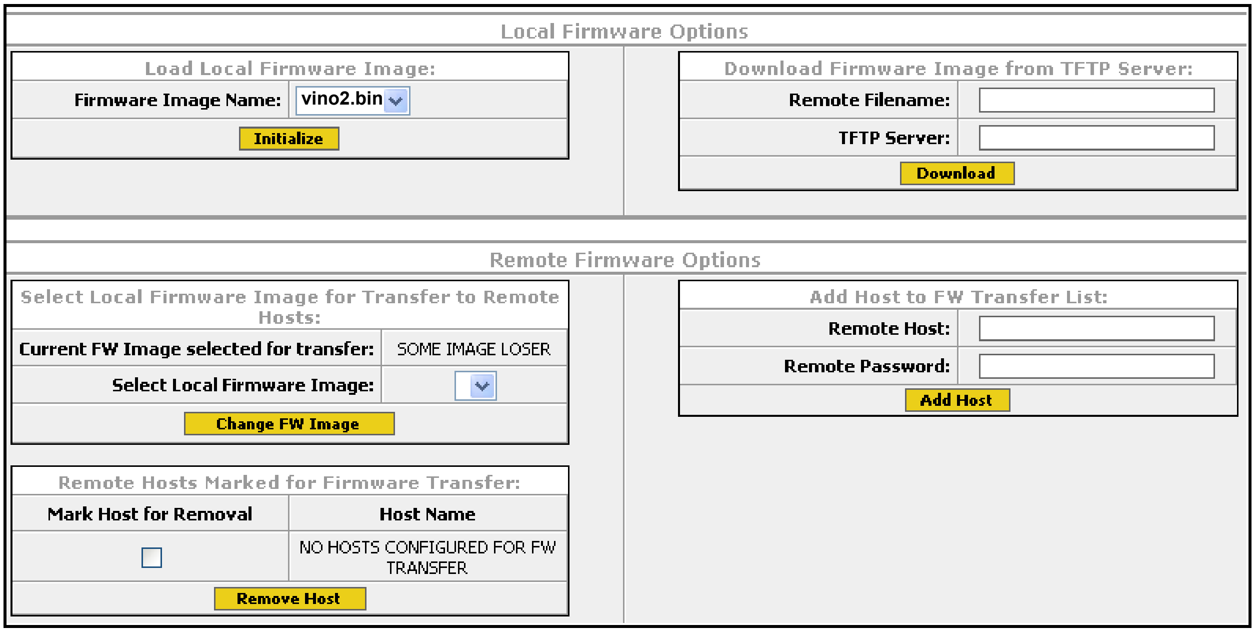
The “startup-config” file is created whenever you reboot after using the Quick Setup web pages to configure the Wi-Fi Switch. It can also be created by saving the configuration using the **System>Config>Save Running Configuration to Flash function** or through the ‘write <enter>” CLI command. The Wi-Fi Switch uses this file to configure itself after a reboot unless you specify a different configuration file to use.

To return the Wi-Fi Switch to the as-delivered factory default configuration, you need to delete the existing “startup-config” file and reboot the Wi-Fi Switch. Use the CLI command **"delete flash: <filename>"** on page 118 to delete the “startup-config” file.

Firmware

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

You can update the firmware on the local Wi-Fi Switch, and also “push” the firmware to a remote Wi-Fi Switch in order to update it.



Local Firmware Options

Load Local Firmware Image:

Firmware Image Name:	vino2.bin

Initialize

Download Firmware Image from TFTP Server:

Remote Filename:	
TFTP Server:	

Download

Remote Firmware Options

Select Local Firmware Image for Transfer to Remote Hosts:

Current FW Image selected for transfer:	SOME IMAGE LOSER
Select Local Firmware Image:	

Change FW Image

Add Host to FW Transfer List:

Remote Host:	
Remote Password:	

Add Host

Remote Hosts Marked for Firmware Transfer:

Mark Host for Removal	Host Name
□	NO HOSTS CONFIGURED FOR FW TRANSFER

Remove Host

Local Firmware Options

To download firmware from a trivial file transfer protocol (TFTP) server, enter the following information:

- **Remote Filename**: Enter the file name of the firmware that you want to download.
- **TFTP Server**: Enter the host name or IP address of the TFTP server where the firmware file resides.
- **Download**: Download the firmware file into the Wi-Fi Switch’s flash memory.

To start using the new firmware, select the file name using the Select Local Firmware Image function, and click on Initialize.

Remote Firmware Options

You can “push” a new version of firmware to one or more remote Wi-Fi Switch’s in order to upgrade them at the same time.

Adding a Remote Host to The Firmware Transfer List

You can create a list of remote hosts in which you want to save the new firmware. For each host, enter the Remote Host name or IP address, and the Remote Password (read password) for that host. When Add Host is selected, that host is shown in the “Remote Hosts Marked for Firmware Transfer” list.

Removing a Remote Host from the Firmware Transfer List

To remove a host from this list, check the corresponding “Mark Host for Removal” box and select Remove Host.

Selecting the Local Image to Transfer

Use the “Select Local Firmware Image” drop-down menu to select the firmware image to transfer to the remote hosts listed in the firmware transfer list. The firmware is transferred to each host when you select Change FW Image.

Important ❗	The Wi-Fi Switch can contain a maximum of two firmware images. If two images already exist in memory, you need to remove one of the images (typically the older image) before loading a new image.

Quick Setup

Displays the initial Quick Setup screen to access the quick setup pages and make any changes. See **"Initial Configuration Using the Built-In Web Pages"** on page 35.

Diagnostics and Help Web Screens

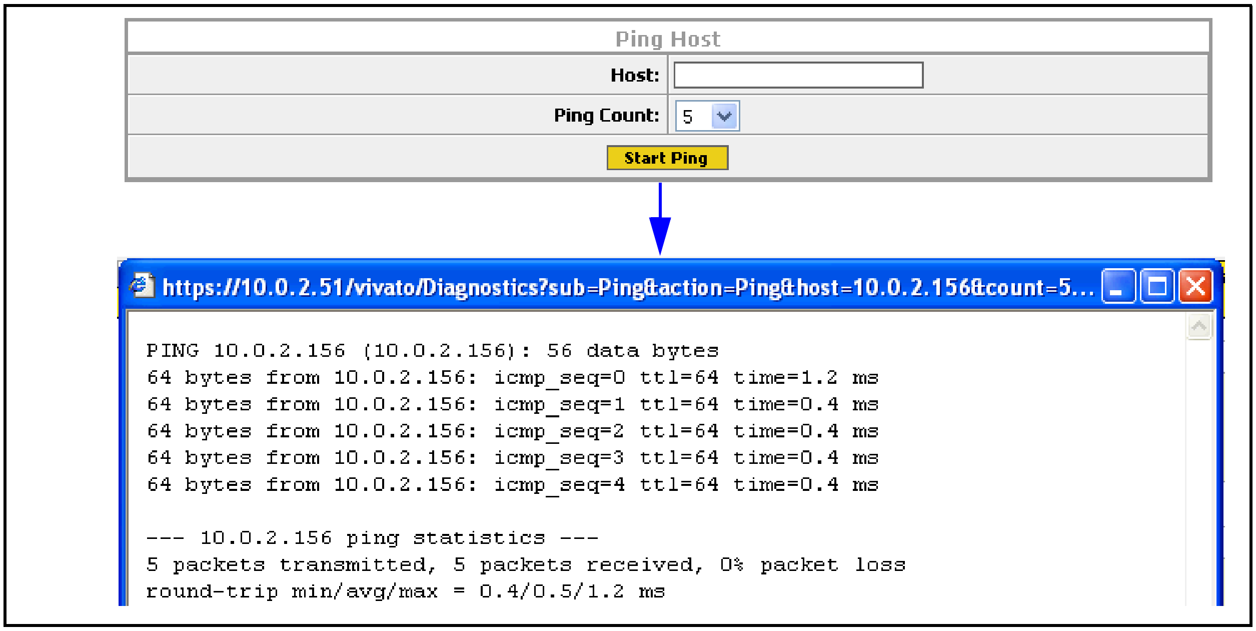
A **Diagnostics** web page is available to troubleshoot communications problems, and a **Help** link is provided to access the Vivato home page.

Diagnostics

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

Ping

Pinging a device tests 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. An example ping result is shown **Figure 44—Example Results of Pinging a Host With Five Packets**.



Host:
Ping Count: 5

https://10.0.2.51/vivato/Diagnostics?sub=Ping&action=Ping&host=10.0.2.156&count=5...

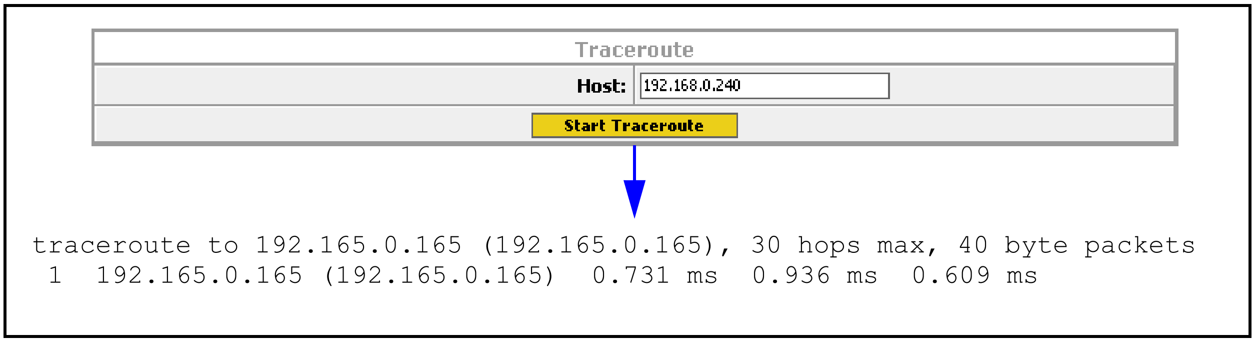
```
PING 10.0.2.156 (10.0.2.156): 56 data bytes
64 bytes from 10.0.2.156: icmp_seq=0 ttl=64 time=1.2 ms
64 bytes from 10.0.2.156: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 10.0.2.156: icmp_seq=2 ttl=64 time=0.4 ms
64 bytes from 10.0.2.156: icmp_seq=3 ttl=64 time=0.4 ms
64 bytes from 10.0.2.156: icmp_seq=4 ttl=64 time=0.4 ms

--- 10.0.2.156 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/1.2 ms
```

Figure 44—Example Results of Pinging a Host With Five Packets

Traceroute

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



```
traceroute to 192.165.0.165 (192.165.0.165), 30 hops max, 40 byte packets
 1  192.165.0.165 (192.165.0.165)  0.731 ms  0.936 ms  0.609 ms
```

Help

Selecting the Help tab causes the Wi-Fi Switch to access the Vivato website (www.vivato.net). Select the Customer Support link to view the latest available help information.

