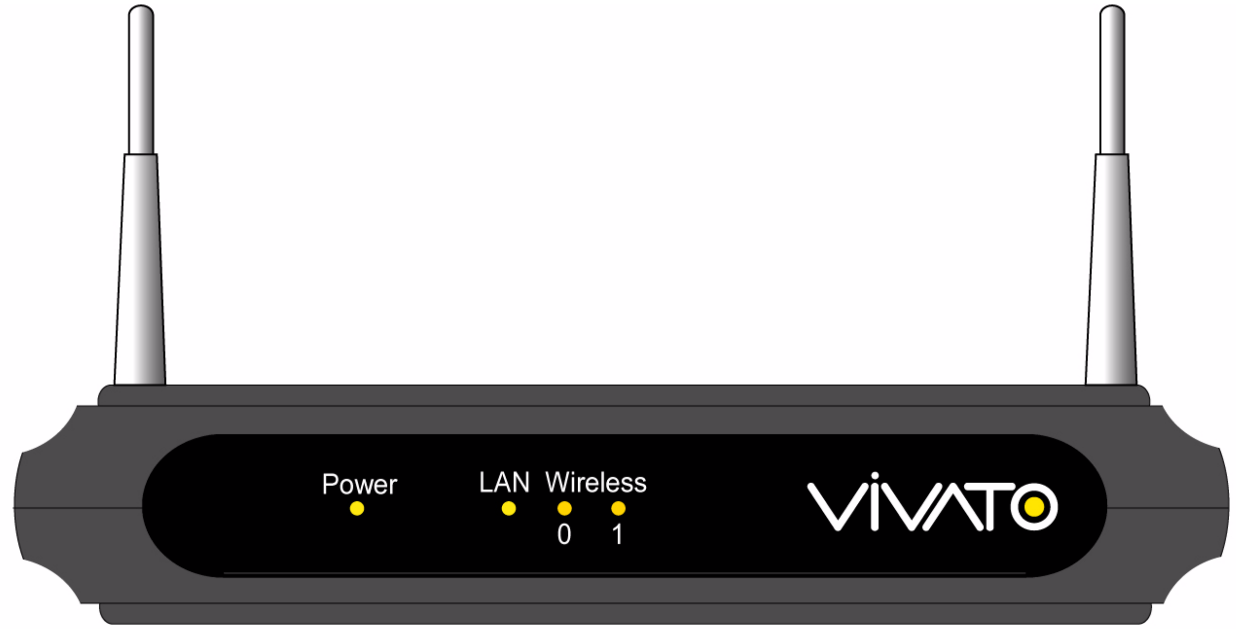
VA4200 AP/Bridge User Guide

Manual P/N: 770-01588-02
Release 2.1
May 5, 2005



The content of this manual is furnished for informational use only, and is subject to change without notice. Vivato, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual.

Documentation Updates

The most current documentation and firmware for this Vivato product is available on the Vivato Customer Support website. See “Contact Information” on page 13.

VIVATO, INC. END USER LIMITED WARRANTY AND LICENSE TERMS

Limited Warranty

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

REMEDY

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

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

LIMITATIONS OF WARRANTY

This warranty does not apply to Product or Software which fails to perform as warranted due to: (a) improper handling, installation, removal, repair, maintenance, abuse or improper use; (b) damage caused by vandalism, severe weather, lightning, chemical hazards, fire, contact with high-voltage power lines or other electrical stress; (c) repairs, modifications, or any alterations performed or attempted by End User or any third party, unless authorized by Vivato as stated below; (d) use in conjunction with equipment which is not compatible with Product or Software; (e) documentation errors; (f) software errors; or (g) Product or Software provided to End User for evaluation, testing, demonstration or other purposes for which Vivato does not receive payment of purchase price or license fee.

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

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

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

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

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

LIMITATION OF LIABILITY

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

END USER LICENSE

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

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

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

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

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

3. **Proprietary Rights**. End User acknowledges that all patents, copyrights, trade secrets, trade names, trademarks, and all other intellectual property rights in or related to the Product and Software are the exclusive property of Vivato and its licensors (if any). No right, title or interest, expressed or implied, in or to the Product or Software, including without limitation patent, copyright, trade secret or other intellectual property rights therein, other than the limited license granted above, is transferred from Vivato to End User. Title to and ownership of the Software shall remain with Vivato and its licensors (if any). End User shall not alter or erase any copyright, confidential or proprietary notices appearing on the Product, Software or related documentation.

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

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

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

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

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

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

Contents

Documentation Updates 2

About This Document. 14

User and Developer Audience 14

Online Help Features 14

Guidance on Configuring the AP/Bridge with Recommended Settings. 14

Typographical Conventions 15

Introduction. 16

Overview of the Vivato Wi-Fi AP/Bridge 16

Features and Benefits 17

Indicators and Connectors 18

What's Next? 19

PreLaunch Checklist: Default Settings and Supported User/Client Platforms 20

Vivato Wi-Fi AP/Bridge. 20

User's Computer. 22

Wireless Client Computers. 23

Understanding Dynamic and Static IP Addressing on the Vivato Wi-Fi AP/Bridge. 25

Quick Steps for Setup and Launch of Your Wireless Network 26

Step 1. Install the AP/Bridge 26

Step 2. Set the PC's Network Interface to Talk to the AP/Bridge 26

Step 3. Log in to the VivatoVision Web Pages 27

Step 4. Configure the Basic Settings 28

Step 5. Specify the IP Address and Security Settings for the Primary Wireless Network. 29