Command Line Interface

Refer to **"Default Configuration"** on page 36 before performing additional configuration using the CLI.

The command line interface (CLI) is used to change settings and query values in the Vivato Wi-Fi Switch; it is an alternative to using the web page interface. The CLI can be used to initially configure the Wi-Fi Switch 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. Almost every function in the Vivato Wi-Fi Switch 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.

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

Connections and Terminal Settings

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

- Running a Secure Shell (SSH) session configured for TCP/IP, and connected to the Wi-Fi Switch's Secure Management port or LAN port (eth0). See **"Connections to the Vivato Wi-Fi Switch"** on page 17). 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 Wi-FI Switch. See **"Enabling Your Network Adapter to Access the Wi-Fi Switch"** on page 38.
- 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

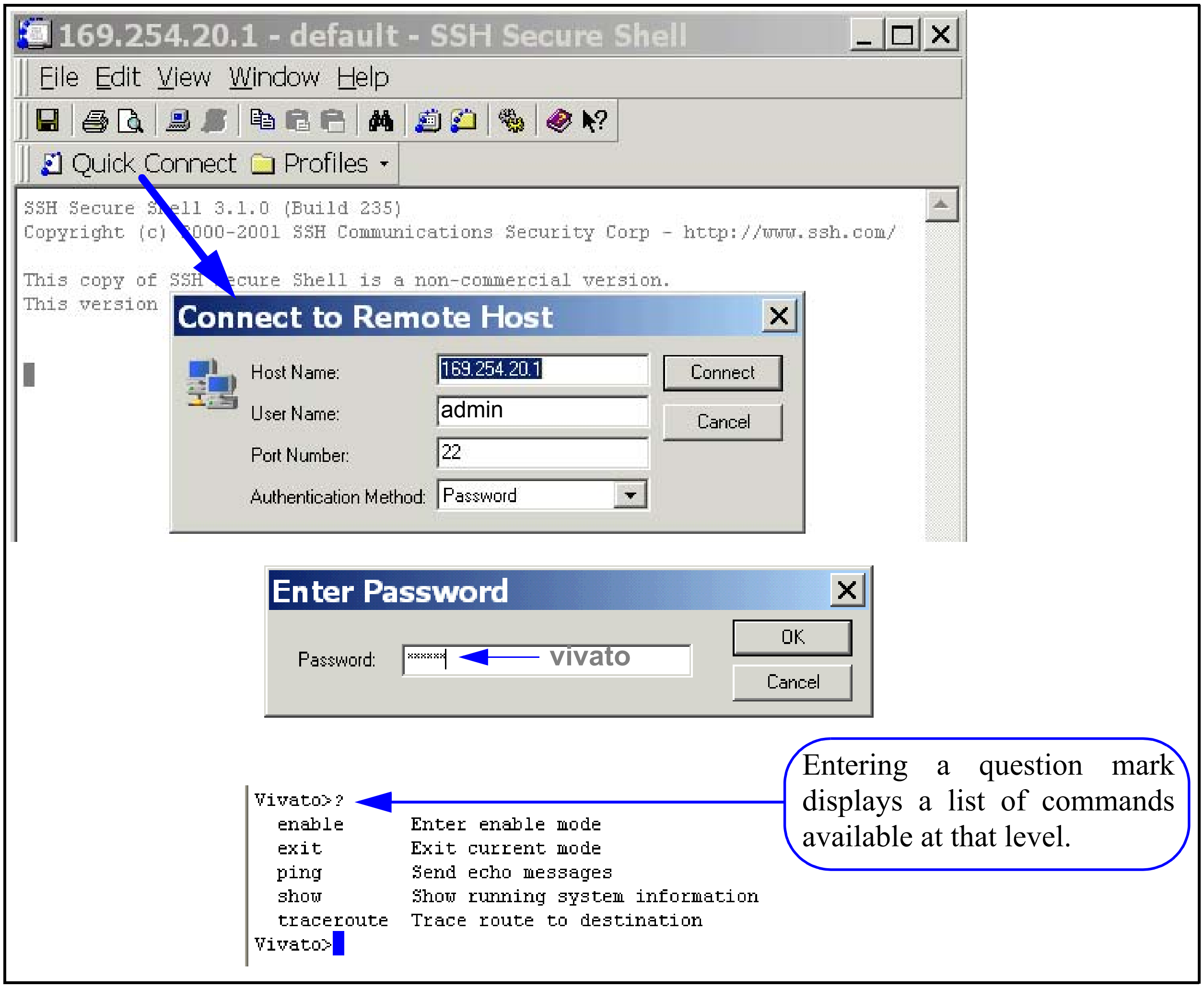
After connecting the switch to your computer and initiating communications, a command prompt should be displayed on your computer. The following example illustrates how to access the read level using the SSH Secure Shell© client:

1 Using the Quick Connect feature of the secure shell client, enter the IP address of the Wi-Fi Switch 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).



```
SSH Secure Shell 3.1.0 (Build 235)
Copyright (c) 2000-2001 SSH Communications Security Corp - http://www.ssh.com/

This copy of SSH Secure Shell is a non-commercial version.
This version
```

Host Name: 169.254.20.1

User Name: admin

Port Number: 22

Authentication Method: Password

Password: ****** vivato

```
Vivato>?
  enable      Enter enable mode
  exit        Exit current mode
  ping        Send echo messages
  show        Show running system information
  traceroute  Trace route to destination
Vivato>
```

Entering a question mark displays a list of commands available at that level.

Figure 45—**Using Secure Shell to Access the CLI and Display Read Level Commands**

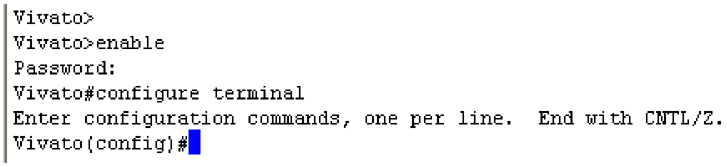
Accessing the Configuration Level

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

1 At the **vivato>** prompt, enter **enable**.

2 The Wi-Fi Switch is shipped without an enable password. If you have created an enable password (when using the Quick Setup web pages or by using the CLI), enter that password when prompted.

3 Enter **configure terminal** to access the global configuration level. The prompt changes to **vivato (config)#**. At this point you can start configuring the Wi-Fi Switch.



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

Figure 46—Accessing the Global Configuration Level

Configuration Example

This example mimics setting the Wi-Fi Switch 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)% essid 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 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 11
vivato (config-wlan4)% exit
vivato (config)$ interface wireless 5
vivato (config-wlan5)% channel 11
vivato (config-wlan5)% exit
vivato (config)$ interface wireless 6
vivato (config-wlan6)% channel 11
vivato (config-wlan6)% exit
vivato (config)$ interface wireless 7
vivato (config-wlan7)% channel 1
vivato (config-wlan7)% exit
vivato (config)$ interface wireless 8
vivato (config-wlan8)% channel 1
vivato (config-wlan8)% exit
vivato (config)$ interface wireless 9
vivato (config-wlan9)% channel 1
vivato (config-wlan9)% exit
vivato (config)$ interface wireless 10
vivato (config-wlan10)% channel 1
vivato (config-wlan10)% exit
vivato (config)$ interface wireless 11
vivato (config-wlan11)% channel 1
vivato (config-wlan11)% exit
vivato (config)$ interface wireless 12
vivato (config-wlan12)% channel 1
vivato (config-wlan12)% exit
vivato (config)$ interface wireless 13
vivato (config-wlan13)% channel 1
vivato (config-wlan13)% 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 1
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)$ add interface wireless 6
vivato (config-br0)$ add interface wireless 7
vivato (config-br0)$ add interface wireless 8
vivato (config-br0)$ add interface wireless 9
vivato (config-br0)$ add interface wireless 10
vivato (config-br0)$ add interface wireless 11
vivato (config-br0)$ add interface wireless 12
vivato (config-br0)$ add interface wireless 13
```

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 Wi-Fi Switch 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 EAP and PPTP security are disabled.

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

Enable Traffic Shaping

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

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 Wi-Fi Switch 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”.
Enable (Global Configuration)	From the Enable level, enter **configure terminal**	**vivato (config)#**	Type “exit”.
Configure Specific Functions	At the global configuration prompt, enter the appropriate configuration command. For example, entering **interface ethernet 0** accesses the configuration settings for the ethernet 0 port.	Depends on the configuration function. For configuring the wireless interface, the prompt would be **vivato (config-eth0)#**	Type “exit” to return to the global configuration prompt. You also enter **Ctrl-z** to exit the global configuration mode are return to the initial enable prompt.

Command Conventions

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

Entering Commands on the Command LIne

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

Reading the Command LIsting

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

Entering Variables

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

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

Optional Entries

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

Read Level Command Descriptions

The following commands are available at the read level.

enable

Enter the enable mode. This command must be issued any time you are going to change any 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 Wi-Fi Switch 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 47—**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.

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 48—**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 49—Example "show eap" Output

show http-server

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

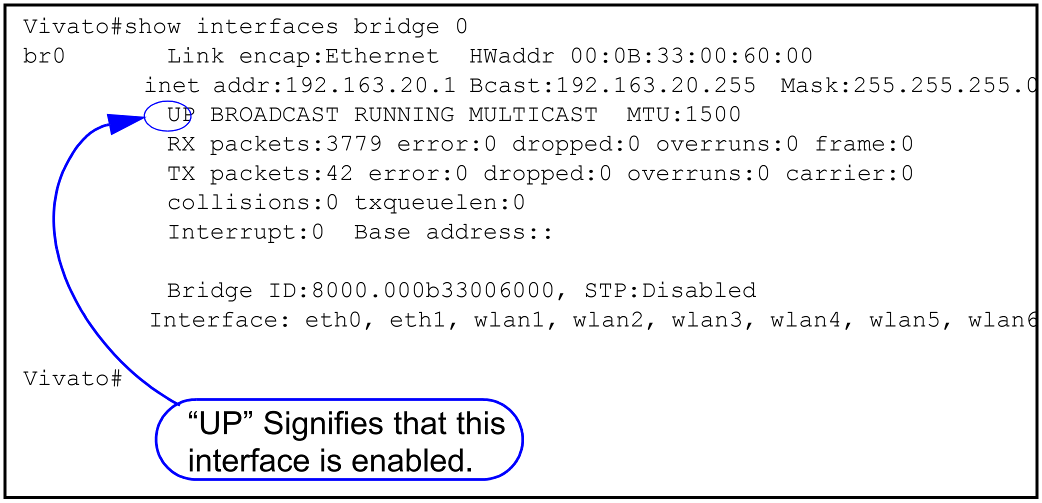
show interfaces

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”).



```
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#
```

Figure 50—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 51—Example “show interfaces bridge 0 fdb” Output

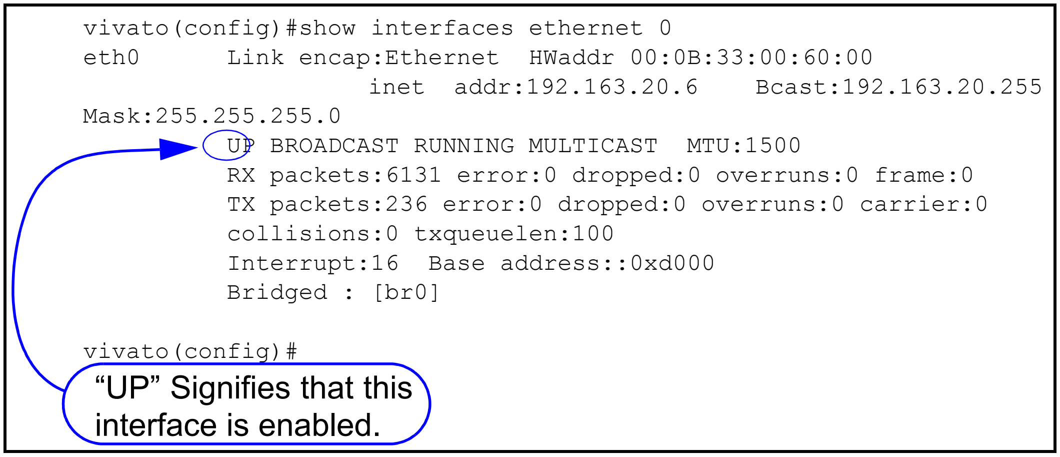
show interfaces bridge <0-4094> stp

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”).



```
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)#
```

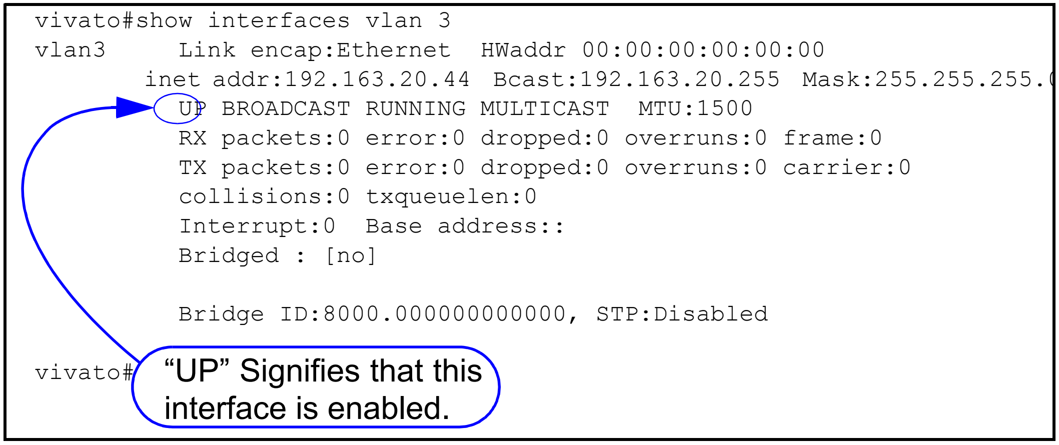
“UP” Signifies that this interface is enabled.

Figure 52—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, which interfaces are part of each VLAN, and whether spanning tree protocol (STP) is enabled on that 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”).



```
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.
          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 53—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 Wi-Fi Switch 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 54—Example “show interfaces vlan fdb” Output

show interfaces wireless [associations]

Displays the configuration of all wireless interfaces, or (optionally) the number of clients associating with each interface. Configuration information includes the ESSID and WEP encryption key value (if used), channel assignment, association with any bridges, and bit rate.

```
Vivato# show interfaces wireless 1 associations
wlan1 - There are 1 associated stations
STA MAC Addr          SNR Sig Noi   Rate IP                    Rx       Tx Idle
================================================================================
 1 00:02:2d:66:53:8d  24 -61 -85 11Mbps 192.163.0.135    1.6KB   0.8KB 50 seconds

Vivato#
```

Figure 55— Example “show interfaces wireless associations” Output

show interfaces wireless <1-13> [associations]

Displays the configuration of the specified wireless interface, or (optionally) the number of clients associating with that interface. Configuration information includes the ESSID and WEP encryption key value (if used), channel assignment, association with any bridges, and bit rate.

```
Vivato#show interfaces wireless 1
wlan1     Link encap:Ethernet  HWaddr 00:0B:33:00:60:09
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:512 error:62670 dropped:1 overruns:0 frame:0
          TX packets:10226 error:185 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:21  Base address::0xd140
          Bridged : [br0]

          Essid:spongebob
          Channel:1  Access Point:00:0B:33:00:60:09
          Bit Rate:11Mb/s
          Encryption key:XXXX   Encryption mode:restricted
          Link Quality:0   Signal level:0   Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:0   Missed beacon:0

Vivato#
```

Figure 56—Example "show interfaces wireless 1" Output

show ip domainname

Displays the domain name for the Wi-Fi Switch.

show ip host

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

show ip hostname

Displays the host name for the Wi-Fi Switch.

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 Wi-Fi Switch. 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.

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 pptp

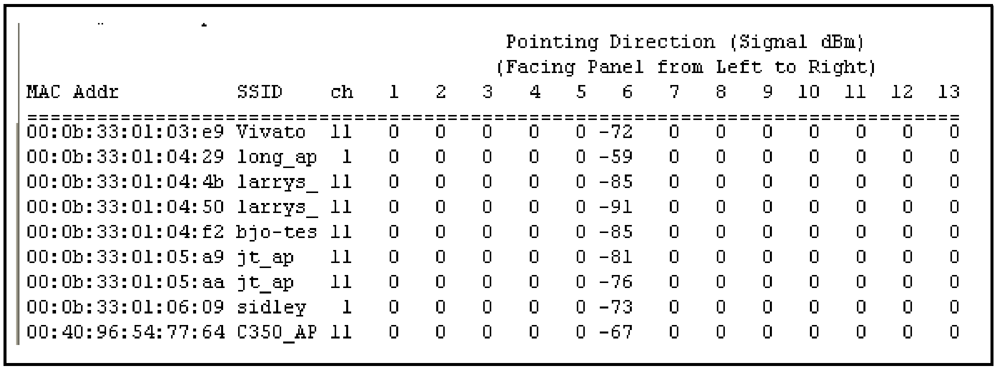
Displays the status and configuration for point to point tunneling protocol (PPTP) security.

```
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 57—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 Wi-Fi Switch’s antenna pattern. The results for each detected signal are only displayed for the channel with the greatest signal strength for any MAC address.

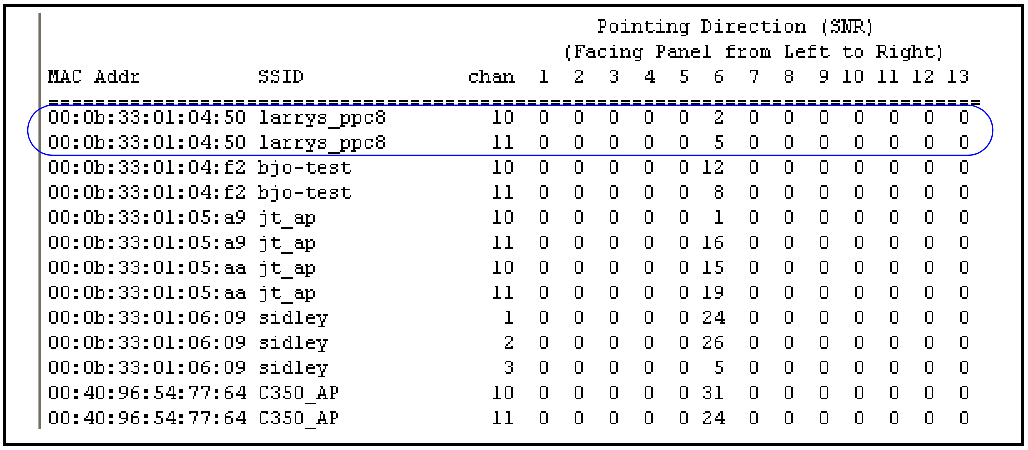


```
                                         Pointing Direction (Signal dBm)
                                        (Facing Panel from Left to Right)
MAC Addr          SSID     ch   1   2   3   4   5   6   7   8   9  10  11  12  13
================================================================================
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 58—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 Wi-Fi Switch's antenna pattern. Because a signal can "bleed over" into an adjacent channel, the power of the signal with a particular MAC address my be displayed for more than one channel (as shown in the example below).

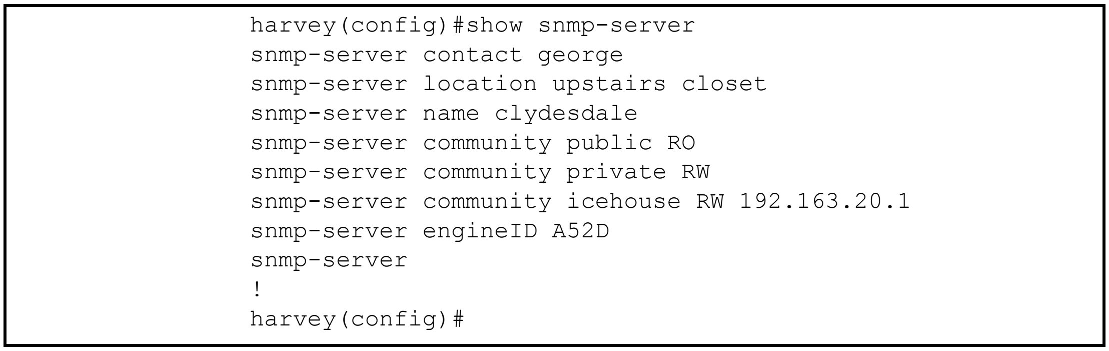


```
                                                       Pointing Direction (SNR)
                                                    (Facing Panel from Left to Right)
MAC Addr          SSID                    chan  1  2  3  4  5  6  7  8  9 10 11 12 13
==================================================================================
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 59—Example "show rapd-full" Output

show snmp-server

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



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

Figure 60—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

Displays information about the version of software that is installed in the switch.

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 Wi-Fi Switch. Configuration files are saved using the **write network fla sh:**.

show running-config

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

traceroute <ipaddress|hostname>

Displays information about the network route used to access the specified destination address or host name. If the specified address or host is not found, the Wi-Fi Switch 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 105).

Table 5—Enable Level Commands

configure [terminal]
Commands for Managing Configuration Files
Configure System (boot system flash:)
Configure Clock
Configure Crypto (Generate Keys)
Configure EAP Commands
Configure No EAP Commands
Configure Enable Secret
Configure HTTP-Server
Configure Interface Commands
interface bridge <0-4094>
interface ethernet <0-3>
interface vlan <vlan id>
interface wireless <1-13|all>
disable
exit

Configure No Interface Commands
Configure IP Command
Configure Log Commands
Configure PPTP Commands
Configure No PPTP Commands
Configure RAPD
Configure SNMP-Server Commands
Configure No SNMP-Server Commands
Configure Username Admin (Read Level) Secret
Configure Vivato Packet Shaping
edit flash:
reboot

configure [terminal]

This command tells the CLI to use your terminal to configure the switch after accessing the enable level (see "enable" on page 105). 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 Wi-Fi Switch. All of these commands are available at the enable level prompt, **Vivato#**, but are not available at the configuration prompt, **Vivato(conf)#**.

configure network flash: <filename>

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.

Important

The default configuration file name is “startup-config”, and is created the first time you use the Quick Setup web pages for the initial configuration or when you save a configuration using that default file name. Once startup-config is created, the Wi-Fi Switch is *always* configured using that file whenever a reboot occurs by cycling power or by issuing the “reboot” command. To use a different configuration file as the default reboot configuration, use the **copy flash: flash:** command to rename that file “startup-config”. When you reboot the Wi-Fi Switch, the settings in the new startup-config file are used. The **copy flash: flash:** command can be used to save a copy of the current startup-config file before replacing it. See also **"Returning to Factory Configuration Defaults"** on page 90.

copy flash: flash:

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