Step 6. Configure the Default Gateway and DNS Nameserver IP Addresses 30

Next Steps. 31

Installation 32

Shipping Contents. 32

Environmental Considerations 32

Mounting Weight Considerations. 32

Powering the VA4200 33

Positioning The VA4200 33

Mounting the VA4200 37

Preparing the VA4200 for Operation 37

Configuring Basic Settings. 38

Navigating to Basic Settings. 38

Review / Describe the AP/Bridge. 39

Specify a New User Password and the Wireless Network Name. 40

Update Basic Settings. 41

Global Network Settings 42

Navigating to Global Network Settings 42

Specifying the Default Gateway. 42

Specifying the DNS Nameservers 43

Updating Settings 43

Setting Interface IP Addresses. 44

Managing User Accounts 45
Navigating to User Management 46
Viewing User Accounts 46
Adding a User 46
Editing a User Account 47
Enabling and Disabling User Accounts 47
Removing a User Account 48

Enabling the Network Time Protocol Server 49
Navigating to Time Protocol Settings. 49
Enabling or Disabling a Network Time Protocol (NTP) Server 50
Updating Settings 50

Configuring Radio Settings 51
Understanding Radio Settings 51
Navigating to Radio Settings 51
Configuring Radio Settings 52
Updating Settings 55

Viewing the Wireless Interface Settings 56
Navigating to Wireless Settings 56

Controlling Access by MAC Address Filtering 57
Navigating to MAC Filtering Settings 57
Using MAC Filtering 58
Updating Settings 58

Configuring Queues for Quality of Service (QoS) 59
Understanding QoS 59
Navigating to QoS Settings. 62
Configuring QoS Queues 63
Updating Settings 65

Configuring the Wireless Distribution System (WDS) 66
Understanding the Wireless Distribution System 66
Navigating to WDS Settings. 68
Configuring WDS Settings 69
Updating Settings 71

Setting the User Password 72
Navigating to Administrator Password Setting 72
Setting the User Password 72
Updating Settings 73

Maintenance and Monitoring 74
Interfaces. 74
Event Log 75
Transmit/Receive Statistics. 76
Associated Wireless Clients 77
Rebooting the AP/Bridge 77
Resetting the Configuration 79
Upgrading the Firmware 80
Rogue Access Points. 82

Creating and Managing Multiple Networks (SSIDs) 85
Using SSIDs with VLANs to Create Logically Separate Networks. 85
Navigating to Current SSID Settings 86
Creating and Editing SSIDs 87
Updating Settings 88

Automatic VLAN Assignment 89

Specifying the Management Interface(s) 90
Navigating to the Management Interfaces Settings 90
Updating Settings 90

Configuring Security 91
Understanding Security Issues on Wireless Networks 91
Navigating to Security Settings 97
Configuring Security Settings. 97
Updating Settings 109

Simple Network Management Protocol (SNMP) 110
Navigating to SNMP Settings. 110
. . . . 111
Updating Settings 111

Enabling Logging 112
Navigating to Log Server Configuration Settings 112
. . . . 113
Updating Settings 113

System Recovery and File System Commands. 114
Restoring the Default Administrator Password 114
Restoring the Default AP/Bridge Configuration 115
Linux Commands 117

Appendix A. Configuring Security Settings on Wireless Clients 120
Make Sure the Wireless Client Software is Up-to-Date 121
Accessing the Microsoft Windows Wireless Client Security Settings 122
Configuring a Client to Access an Unsecure Network (Plain Text mode) 124
Configuring Static WEP Security on a Client 125
Configuring IEEE 802.1x Security on a Client 127
Configuring WPA with RADIUS Security on a Client 133
Configuring WPA-PSK Security on a Client 140
Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/Bridge 142
Obtaining a TLS-EAP Certificate for a Client 145
. . . . 148

Appendix B: Assessing Traffic and Interference 149
ISM-Band Channel Spacing 149
Sources of Noise and Interference 150
Determining if a Signal is Strong Enough to Affect Wi-Fi Operation 154
Measuring Interfering Signal Levels 154

Glossary 156

Safety Information

You must heed any and all safety precautions and warnings in this document or indicated on the Vivato VA4200 Wi-Fi AP/Bridge whenever you are operating or servicing this product. Failure to comply with all precautions and warnings found in this document violates the design, manufacture, and intended use requirements of the product. Vivato, Inc. assumes no liability for the operator's failure to obey these warnings and cautions.

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

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

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

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

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

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

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

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

Maintenance

There are no user serviceable components or adjustments in Vivato equipment.

The normal course of care and maintenance for electrical equipment should be followed for all Vivato equipment. The following should be performed on a semi-annual basis:

1. Inspection of housing for signs of external damage, such as a torn radome, dented or breached housing, or other external damage.

2. Inspection of mounting hardware for missing fasteners, loose fasteners, excessive corrosion, or changes in mounting orientation.

3. Inspection of ventilation holes for blockage.

4. Inspection of cables for proper stress/strain relief and drip loop (if required).

5. Inspection of cables for any signs of fraying, wear, or damage.

Any of the above conditions could lead to failure or reduced performance and should be rectified as soon as possible.

FCC Declaration of Conformity

Responsible Party
Manufactured by Vivato, Inc.
12610 E Mirabeau Parkway, Suite 900
Spokane, WA, USA
Phone: (509) 343-6001, Fax (509) 343-6020

Product: VA4200 Wi-Fi AP/Bridge
This product is certified for home or office use.

The Vivato VA4200 Wi-Fi AP/Bridge 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 AP/Bridge should be at least 20 cm (7.8 in.) from people when operating using the supplied antennas.

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.

Contact Information

For customer support:

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

Go to www.vivato.com and select the **Customer Support** link. Enter the required information for setting up a user account. A support password is e-mailed to you after validating the information (usually within 1 business day). You can then search the online knowledge base for information by clicking on “**Find Answers / Questions**”. You can also access the latest firmware downloads and user documents from the support site.

To provide feedback on our documentation:

Feedback on the documentation shipped with the Vivato AP/Bridge is greatly appreciated, and will always be reviewed by our Technical Publications department. Please send your suggestions to **manuals_feedback@vivato.com**.

Gerry Caesar
Technical Publications
Vivato, Inc.

About This Document

This User Guide describes setup, configuration, administration and maintenance of a Vivato Wi-Fi AP/Bridge on a wireless network.