```
Vivato#copy flash: flash:

Source file: startup-config

Destination file: old-config

Vivato>
```

copy flash: scp:

This command is used to copy a configuration file from the Wi-Fi Switch to another device. After entering this command, you are prompted to enter the name of the configuration file on the Wi-Fi Switch, 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 (as shown below):

```
Vivato#copy flash: scp:

Source file: startup-config

Username: gerry

Password:

Hostname: gardenhose

Directory [/]: wifibackups

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

copy scp: flash:

This command is used to copy a configuration file from another device to the Wi-Fi Switch. After entering this command, you are prompted to enter the user name and password on the remote device, the hostname (or IP address) where the file is stored, the full directory path and file name of the file to copy, and the file name to use for storing the copy of the configuration file to the Wi-Fi Switch (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 Wi-Fi Switch using trivial file transfer protocol (TFTP). After entering this command, you are prompted to enter the hostname of the other device, the source file name to download, and the destination file name to use when saving it to the Wi-Fi Switch. A TFTP server must be running on the source device to enable the file transfer.

delete flash: <filename>

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

dir

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

write [memory]

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

write network flash:

This command saves the current configuration to the Wi-Fi Switch'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 System (boot system flash:)

The “boot system flash:” command is used to specify which software image file in the Wi-Fi Switch’s flash memory to use when rebooting the Wi-Fi Switch. When this command is entered, you are prompted to specify the name of this boot image. This allows you to update the Wi-Fi Switch’s software after downloading a new boot image. See **"Wi-Fi Switch Firmware Updates"** on page 163.

After using this command, be sure to save your configuration using the **write [memory]** command *before* rebooting the Wi-Fi Switch. When you then reboot the Wi-Fi Switch, it will load the new software image and the last stored startup-config configuration file.

Configure Clock

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)

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

crypto key generate <dsa|rsa|rsa1>

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

See **"ip ssh genkey"** on page 141 to enable secure shell operation on the Wi-Fi Switch. This command also provides regeneration of the encryption keys.

Configure EAP 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 in Your Client"** on page 77 for setting up clients to use EAP/PEAP.

See **"Configure No EAP Commands"** on page 123 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 Wi-Fi Switch. 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 2.4 GHz 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 Wi-Fi Switch 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 Wi-Fi Switch 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 >= Session Timeout, the Key Refresh Timeout is ignored.

(4) **VLAN Configuration** - 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 Wi-Fi Switch 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 Wi-Fi Switch. If there is no VLAN configuration for the client, then:

- (a) if there is default VLAN configured on the Wi-Fi Switch, 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 Wi-Fi Switch 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.

Wi-Fi Switch EAP Configuration Example

The following example shows how EAP may be configured on the Wi-Fi Switch to work with Windows 2000 IAS:

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

```
vivato (config)$ no eap
vivato (config)$ eap server 1 191.173.0.149 1812 3 5
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 Wi-Fi Switch. 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 network access device name. This is the name of the switch defined as the RADIUS server client for authentication.

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). 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 Commands

The following command is used to turn off EAP security. See **"Configure EAP Commands"** on page 120 for configuring EAP security.

no eap

Disable EAP 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 EAP security in order to stop authenticating through this server.

Configure Enable Secret

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

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

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

When enabled, the HTTP daemon provides access to the Wi-Fi Switch'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 Wi-Fi Switch'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 Wi-Fi Switch 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 Wi-Fi Switch. The bridge, Ethernet, VLAN, and Wireless interfaces all support DHCP server 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 Ethernet 0 interface (eth0) and the wireless interfaces (wlan1-wlan13) for wireless clients to communicate with the wired network.

An Ethernet or a wireless interface can only be assigned to one bridge. Therefore, you must first remove any Ethernet or wireless interfaces from the default bridge (br0) before they can be assigned to a new bridge.

add interface ethernet <0-3>

Enter the number of the Ethernet interface to add to 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.

no add interface wireless <1-13>

Remove the specified wireless interface from this 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 the name of the domain in which the DHCP server is operating.

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 for the default gateway to access the DHCP server.

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 server. Up to three time servers can be specified by issuing this command for each entry.

no dhcp-server ntp-server <ip address>

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

dhcp-server wins <ip address>

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

no dhcp-server wins <ip address>

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

exit

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

forward-time <4-200 seconds>

The forward time specifies how much time a bridge spends in the listening and learning states before forwarding a packet. This is used to prevent a bridge from starting to forward data packets over a link until the bridged network has been informed of the topology change and the affected links have been turned on or off.

If you set this value too low, loops can exist until the spanning tree algorithm protocol reconfigures the topology. Setting the value too high can cause delays until the spanning tree protocol reconfigures the topology. The default setting is 15 seconds.

no forward-time

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

hello-time <1-10 seconds>

The hello time is the period between the configuration messages generated by a root bridge. If you believe that configuration messages may be getting lost, shorten the hello time. To reduce the amount of overhead messages, increase the hello time. The default setting is 2 seconds.

no hello-time

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

ip address <ipaddress> <netmask> [secondary]

Enter an IP address and a subnet mask for the bridge. In the default configuration, an IP address is assigned to the default bridge (br0), which is the IP address that is used to access the Wi-Fi Switch. 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.

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.

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 Wi-Fi Switch’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.

no jail [add mac <mac address>]

Remove a MAC address from the list of clients authenticating through this interface to access a web page.

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

shutdown

Disable the bridge interface.

no shutdown

Re-enable the bridge interface.

stp

Enable spanning tree protocol (STP) on this bridge.

no stp

Disable spanning tree protocol on this bridge.

show <text>

See **"show interfaces bridge [0-4094]"** on page 108.

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 **"Connector Designations"** on page 17. 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 Operation

Refer to the bridge interface’s DHCP command descriptions for DHCP operation on any interface. See **"dhcp-server"** on page 125.

exit

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

ip address <ipaddress> <netmask>

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

Note: In most applications, an IP address does not need to be assigned to the ethernet interface. Instead, the IP address of the default bridge that bridges the Ethernet and wireless interfaces (bro) is typically used provide access to the Wi-Fi Switch. See **"interface bridge <0-4094>"** on page 124.

ip broadcast-address <ipaddress> [secondary]

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

ip address dhcp

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

no ip address dhcp

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

ip address dhcp renew

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

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface 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 Wi-Fi Switch'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 109.

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 !	After being created, a VLAN it is not enabled 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.

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.

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>

Set the forwarding entry aging time in seconds.

default

Enter this command to make this the default VLAN.

no default

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

DHCP Operation

Refer to the bridge interface’s DHCP command descriptions for DHCP operation on any interface. See **"dhcp-server"** on page 125.

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.

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.

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 Wi-Fi Switch’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|wirless 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|wirless 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 the 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>

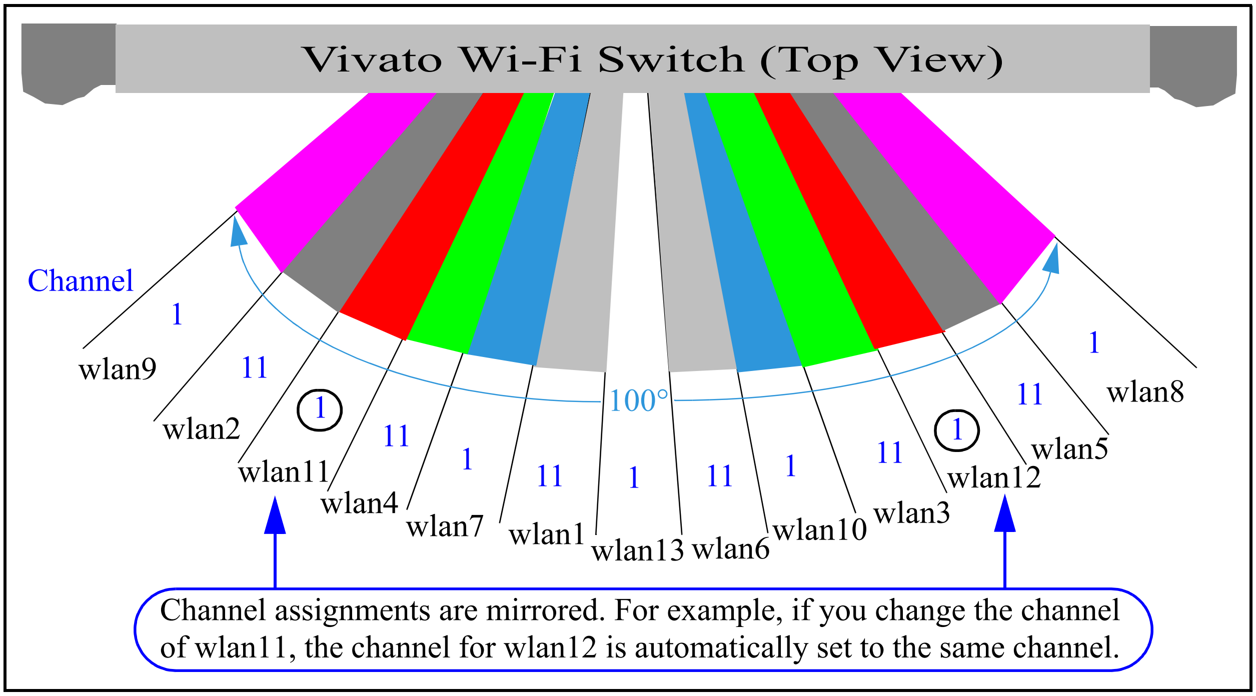
This command selects the wireless interface for configuration. The Wi-Fi Switch contains 13 fully configurable wireless interfaces. Each interface can be configured individually, or all interfaces can be configured as a group.

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.

Note: By default, wireless interfaces are bridged (using br0) 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 124.

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 automatically "mirrored" across the face of the Wi-Fi Switch. Therefore, any time you change a wireless interface channel (other than wlan13's channel) the channel assignment of the corresponding wireless interface on the opposite side of the Wi-Fi Switch is changed to match. The colors shown below illustrate the mirrored channel settings.



Channel assignments are mirrored. For example, if you change the channel of wlan11, the channel for wlan12 is automatically set to the same channel.

Figure 61—Automatic Channel Assignment Mirroring Across the Wi-Fi Switch

Important

Under most circumstances, the default channel assignments shown above should be used, especially when using the Wi-Fi Switch in areas of heavy Wi-Fi traffic. Channel 6 can be used to provide three channel operation (along with channels 1 and 11) when Wi-Fi traffic is light.

DHCP Operation

Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface. See **"dhcp-server"** on page 125.

disable beacon-essid

This command prevents the ESSID from being sent in beacons issued by this wireless interface. Since the ESSID is no longer sent, clients cannot display it in their list of available networks and automatically send it in a response to try to associate. Therefore, only clients that have had the ESSID manually entered into their preferred wireless network list can associate with the Wi-Fi Switch. The default state is disabled, resulting in the ESSID being sent in beacons until this command is sent.

no disable beacon-essid

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

essid <text>

Enter an identifying name for the extended service set for this wireless interface. The name must be in the range of 1 to 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 ipaddress <ipaddress> <netmask>

Remove the IP address on this interface.

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 Wi-Fi Switch’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 -wlans)%** prompt: **key s:gmv8a18436572 1**

sensitivity <1-5>

Change the receiver sensitivity for this wireless interface: 1 = most sensitive (default), 5 = least sensitive. Under most conditions this value should be left at “1”. If the data rate for close-in clients is *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.

shutdown

Issuing this command disables the wireless interface.

no shutdown

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

no wep

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

show <text>

See **"show interfaces wireless <1-13> [associations]"** on page 112.

shutdown

Disables the ethernet interface indicated in 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 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. When WDS is enabled on a wireless interface, that interface can only be used for WDS. The default state is disabled.

wds <port (1-6)> <mac>

Enter a port number (1-6) *for this wireless interface*, and enter the MAC address of the wireless interface *on another Vivato Wi-Fi Switch*, for a wireless distribution system (WDS) connection between the two switches. Each wireless interface can support up to six (6) WDS connections.

WDS provides a wireless link between two Wi-Fi Switch's in order to provide Wi-Fi service to clients associating through another Wi-Fi Switch that is not connected to a wired backhaul. WDS must be configured on both Wi-Fi Switches to provide the link between them. The MAC address you enter in this command is the address of one of the wireless interfaces on the other Wi-Fi Switch used in the WDS link.

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.

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 Command

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 Wi-Fi Switch. No default domain name is configured.

ip host <hostname> [ipaddress]

Enter a host name (and optional IP address) to enter into the host table. Use the **"show ip host"** on page 112 to view the contents of the host IP table.

ip hostname <hostname>

Enter a host name for the Wi-Fi Switch 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 Wi-Fi Switch to route all IP datagrams destined for the 135.228.6.0/24 network through a gateway who's IP address is 135.228.4.203.

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 Wi-Fi Switch. 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 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 Wi-Fi Switch's memory. Use the **"show logging"** on page 113 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 PPTP Commands

The following commands are used to define point to point tunneling protocol (PPTP) settings. For more information on PPTP operation, see **"Point to Point Tunneling Protocol (PPTP) Operation"** on page 165.

Note: The PPTP daemon must first be started (using the **pptp** command) before PPTP can be configured and used.

pptp

Enable PPTP security by starting the PPTP daemon. The default state is disabled.

pptp auth <pap|chap|mschap|mschap-v2|radius>

Enter the name of the authentication scheme name used for point to point tunneling protocol (PPTP).

pptp chap-secrets <username> <password>

Enter the challenge handshake authentication protocol (CHAP) user name and password when using point to point tunneling protocol (PPTP).

Note: CHAP cannot be used if mppe-40 or mppe-128 encryption has been enabled. Use the **no pptp encryption <mppe-40|mppe-128>** command to turn encryption off.

pptp encryption <mppe-40|mppe-128>

Enter the type of Microsoft point to point encryption (MPPE) to use with the authentication server for point to point tunneling protocol (PPTP). The default is mppe-128.

Note: PAP or CHAP authentication cannot be enabled when using mppe-4 or mppe-128 encryption. If PAP or CHAP authentication is enabled, disable it using the **no pptp chap-secrets <username> <password>** and **no pptp pap-secrets <username> <password>** commands.

pptp listen <ipaddress>

This is the address that the PPTP daemon process listens on for new client connections. This address can either be a associated with a bridge or a VLAN. However, to use the default bridge (br0), you must assign a secondary IP address to that bridge and use that IP address as the listen address.

If PPTP is already enabled when this command is issued, it must be disabled (using the **no pptp** command) and re-enabled (using the **pptp** command) before this value takes effect.

pptp localip <ipaddress>

Enter the IP address within the Wi-Fi switch that wireless clients will connect to for backhaul access. This is the same IP address that devices on the Wi-Fi Switch’s backhaul use to access the Wi-Fi Switch. Unless a VLAN or another bridge is created and given an IP address, this is the IP address that is associated with the default bridge, br0.

If PPTP is already enabled when this command is issued, it must be disabled (using the **no pptp** command) and re-enabled (using the **pptp** command) before this value takes effect.

pptp msdns <ipaddress> [secondary]

Enter the IP address for the Microsoft® domain name service (DNS) server.You can assign a secondary MSDNS server using the optional [secondary] entry.

pptp mswins <ipaddress> [secondary]

Enter the IP address of a Microsoft Windows Internet Naming Service (MS-WINS) server to use when a server name is used when specifying a radius authentication server. You can assign a secondary MS-WINS using the optional [secondary] entry.

pptp pap-secrets <username> <password>

Enter the password authentication protocol (PAP) user name and password when using point to point tunneling protocol (PPTP).

Note: PAP cannot be used is mppe-40 or mppe-128 encryption has been enabled. Use the **no pptp encryption <mppe-40|mppe-128>** command to turn encryption off.

pptp radius-authserver <ipaddress|servername> <port number> <secret>

Enter the RADIUS authentication server's IP address or name, port number, and secret string in the range of 7 to 48 characters. The secret appears as clear text as it is entered.

pptp radius-authserver <ipaddress|servername> <port number> <ENTER> (prompt) <secret>