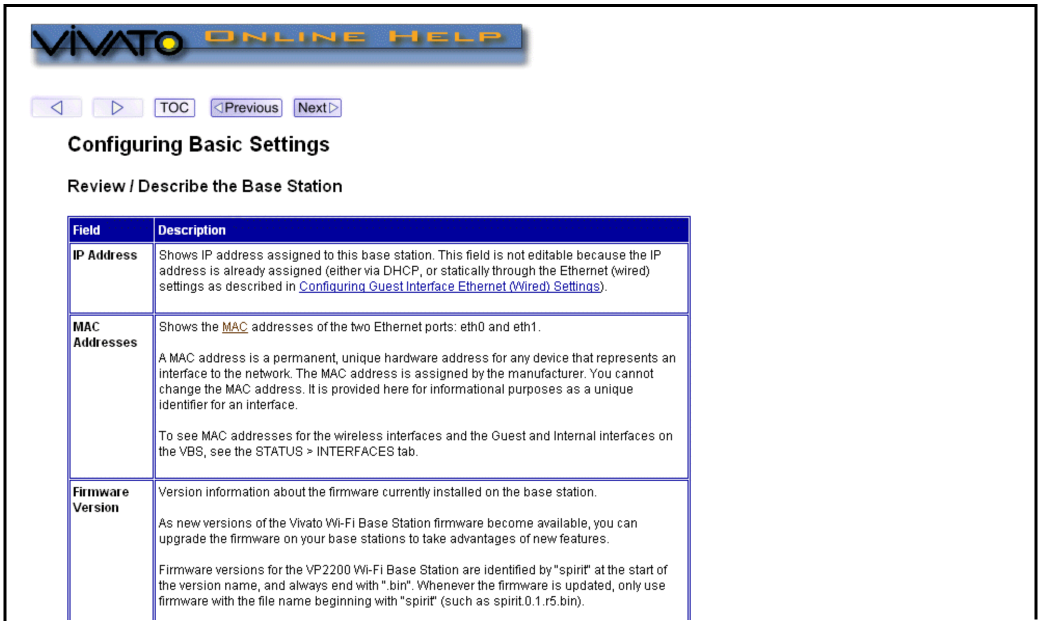
User and Developer Audience

This information is intended for the person responsible for installing, configuring, monitoring, and maintaining the Vivato Wi-Fi AP/Bridge.

Online Help Features

Online Help for the Vivato Wi-Fi AP/Bridge web user interface (UI) pages provides information about all fields and features available on the user interface. The information in the Online Help is a subset of the information available in the full User Guide.

Online Help information corresponds to each tab on the Vivato Wi-Fi AP/Bridge VivatoVision user interface. Click the **Help** button or the "More . . ." link at the bottom of the inline help panel on the UI for help information for the settings on the current tab.



Configuring Basic Settings

Review / Describe the Base Station

Field	Description
IP Address	Shows IP address assigned to this base station. This field is not editable because the IP address is already assigned (either via DHCP, or statically through the Ethernet (wired) settings as described in Configuring Guest Interface Ethernet (Wired) Settings).
MAC Addresses	Shows the MAC addresses of the two Ethernet ports: eth0 and eth1. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. To see MAC addresses for the wireless interfaces and the Guest and Internal interfaces on the VBS, see the STATUS > INTERFACES tab.
Firmware Version	Version information about the firmware currently installed on the base station. As new versions of the Vivato Wi-Fi Base Station firmware become available, you can upgrade the firmware on your base stations to take advantages of new features. Firmware versions for the VP2200 Wi-Fi Base Station are identified by "spirit" at the start of the version name, and always end with ".bin". Whenever the firmware is updated, only use firmware with the file name beginning with "spirit" (such as spirit.0.1.r5.bin).

Guidance on Configuring the AP/Bridge with Recommended Settings

▶ An arrow next to field description information (usually in tables) indicates a recommended or suggested configuration setting for an option on the AP/Bridge.

Typographical Conventions

This guide uses the following typographical conventions:

italics	Glossary terms, new terms, and book titles
`typewriter font`	Screen text, URLs, IP addresses, and MAC addresses, UNIX file, command, and directory names, user-typed command-line entries
`typewriter font italics`	Variables
Bold Keywords	Menu titles, window names, and button names
DANGER ⚠	This symbol and adjoining text warn the installer or user of a potentially dangerous conditional that may result in physical injury or death.

Introduction

Overview of the Vivato Wi-Fi AP/Bridge

The Vivato Wi-Fi AP/Bridge provides continuous, high-speed access between IEEE 802.11a/b/g wireless clients and wired Ethernet networks. It is an advanced, standards-based solution for wireless networking in indoor areas. The Vivato Wi-Fi AP/Bridge enables zero-administration wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The Vivato Wi-Fi AP/Bridge provides the strongest security, ease-of-administration, and industry standards — providing a standalone and fully-secured wireless network without the need for additional management and security server software.

What's Inside the AP/Bridge?

Inside the AP/Bridge is a Wi-Fi radio system and a central microprocessor that coordinates all activities. The AP/Bridge contains two wireless interfaces. Each interface supports 802.11a, 802.11b, and 802.11g operation. Two removable 2.2 dBi omnidirectional antennas are included that thread into the VA4200's RP-TNC (male) connectors.

The AP/Bridge boots from Flash ROM that contains firmware with the configurable, runtime features summarized in "Overview of the Vivato Wi-Fi AP/Bridge" on page 16.

As new features and enhancements become available, you can upgrade the firmware to add new functions and performance improvements to the AP/Bridges that make up your wireless network. (See "Upgrading the Firmware" on page 80.)

The following sections list features and benefits of the Vivato Wi-Fi AP/Bridge, and describes the operation of the front panel indicators and rear panel connectors.