Enter the RADIUS authentication server's IP address or name and port number, and press the **Enter** key. You are prompted to enter the secret string in the range of 7 to 48 characters. The secret is not displayed as it is entered. The secret must be entered twice before it is changed.

pptp remoteip start <start ip address> end <2-254>

Enter the full IP start address, and the last three digits of the ending IP address, to assign to wireless clients. For example; **pptp remoteip start 10.0.3.156 end 180** would assign addresses 10.0.3.156 through 10.0.3.180 to wireless clients associating through the specified pptp listen address.

If PPTP is already enabled when this command is issued, it must be disabled (using the **no pptp** command) and re-enabled (using the **pptp** command) before this value takes effect.

Configure No PPTP Commands

The following commands are used to disable or remove point to point tunneling protocol (PPTP) configuration settings.

no pptp

Disable PPTP security.

no pptp auth <pap|chap|mschap-v2|radius>

Disable the authentication scheme used for point to point tunneling protocol (PPTP).

no pptp chap-secrets <username> <password>

Remove the challenge handshake authentication protocol (CHAP) user name and password used for point to point tunneling protocol (PPTP) operation.

no pptp encryption <mppe-40|mppe-128>

Disable the encryption name used by the authentication server for point to point tunneling protocol (PPTP).

no pptp listen <ipaddress>

Enter the IP address within the Wi-Fi switch to disable the pptp daemon process that listens for new client connections.

no pptp localip <ipaddress>

Disable the IP address within the Wi-Fi switch where the wireless clients are connected to.

no pptp msdns <ipaddress>

Enter the IP address of the domain name server (DNS) to disable for point to point tunneling protocol (PPTP) operation.

no pptp mswins <ipaddress> [secondary]

Enter the IP address of a Microsoft Windows Internet Naming Service (MS-WINS) server to disable its use when a server name is used when specifying a radius authentication server. Use the optional [secondary] entry to disable the secondary MS-WINS server.

no pptp pap-secrets <username> <password>

Remove the password authentication protocol (PAP) user name and password used for point tunneling protocol (PPTP) operation.

no pptp radius-authserver <ipaddress> <port number> <secret>

Enter the IP address, port number, and the secret associated with a RADIUS authentication server to disable authentication through that server.

no pptp radius-authserver <server name> <port number> <secret>

Enter the RADIUS authentication server name, port number, and its secret to disable authentication through that server.

no pptp remoteip <ipaddress>

Disable the IP addresses that can be assigned to wireless clients, either as an individual IP address or as a contiguous range, such as 1.2.3.10-50.

Configure RAPD

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 Wi-Fi Switch. These access points can interfere with the operation of the Wi-Fi Switch, 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 community <community name> RO|RW [<source ip address>]

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

snmp-server contact <text>

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

snmp-server engineID <engine identifier>

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

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

Use this command to create a trap sink for SNMP version 1. Enter the host name or IP address and the community name. See **Table 6—Examples for Creating Traps/Informs Sinks on page 146**.

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 146**.

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 146**.

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
Create a user named “lrs” with authentication and with encryption that uses it's own password	snmp-server user lrs auth MD5 12345678 priv DES 23456789

Configure No SNMP-Server Commands

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

no snmp-server

Disables the SNMP daemon.

no snmp-server community <community name>

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

no snmp-server contact

Deletes the SNMP contact information.

no snmp-server engineID

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

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

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

no snmp-server location

Deletes the SNMP location information.

no snmp-server name

Deletes the SNMP name information

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

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

Configure Username Admin (Read Level) Secret

The read level secret is used to access the Wi-Fi Switch 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 Vivato Packet Shaping

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

vps

Enable packet shaping. The default state is enabled.

no vps

Disable packet shaping.

disable

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

edit flash:

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

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

exit

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

no <configuration command>

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

reboot

Issuing this command causes the Wi-Fi Switch to be reset, and powers on using the last saved configuration. See **write network fla sh:** or **"write [memory]"** on page 118 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.*

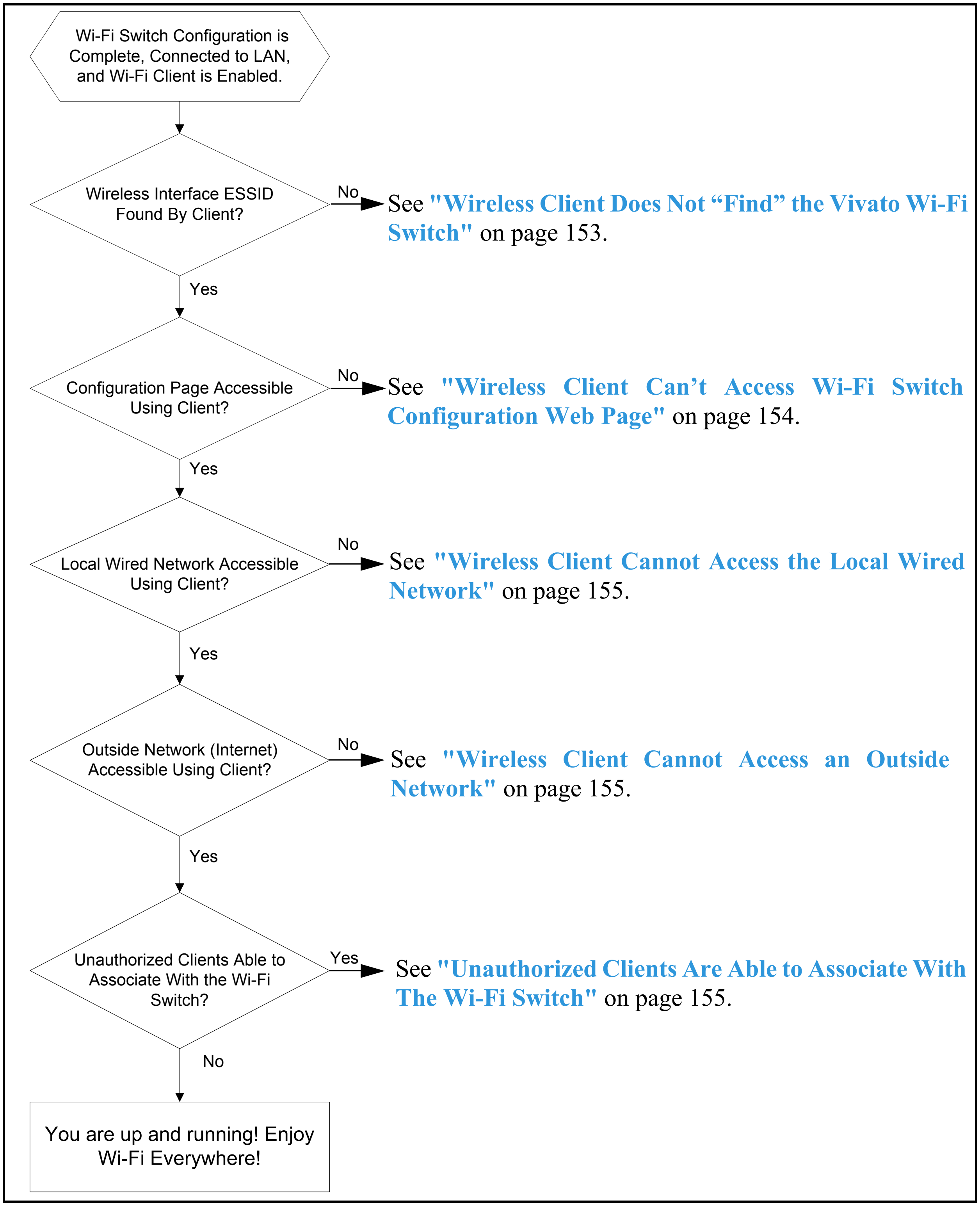
Verifying Wi-Fi Operation

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

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

Verification Process

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


Wi-Fi Switch Configuration is Complete, Connected to LAN, and Wi-Fi Client is Enabled.
Wireless Interface ESSID Found By Client?
No
Yes
Configuration Page Accessible Using Client?
No
Yes
Local Wired Network Accessible Using Client?
No
Yes
Outside Network (Internet) Accessible Using Client?
No
Yes
Unauthorized Clients Able to Associate With the Wi-Fi Switch?
Yes
No
You are up and running! Enjoy Wi-Fi Everywhere!

See "Wireless Client Does Not “Find” the Vivato Wi-Fi Switch" on page 153.

See "Wireless Client Can’t Access Wi-Fi Switch Configuration Web Page" on page 154.

See "Wireless Client Cannot Access the Local Wired Network" on page 155.

See "Wireless Client Cannot Access an Outside Network" on page 155.

See "Unauthorized Clients Are Able to Associate With The Wi-Fi Switch" on page 155.

Figure 62—Wi-Fi Switch Verification Flowchart

Wireless Client Does Not "Find" the Vivato Wi-Fi Switch

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

- The Wi-Fi Switch's power LED must indicate that the switch is operating. See **"Connections to the Vivato Wi-Fi Switch"** on page 17.
- The Wi-Fi Switch's wireless interfaces must be enabled and their ESSID specified. If only a portion of the wireless interfaces have been enabled, the Vivato Wi-Fi Switch will not be transmitting through its entire 100° pattern. See **"Wireless Interfaces"** on page 56.
- To ensure access, the client should be within the antenna pattern of the Wi-Fi Switch. See **"Wireless Interfaces"** on page 56.
- Your Wi-Fi client is configured and working correctly. Refer to your client's documentation.

Variations in Client Performance Due to Physical Orientation

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

If you are in an area that is partially blocked from the Wi-Fi Switch's antenna pattern, try rotating the client 90 degrees (horizontally) to see if your reception is improved.

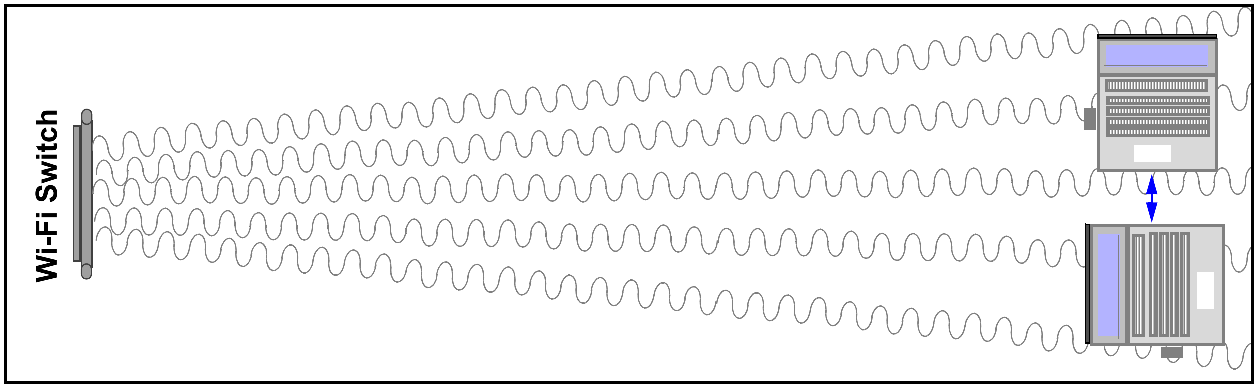


Figure 63—Rotating the Client to Improve Performance

Wireless Client Can’t Access Wi-Fi Switch Configuration Web Page

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

- The correct Address/Location must be specified in your web browser. See **"Configuration Connections"** on page 37.
- The security settings for your client and the Wi-Fi Switch must match. If you enabled security (such as WEP) in the Wi-Fi Switch, and your client’s security settings are not providing access to the Wi-Fi Switch, you must use a wired connection to the Wi-Fi Switch to access the configuration web page and match the security settings between the switch and your client. See **"Configuration Connections"** on page 37.
- The level of interfering signals must not be so great that the lowest allowed data rate (1 Mbps) cannot be used. Verify that Wi-Fi access points using the same channel assignments as the Wi-Fi Switch are not in close proximity. Also make sure that one or more microwave ovens are not operating within the Wi-Fi Switch’s coverage area for channel 6. See **"Wireless Interfaces"** on page 56 and **"Interfering Signal Sources"** on page 7.

Wireless Client Cannot Access the Local Wired Network

If you are able to access the Vivato Wi-Fi Switch's configuration web page using your wireless client but you are unable to access the wired network connected to the switch's Ethernet LAN port, verify that the following conditions are present:

- The default bridge between the Ethernet and wireless interfaces (br0) is enabled, or you have created a VLAN for carrying traffic. See **"Network Settings"** on page 55.

Your wired network is connected to the Wi-Fi Switch's LAN port. See **"Connections to the Vivato Wi-Fi Switch"** on page 17.

- The LAN port (eth0) has been enabled. The Vivato Wi-Fi Switch is pre configured with the LAN port enabled. See **"Ethernet Interfaces"** on page 55.
- The Vivato Wi-Fi Switch has been entered in the list of permissions for your local area network (LAN) server. If your server uses an access list to allow access to the network, make sure that the Wi-Fi Switch has been added to that list.
- When authenticating through a RADIUS service, the RADIUS configuration information must be correctly entered. See **"EAP"** on page 69.

Wireless Client Cannot Access an Outside Network

If you are able to connect to your local network through the Vivato Wi-Fi Switch, 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 **"EAP"** on page 69.
- The correct default gateway must be specified. See **"Basic Network Setup"** on page 46.

Unauthorized Clients Are Able to Associate With The Wi-Fi Switch

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

Network Monitoring

Three methods can be used to monitor Vivato Wi-Fi Switch 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 79.
- 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 97.
- Simple network management protocol (SNMP)

SNMP Operations

You can use third-party SNMP management software to monitor operations within the Vivato Wi-Fi Switch. These software packages are designed to use standard SNMP versions that have been defined to work with devices created by various manufacturers. The Wi-Fi Switch 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. The following MIBs are provided on the Wi-Fi Switch's CD-ROM in the MIBs directory:

Pre-release Operating Considerations

Not all MIB objects are supported in this pre-release version of the Vivato Wi-Fi Switch. 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 Wi-Fi Switch CD. Operating limitations for each MIB are relevant for this firmware release, but may not be present in future firmware releases.

80211-MIB.txt

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

- The following are not supported:
- dot11AuthenticationAlgorithmsTable
- dot11WEPDefaultKeysTable
- 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:

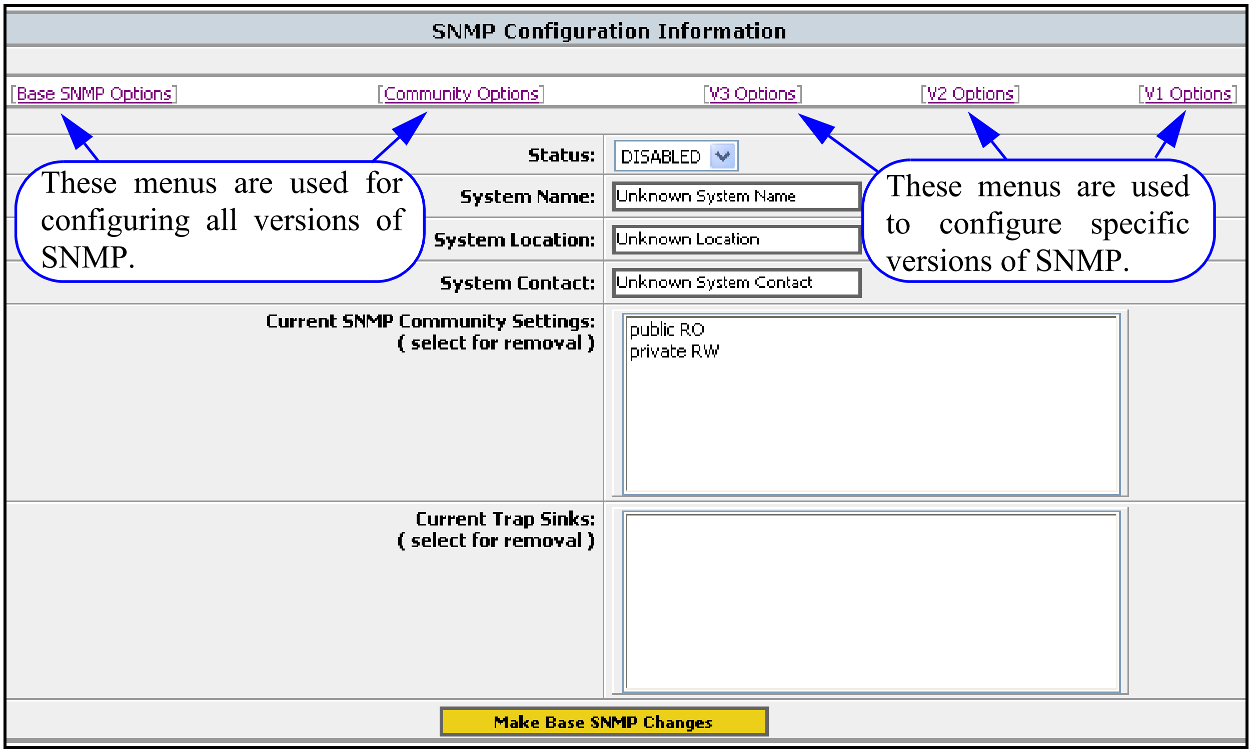
- snmpUsmMIB
- snmpVacmMIB

Enabling SNMP Operation

To use SNMP in the Wi-Fi Switch, 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 145 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

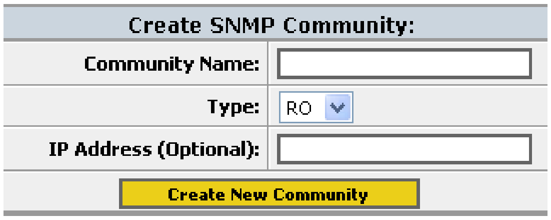
These menus are used for configuring all versions of SNMP.

These menus are used to configure specific versions of SNMP.

Status:	DISABLED
System Name:	Unknown System Name
System Location:	Unknown Location
System Contact:	Unknown System Contact
Current SNMP Community Settings: (select for removal)	public RO private RW
Current Trap Sinks: (select for removal)	

Figure 64—**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.

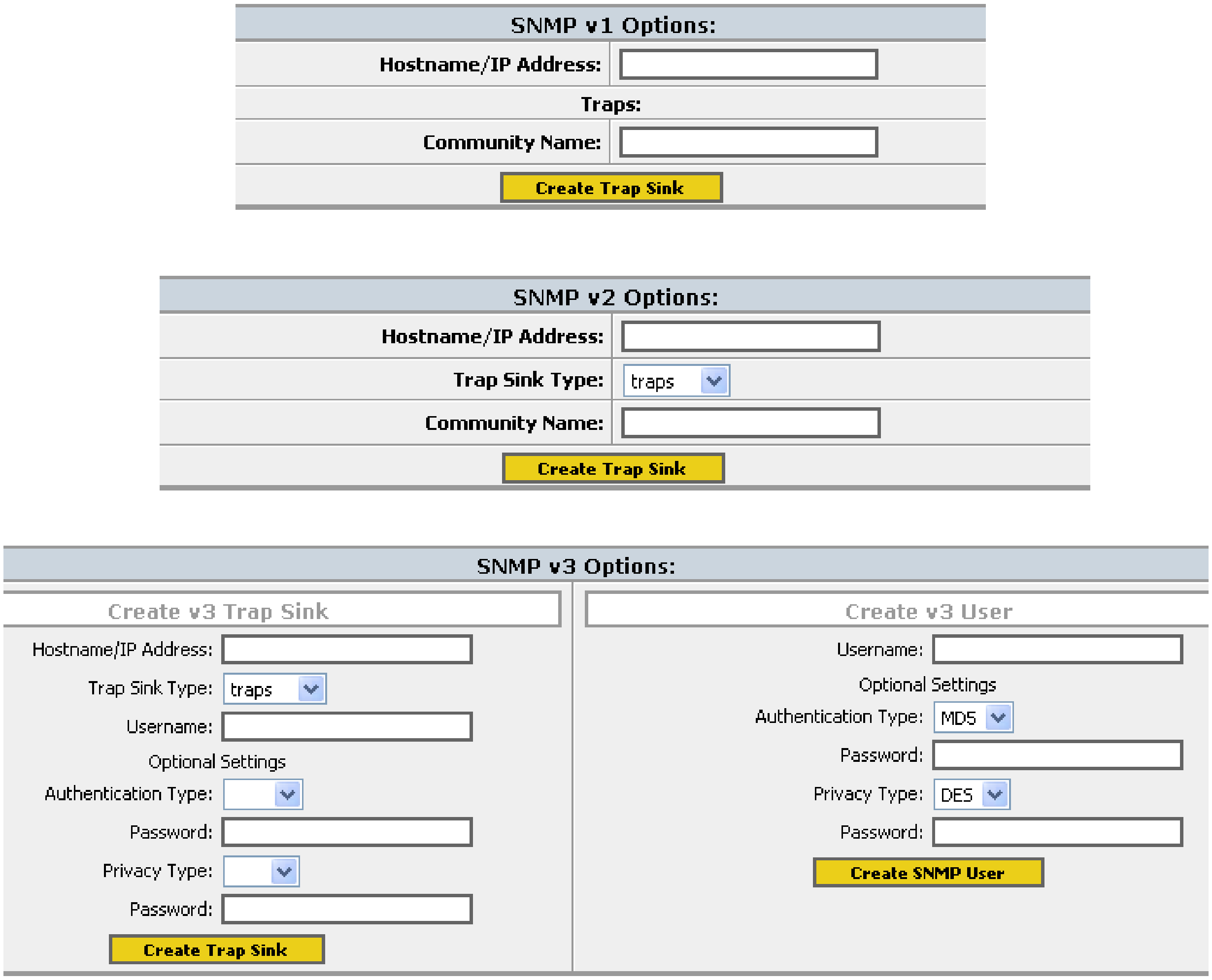


Create SNMP Community:

Community Name:
Type: RO
IP Address (Optional):

Figure 65—**Creating an SNMP Community**

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



SNMP v1 Options:

Hostname/IP Address:
Traps:
Community Name:

SNMP v2 Options:

Hostname/IP Address:
Trap Sink Type: traps
Community Name:

SNMP v3 Options:

Create v3 Trap Sink

Hostname/IP Address:
Trap Sink Type: traps
Username:
Optional Settings
Authentication Type:
Password:
Privacy Type:
Password:

Create v3 User

Username:
Optional Settings
Authentication Type: MD5
Password:
Privacy Type: DES
Password:

Figure 66—**Specifying Settings for SNMP Versions 1, 2c, and 3**

Wi-Fi Switch Firmware Updates

Firmware updates in the Wi-Fi Switch provide additional functions and improve overall operation. All firmware images are in binary (.bin) format.

The latest firmware can be downloaded from the Vivato.net/Support web page. You can use the web interface or the command line interface (CLI) to perform the update. See **"Firmware"** on page 91 for information on using the web interface to update the firmware.

Important	The Wi-Fi Switch can contain a maximum of two firmware images. If two images already exist in memory, you need to remove one of the images (typically the older image) before loading a new image. To see what images have already been downloaded, use the **show flash:** CLI command. To delete an old image, use the **delete flash: <filename>** command.

Firmware Update Process Using the Command Line Interface

Use these steps to update the software in your Wi-Fi Switch:

Step 1. Using a web browser, download the new software image file from the Vivato support website onto a local computer on your network. Go to http://www.vivato.net , select the *Customer Support* link, and enter your user name and password.

Caution	The Wi-Fi Switch defaults to using an image named “vino.bin”. However, do not rename the firmware image you are going to download “vino.bin”. Otherwise, if the file transfer is somehow interrupted or corrupted, your Wi-Fi Switch may no longer have a boot-able image in it as a result.

Step 2. Use the **copy scp: flash:** command to copy the software image file from the local computer to the Wi-Fi Switch’s flash memory. Alternatively, you can use the **copy tftp: flash:** command with a TFTP server to transfer the file, but it typically takes much longer than the “copy scp: flash:” method.

Step 3. Use the **Configure System (boot system flash:)** command to tell the Wi-Fi Switch that you want to use the new image when rebooting the Wi-Fi Switch.

Step 4. Use the **write [memory]** command to save the current configuration.

Step 5. Reboot the Wi-Fi Switch using the **reboot** command. The configuration that you saved tells the Wi-Fi Switch to reboot using the new firmware image.

Firmware Update Example

This example copies a downloaded image file (“vino_1_2_5.bin”) into the Wi-Fi Switch’s flash memory using the name “vino125.bin”. Once the file is transferred, the Wi-Fi Switch is configured to use the new image and is rebooted.

```
Vivato#
Vivato#copy scp: flash:
Username: gerry
Password:
Hostname: 195.162.0.240
Directory [/]: vivato/images
Source file: vino_1_2_5.bin
Destination file vino_1_2_5.bin]: vino125.bin
The authenticity of host '195.162.0.240 (195.162.0.240)' can't be established.
RSA key fingerprint is fc:35:59:7e:e9:62:ae:b5:6f:2d:29:3a:b2:a3:bb:a0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '195.162.0.240' (RSA) to the list of known hosts.
vino1_2_5 100%
|*****************************************************************************| 4795 KB   0:54
Vivato#
```

Enter the “copy scp: flash:” command, and enter the user name, password, and file information needed for the Wi-Fi Switch to access the downloaded image file on your network.

```
Vivato#show flash
-rw-------    1 root     root          668 Jan  1 00:01 ssh_host_dsa_key
-rw-r--r--    1 root     root          601 Jan  1 00:01 ssh_host_dsa_key.pub
-rw-------    1 root     root          526 Jan  1 00:00 ssh_host_key
-rw-r--r--    1 root     root          330 Jan  1 00:01 ssh_host_key.pub
-rw-------    1 root     root          887 Jan  1 00:01 ssh_host_rsa_key
-rw-r--r--    1 root     root          221 Jan  1 00:01 ssh_host_rsa_key.pub
-rw-r--r--    1 root     root         1507 Jan  1  1970 startup-config
-rw-r--r--    1 root     root      4910296 May  8  2003 vino.bin
-rw-r--r--    1 root     root      4910296 Jan  1  1970 vino125.bin
Vivato#
```

You can use the “show flash” or “dir” command to verify that the image was loaded into the Wi-Fi Switch using the “destination” name that you specified.