Features and Benefits

- IEEE Standards Support
- Wireless Features
- Security Features
- Networking
- Simple Network Management Protocol (SNMP) Support
- Maintainability
- Indicators and Connectors

Features and Benefits

IEEE Standards Support

- Support for IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g wireless networking standards.
- Provides data rates of up to 54 Mbps

Wireless Features

- Allows simultaneous 802.11a and 802.11b/g operation using two separately configurable wireless interfaces.
- Transmit power adjustment.
- Wireless Distribution System (WDS) for connecting multiple AP/Bridges wirelessly. Extends your network with less cabling and provides a seamless experience for roaming clients.
- Quality of Service (QoS) for enhanced throughput and better performance of time-sensitive wireless traffic like Voice over IP (VoIP) and streaming media.
- Built-in support for multiple SSIDs (network names) and multiple BSSIDs (basic service set IDs) on the same AP/Bridge.
- Rogue access point detection.
- Prioritization of SpectraLink® Voice Priority (SVP) packets to optimize Voice over IP (VoIP) operation using SVP-based IP phones.

Security Features

- Inhibit SSID Broadcast
- Weak IV avoidance
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Advanced Encryption Standard (AES)
- User-based access control with local authentication server.
- Local user database and user life-cycle management.
- MAC address filtering
- Hardware watchdog

Networking

- Dynamic Host Configuration Protocol (DHCP) client support for dynamically assigning network configuration information to systems on the LAN.
- Virtual Local Area Network (VLAN) support

- Automatic assignment of VLANs from an external RADIUS server.
- One 10/100 Ethernet port
- IEEE 802.3af-compliant to allow power over Ethernet

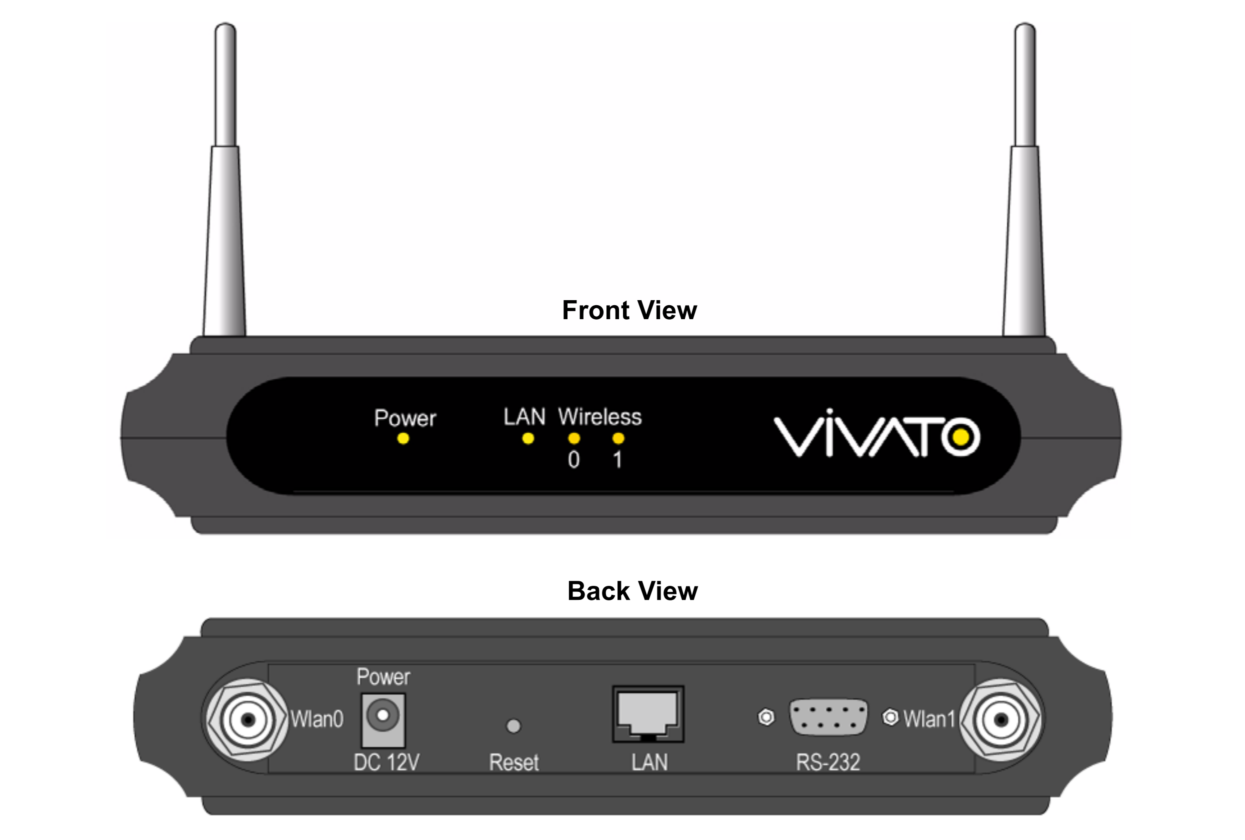
Simple Network Management Protocol (SNMP) Support

- Support for versions 1 and 2c.
- Management Information Base (MIBs) provided to monitor and manage AP/Bridge operation.
- Traps can be set to alert the system administrator to specific conditions.

Maintainability

- Status, monitoring, and tracking views of the network including client associations, transmit/receive statistics, and event log.
- Reset configuration option to restore factory defaults.
- Firmware upgrade using downloads that you retrieve from the Vivato Customer Support website.

Indicators and Connectors



Front Panel Indicators

Power LED - Illuminated but not blinking indicates that the VA4200 is powered on and is booting up. Blinking indicates that the boot sequence has completed.

LAN LED - Illuminated but not blinking indicates a connection, but no link activity. Blinking indicates link activity. Not illuminated indicates no recognized connection to a device.

Wireless LEDs - When off, indicates that the corresponding wireless interface (0 or 1) is disabled. When blinking, indicates that the corresponding wireless interface is enabled. LED color indicates the current 802.11 mode used on that interface: green = 802.11b or 802.11b/g mode, amber = 802.11a mode.

Rear Panel Connections

Antenna connectors - Two RP-TNC (male) connectors.

Power - 12 VDC power connector. Center conductor is positive (+). Power supply plug required: 2mm pin opening x 6mm outside diameter.

Reset - Using the end of a paper clip or other small shaft, quickly press and release the recessed button to reboot the VA4200 using the last saved configuration. Holding the button in for approximately four seconds causes the current configuration to be deleted and reboots the VA4200 using the factory default configuration.

LAN RJ-45 10/100 Base-T Ethernet port. This MDI-MDIX auto-crossover and auto-sensing port is enabled by default, and remains enabled unless you disable it during configuration. This port can also be used to provide power to the AP/Bridge using an IEEE 802.3af-compliant power over Ethernet (PoE) device. Category 5 (CAT-5) cabling to the VA4200 should be limited to a maximum length of 100 meters.

RS232 Serial (DB-9, male) - This serial communications (console) port provides direct control access to the AP/Bridge’s operating system. This port is not used to perform any regular AP/Bridge operations, but is provided to allow future operations, such as bootloader updates. The following are the required communication settings:

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

What’s Next?

Determining the best location for the VA4200 AP/Bridge requires careful planning and consideration. Refer to “Installation” on page 32.

After mounting the AP/Bridge, read through the “PreLaunch Checklist: Default Settings and Supported User/Client Platforms” on page 20 and then follow the steps in “Quick Steps for Setup and Launch of Your Wireless Network” on page 26.

PreLaunch Checklist: Default Settings and Supported User/Client Platforms

Before you power-up a new AP/Bridge, review the following sections for a quick check of required hardware components, software, client configurations, and compatibility issues. Make sure you have everything you need ready to go for a successful launch and test of your new (or extended) wireless network.

- Vivato Wi-Fi AP/Bridge
    - › Default Settings for the Vivato Wi-Fi AP/Bridge
    - › What the AP/Bridge Does Not Provide
- User's Computer
- Wireless Client Computers
- Understanding Dynamic and Static IP Addressing on the Vivato Wi-Fi AP/Bridge
    - › How Does the AP/Bridge Obtain an IP Address at Startup?
    - › Dynamic IP Addressing
    - › Static IP Addressing

Vivato Wi-Fi AP/Bridge

The Vivato Wi-Fi AP/Bridge is a wireless communications hub for devices on your network. It provides continuous, high-speed access between your wireless and Ethernet devices in IEEE 802.11a, 802.11b, and 802.11g modes.

The Vivato Wi-Fi AP/Bridge offers a multiple service set identifiers (SSID) feature that allows it to be configured to provide several separate wireless networks, each using its own type of security. SSIDs use virtual local area networks (VLANs) to separate network traffic.

Default Settings for the Vivato Wi-Fi AP/Bridge

Option	Default Settings	Related Information
System Name	VA4200	
User Name	admin The user name is read-only. It cannot be modified.	
Password	vivato	“Specify a New User Password and the Wireless Network Name” on page 40 in “Configuring Basic Settings” on page 38 “Setting the User Password” on page 72.
Network Name (SSID)	"Internal Vivato Network"	“Review / Describe the AP/ Bridge” on page 39 in “Configuring Basic Settings” on page 38
Network Time Protocol (NTP)	None	“Enabling the Network Time Protocol Server” on page 49
IP Address	169.254.20.1 By default, static IP addressing is used. At startup, you assign a new static IP address using the VivatoVision™ Web pages. If you have a DHCP server on the network, an IP address can be dynamically assigned by the server after enabling DHCP operation.	“Understanding Dynamic and Static IP Addressing on the Vivato Wi-Fi AP/Bridge” on page 25 For information on setting the IP address, see Table 2“SSID Configuration Settings” on page 87
Subnet Mask	255.255.0.0	
Radios	On	“Configuring Radio Settings” on page 51
IEEE 802.11 Mode	802.11a/b/g	“Configuring Radio Settings” on page 51
Radio Channel	• Radio 0: Channel 6 (b/g mode) • Radio 1: Channel 52 (a mode)	“Configuring Radio Settings” on page 51
Beacon Interval	500 milliseconds	“Configuring Radio Settings” on page 51
DTIM Period	2 beacons	“Configuring Radio Settings” on page 51
Fragmentation Threshold	2346 bytes	“Configuring Radio Settings” on page 51
Regulatory Domain	FCC	“Configuring Radio Settings” on page 51
RTS Threshold	2347 bytes	“Configuring Radio Settings” on page 51
MAX Stations	2007	“Configuring Radio Settings” on page 51

Option	Default Settings	Related Information
Transmit Power	100 percent	"Configuring Radio Settings" on page 51
Supported Rates (Mbps)	• IEEE 802.11a: 54.0, 48.0, 36.0, 24.0, 18.0, 12.0, 9.0, 6.0 • IEEE 802.11b/g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1	"Configuring Radio Settings" on page 51
Basic Rate (Mbps)	• IEEE 802.11a: 24.0, 12.0, 6.0 • IEEE 802.11b/g: 11.0, 5.5, 2.0, 1.0	"Configuring Radio Settings" on page 51
Broadcast SSID	Allow	See "Does Prohibiting the Broadcast SSID Enhance Security?" on page 97 in "Configuring Security" on page 91
Security Mode	None (plain text)	See "Plain-text" on page 98 in "Configuring Security" on page 91
Authentication Type	None	
MAC Filtering	Allow any station unless in list	"Controlling Access by MAC Address Filtering" on page 57
WDS Settings	None	"Configuring the Wireless Distribution System (WDS)" on page 66

What the AP/Bridge Does Not Provide

The Vivato Wi-Fi AP/Bridge is not designed to function as a Gateway to the Internet. It does not contain a modem or point-to-point protocol over Ethernet (PPPoE) functions to connect to an Internet service provider (ISP). To connect your Wireless LAN (WLAN) to other LANs or the Internet, you need a gateway device.

User's Computer

Configuration and administration of the Vivato Wi-Fi AP/Bridge is accomplished by connecting to the AP/Bridge using an Ethernet connection. The following table describes the minimum requirements for the administrator's computer.