```
Vivato#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Vivato(config)#boot system flash:
Boot image [vino.bin]: vino125.bin
Vivato(config)#exit
Vivato#write
Writing configuration...
OK
Vivato#reboot
Vivato#
```

Use the “boot system flash:” command to tell the Wi-Fi Switch to use the new image.

Use the “write” command to store the new boot configuration.

Use the “reboot” command to reboot and start using the new image.

Point to Point Tunneling Protocol (PPTP) Operation

Point to point tunneling protocol provides a secure virtual private network (VPN) “tunnel” between a Wi-Fi client and the Vivato Wi-Fi Switch. Variations of PPTP configurations allow the Wi-Fi Switch to use local authentication, shared passwords and user names stored in the Wi-Fi Switch, or remote authentication with a RADIUS server.

Note: PPTP secures the connection between the Wi-Fi client and the Vivato Wi-Fi Switch, but does not ensure security between the Wi-Fi Switch and your local wired network. It is assumed that your wired network has been configured to provide a secure path to the Wi-Fi Switch’s wired Ethernet backhaul.

The PPTP tunnel has IP address endpoints that reside on the subnet of the Wi-Fi Switch’s backhaul (eth0). The traffic carried in this tunnel between the client and the Switch is encrypted and encapsulated as generic routing encapsulation (GRE) packets.

When used with MS-CHAPv2, encryption is either mppe-40 or mppe-128 (better security). The shared key for each client can be stored locally in the Wi-Fi Switch’s configuration, and/or stored in a RADIUS server located anywhere that is reachable from the backhaul network.

Authentication of the client may be performed using password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), or Microsoft CHAP version 2 (MS-CHAPv2). MS-CHAPv2 provides the greatest level of security.

PPTP Configuration

PPTP requires the creation of a bridge to be used as the tunnel for transferring packets between the wireless interfaces and the LAN (eth0) port. The bridge can be created by configuring a virtual local area network (VLAN) or by assigning a secondary IP address to the existing default bridge, br0.

If a VLAN is used, the media access control (MAC) of each client must be added to the bridge before that client is allowed to associate.

Creating a Bridge Using a VLAN

When a VLAN is created, a bridge is created with the same numeric ID of the VLAN, and aliases of each ethernet and wireless interface you added to that VLAN are created. For example, when creating a VLAN with an ID of 3 that includes ethernet 0 and wireless interface 1, a bridge is created from eth0.3 to wlan1.3. By assigning an IP address to this VLAN, you create the “listen” address for the PPTP tunnel. This process is shown in the following example (the “show” command is only used in this example to show that the bridge was created):

```
Vivato(config)#interface vlan 3
Vivato(config-vlan3)#add interface ethernet 0
Vivato(config-vlan3)#add interface wireless 1
Vivato(config-vlan3)#ip address 192.168.5.1 255.255.255.0
Vivato(config-vlan3)#show interfaces vlan 3
vlan3     Link encap:Ethernet  HWaddr 00:0B:33:01:05:69
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST 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:8000.000b33010569, STP:Disabled
          Interface: eth0.3, wlan1.3

Vivato(config-vlan3)#
```

After creating the VLAN, each client associating through the VLAN must be added. The following example shows how the MAC addresses of three different clients are added to VLAN 3:

```
Vivato(config-vlan3)#add mac 00:02:3d:23:4a:50
Added MAC[00:02:3d:23:4a:50] to VLAN:3
Vivato(config-vlan3)#add mac 00:02:3d:a4:98:ab
Added MAC[00:02:3d:a4:98:ab] to VLAN:3
Vivato(config-vlan3)#add mac 00:03:31:2c:87:2b
Added MAC[00:03:31:2c:87:2b] to VLAN:3
Vivato(config-vlan3)#
```

Specifying a Secondary IP Address for the Default Bridge

Assigning a secondary IP address is another way to provide the PPTP tunnel. When assigning a secondary IP address to the default bridge (br0), be sure to use an IP address that is on a different subnet from the primary IP address. For example, if the default IP address of bridge br0 is used (169.254.20.1), use a different value for the secondary IP address, such as 192.165.2.225.

Use the **ip address <ipaddress> <netmask> [secondary]** to assign a secondary IP address on a bridge.

Example Configuration

The configuration example illustrated below consists of two clients that associate to the Wi-Fi Switch on VLAN 8, which is on subnet 192.168.5/24. There is nothing special about these selections - any VLAN could be used and the subnet could be anything in the private address space available.

In this example, the association VLAN is isolated from everything else, and only traffic from the tunnel (which is on a different subnet) will be present on the backhaul.

The backhaul is on another VLAN (VLAN 3), with a subnet 10.0.3/24. Any VLAN (other than 8) could be used and any private address space other than the subnet used by VLAN 8 could be used.

After a client has been authenticated, an IP address that is within the backhaul's subnet is given to the client (such as 10.0.3.7, in this example). When configuring PPTP using the CLI, this is one of the addressees specified using the pptp remoteip command.

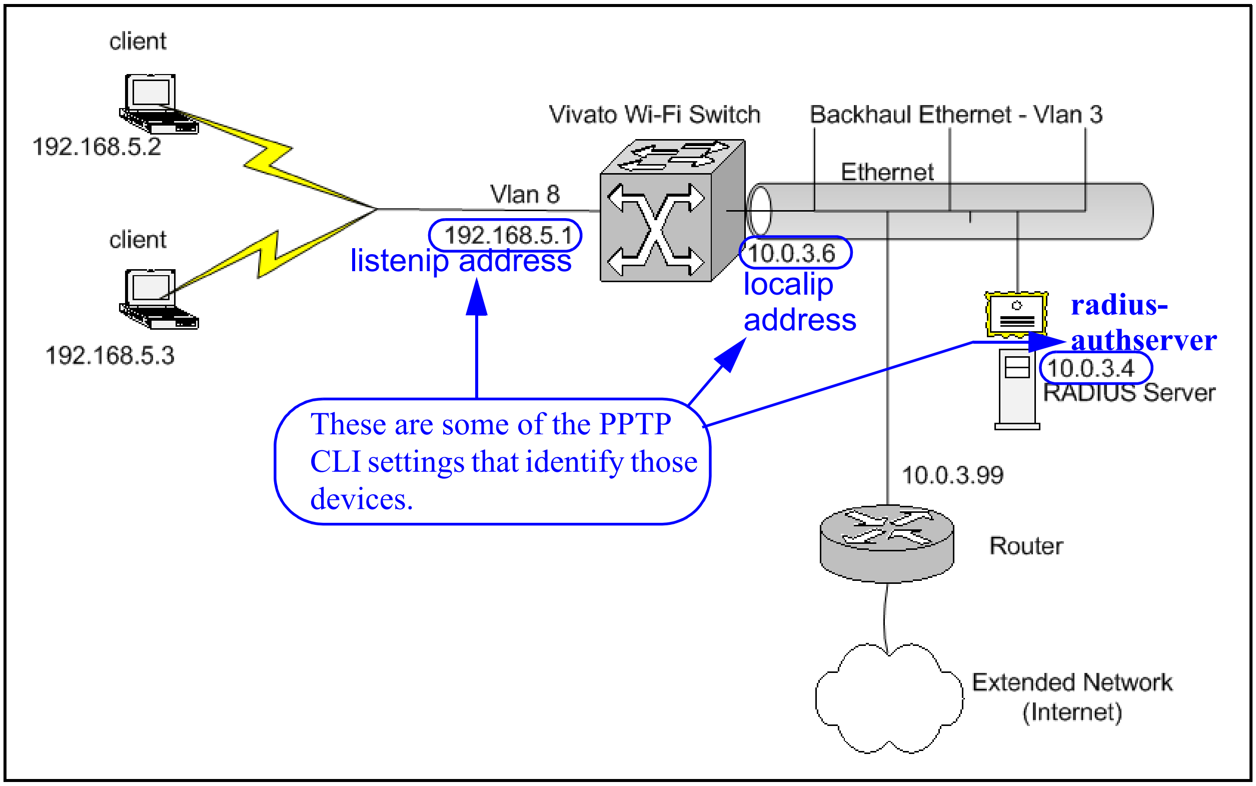


Figure 67—Example PPTP Configuration Using VLANs

Configuring PPTP in Clients

For PPTP operation, the Wi-Fi client's TCP/IP settings must be configured to use a static IP address that is within the subnet of the "tunnel". In the example above, the Wi-Fi client's IP address would be set within the 192.168.5/24 subnet. To do this, go to **Start>Settings>Network Connections** and right-click on the "**Wireless Network Connection**" entry. Select "**Properties**" and configure the "**Internet Protocol (TCP-IP)**" properties to use the static IP address.

The New Connection Wizard in Microsoft Windows is used to set up the 802.11b client for PPTP operation. The wizard is started by going to **Start>Settings>Network Connections** and selecting "Create a new connection".

When using the wizard, be sure to specify the correct settings for the type of PPTP operation being used, and set the destination IP address for the connection to the same IP address set up as the listen

IP address in the Wi-Fi Switch's PPTP setup. When finished, a connection icon for your PPTP configuration is placed in the Virtual Private Network area of the Network Connections.

When using PPTP, you need to first enable the Wi-Fi client and select the Wi-Fi Switch's ESSID from the list of available networks. After a connection is established between the Wi-Fi Switch and the client, the connection details for your wireless client will show that it is using the IP address that was statically assigned to it.

Once the connection to the Wi-Fi Switch is completed, start your PPTP client to connect to the wired network through the Wi-Fi Switch using PPTP. When this is accomplished, the connection details for your wireless client will indicate the IP address that was assigned to the client for that PPTP session (an IP address in the range of the remote IP addresses you configured in the Wi-Fi Switch for PPTP operation).

Index