Required Software or Component	Description
Ethernet Connection to the AP/Bridge	The computer used to configure the AP/Bridge must be connected to the AP/Bridge (either directly or through a hub) by an Ethernet cable. Refer to "Indicators and Connectors" on page 18.

Required Software or Component	Description
Wireless Connection to the Network	After initial configuration and launch of the first AP/Bridge on your new wireless network, you can make subsequent configuration changes through the VivatoVision Web pages using a wireless connection to the "Internal" network. For wireless connection to the AP/Bridge, your administration device will need Wi-Fi capability similar to that of any wireless client: • Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the AP/Bridge. (IEEE 802.11a, 802.11b, and 802.11g modes are supported.) • Wireless client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the Vivato Wi-Fi AP/Bridge. For more details on Wi-Fi client setup, see “Wireless Client Computers” on page 23.
Display Resolution	Higher screen resolutions (such as 1280 x 1024) reduce the amount of scrolling needed to access all settings on the VivatoVision web user interface.
Web Browser / Operating System	Configuration and administration of the Vivato Wi-Fi AP/Bridge is provided through a Web-based user interface hosted on the AP/Bridge. We recommend using one of the following supported Web browsers to access the AP/Bridge VivatoVision Web pages: • Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000 • Netscape Mozilla on Redhat Linux version 2.4 The VivatoVision Web browser must have JavaScript enabled to support the interactive features of this interface. It must also support HTTPS uploads to use the firmware upgrade feature.
CD-ROM Drive	The administrator’s computer must have a CD-ROM drive to access the User Guide on the supplied CD-ROM.
Security Settings	Ensure that security is disabled on the wireless client used to initially configure the AP/Bridge.

Wireless Client Computers

The Vivato Wi-Fi AP/Bridge provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the AP/Bridge is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

In order to connect to the AP/Bridge, wireless clients need the following software and hardware.

Required Component	Description
Wi-Fi Client Adapter	Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the AP/Bridge. (IEEE 802.11a, 802.11b, and 802.11g modes are supported.) Wi-Fi client adapters vary considerably. The adapter can be a PC card built into the client device, a portable PCMCIA or PCI card (types of NICs), or an external device such as a USB or Ethernet adapter that you connect to the client by means of a cable. The VA4200 AP/Bridge supports 802.11a/b/g modes, but you will probably make a decision during network design phase as to which mode to use. The fundamental requirement for clients is that they all have configured adapters that match the 802.11 mode for which your AP/Bridge(s) is configured.
Wireless Client Software	Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the Vivato Wi-Fi AP/Bridge.
Client Security Settings	Security should be disabled on the client used to do initial configuration of the AP/ Bridge. If the Security mode on the AP/Bridge is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the AP/ Bridge and provide a valid username and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.1x, WPA with RADIUS server, and WPA-PSK. For information on configuring security on the AP/Bridge, see “Configuring Security” on page 91.

Understanding Dynamic and Static IP Addressing on the Vivato Wi-Fi AP/ Bridge

How Does the AP/Bridge Obtain an IP Address at Startup?

By default, the AP/Bridge uses a static IP address. This is done to establish a known IP address to use to easily re-access the VivatoVision™ web pages for configuration. After configuration is completed, automatic IP addressing using DHCP can be enabled if desired.

Automatic IP addressing looks for a network DHCP server and, if it finds one, obtains an IP Address from the DHCP server. If no DHCP server is found on the network, the AP/Bridge will continue to use its Static IP Address (169.254.20.1) until you re-assign it a new static IP address (and specify a static IP addressing policy) or until a DHCP server is brought online.

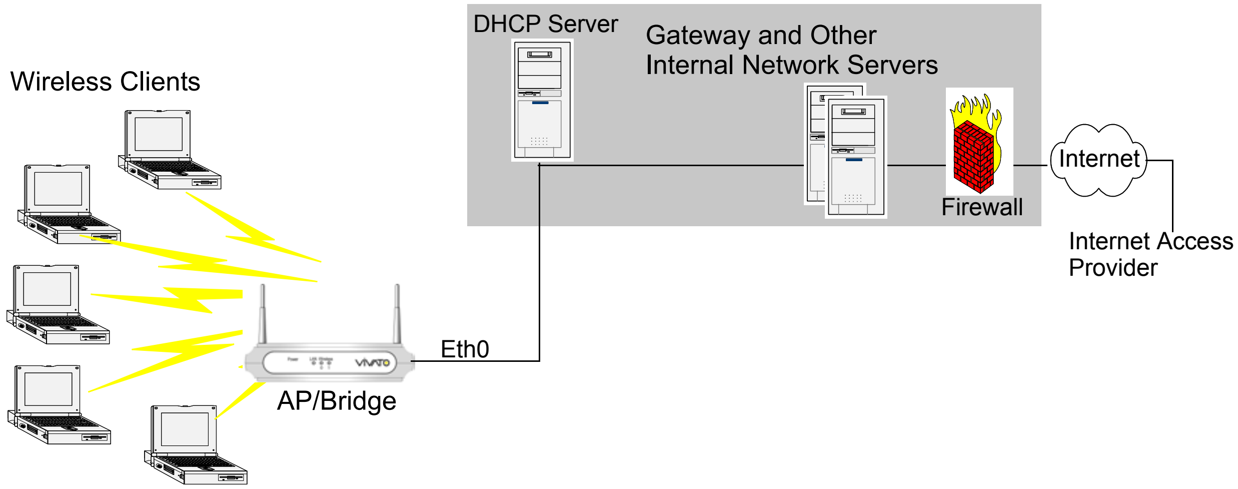
Dynamic IP Addressing

Most home and small business networks already have DHCP service provided either via a gateway device or a centralized server. However, if no DHCP server is present on the Internal network, the AP/Bridge will use the assigned Static IP Address.

Similarly, wireless clients and other network devices (such as printers) will receive their IP addresses from the DHCP server, if there is one. If no DHCP server is present on the network, you must manually assign static IP addresses to your wireless clients and other network devices.

If DHCP is used, the system administrator must look at the DHCP server's log to see what IP address was assigned to the AP/Bridge (by looking for the AP/Bridge's MAC address in the log) in order to use that address to access the VivatoVision web interface.

EXAMPLE NETWORK LAYOUT WHEN USING A DHCP SERVER



Static IP Addressing

The Vivato Wi-Fi AP/Bridge ships with a default Static IP Address of 169.254.20.1 (See "Default Settings for the Vivato Wi-Fi AP/Bridge" on page 21.) The AP/Bridge retains this static IP address until you change it.

Quick Steps for Setup and Launch of Your Wireless Network

Setting up and deploying one or more Vivato Wi-Fi AP/Bridges creates a wireless network. The Basic Settings VivatoVision Web page simplifies this process. Here is a step-by-step guide to setting up your Vivato Wi-Fi AP/Bridge and the resulting wireless network.

The following topics are discussed:

Step 1. Install the AP/Bridge
Step 2. Set the PC’s Network Interface to Talk to the AP/Bridge
Step 3. Log in to the VivatoVision Web Pages
Step 4. Configure the Basic Settings
Step 5. Specify the IP Address and Security Settings for the Primary Wireless Network
Step 6. Configure the Default Gateway and DNS Nameserver IP Addresses

Step 1. Install the AP/Bridge

See "Installation" on page 32 for information on installing your AP/Bridge.

Step 2. Set the PC’s Network Interface to Talk to the AP/Bridge

The IP address of your computer’s network interface must be within the same IP address range as the default IP address of the AP/Bridge in order for the two devices to communicate. If your PC’s operating system supports automatic IP addressing[1] (Microsoft® Windows® 2000 or XP), it can automatically get an IP address that will allow your computer to communicate with the AP/Bridge.

1. With your PC’s network interface card (NIC) configured for automatic IP addressing, turn the PC off for several seconds and then turn it back on.

2. Wait one minute after your computer has completed its reboot. Your computer’s network interface will automatically be assigned an IP address in the range that will allow it to access the AP/Bridge.

If your PC’s operating system does not support automatic private IP addressing, access your network interface’s TCP/IP settings and set a static IP address of **169.254.20.2**, and a Net Mask of **255.255.0.0**.

[1] To see if your network adapter is using automatic IP addressing, go to **Start>Settings>Network Connections>Local Area Connection>Properties>Internet Protocol (TCP/IP) >Properties**, and make sure “Obtain an IP address automatically” is checked, then click on “Alternate Configuration” to make sure “Automatic Private IP Address” is also checked.

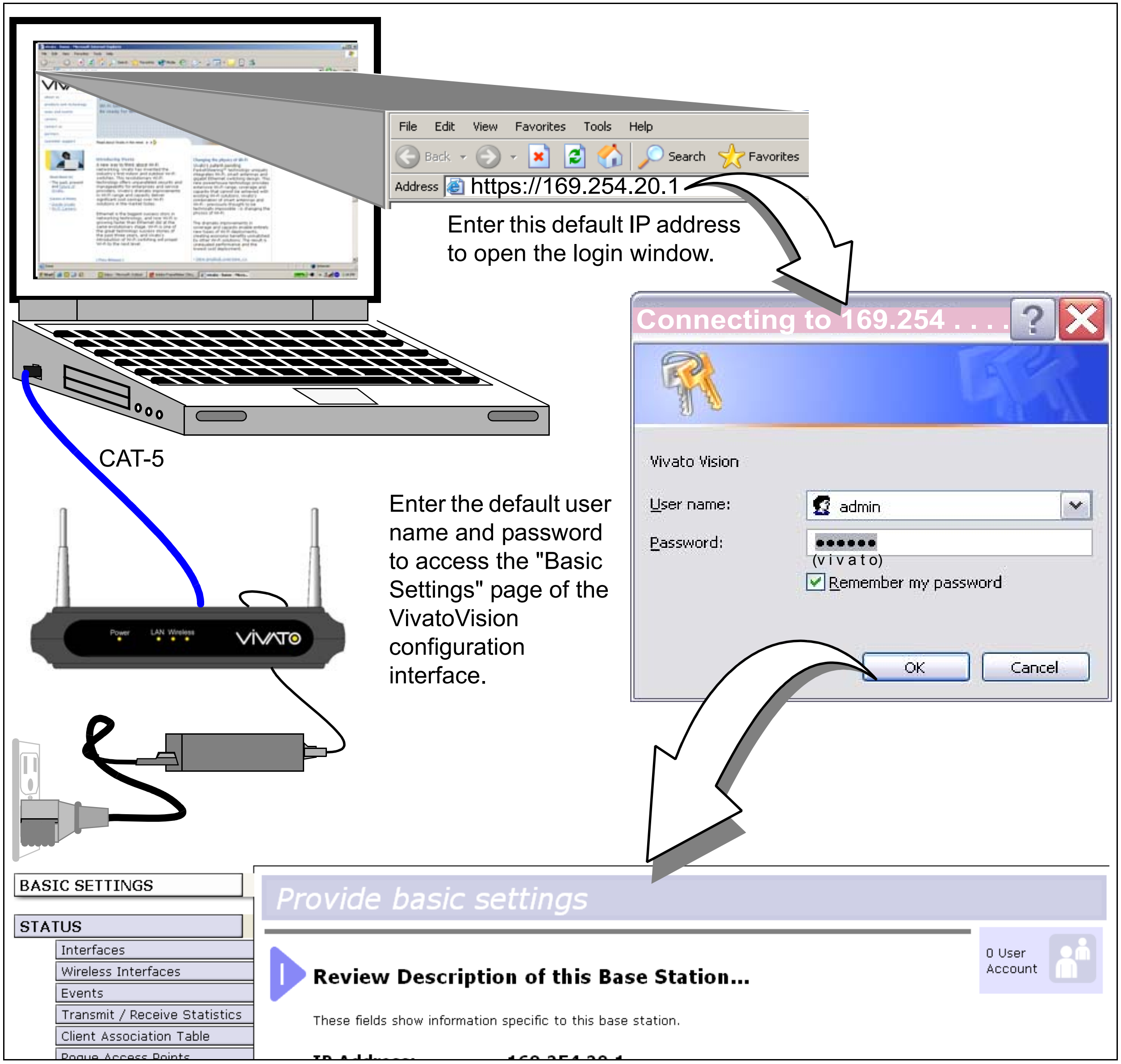
Step 3. Log in to the VivatoVision Web Pages

1. If not already connected, connect the AP/Bridge to the PC’s NIC through a CAT-5 RJ-45 cable.

2. Power on the AP/Bridge. You can use the supplied in-line power supply or use a PoE device.

3. Open a web browser on the PC and enter the default IP address of the AP/Bridge (https://169.254.20.1) for the address/location as shown below. A login screen is then displayed.

4. Enter "admin" for the user name and "vivato" for the password. The user name will never change, but you should change the password before you are done configuring the AP/Bridge to avoid unauthorized access. When you first log in, the BASIC SETTINGS page is displayed..



Address https://169.254.20.1

Enter this default IP address to open the login window.

Enter the default user name and password to access the "Basic Settings" page of the VivatoVision configuration interface.

Vivato Vision

User name: admin

Password: ●●●●●● (vivato)

☑ Remember my password

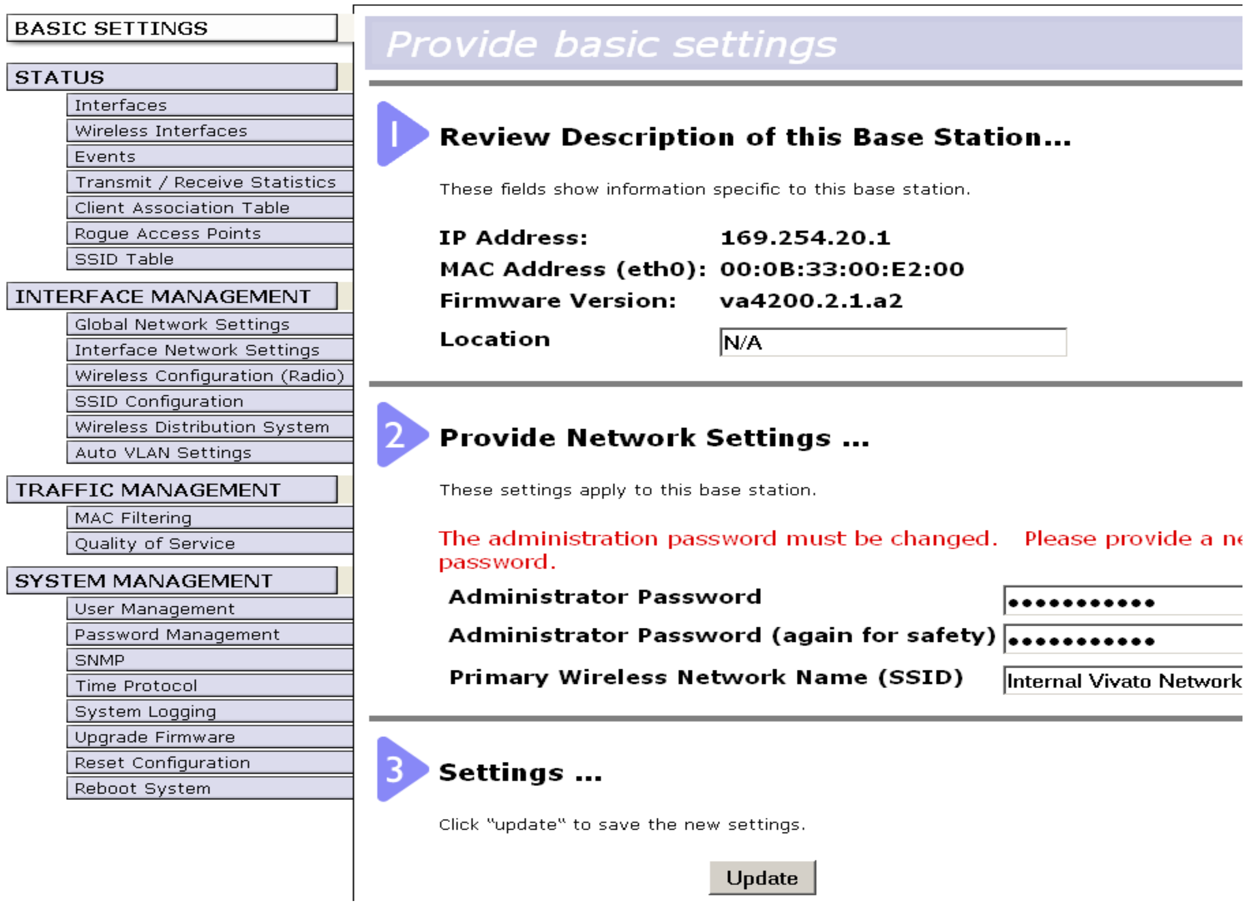
Provide basic settings

Review Description of this Base Station...

These fields show information specific to this base station.

Step 4. Configure the Basic Settings

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are available on the Basic Settings page, and are organized as steps 1-3 on the web page.



Provide basic settings

1 Review Description of this Base Station...

These fields show information specific to this base station.

IP Address: 169.254.20.1
MAC Address (eth0): 00:0B:33:00:E2:00
Firmware Version: va4200.2.1.a2
Location N/A

2 Provide Network Settings ...

These settings apply to this base station.

The administration password must be changed. Please provide a ne
password.

Administrator Password ●●●●●●●●●●●
Administrator Password (again for safety) ●●●●●●●●●●●
Primary Wireless Network Name (SSID) Internal Vivato Network

3 Settings ...

Click "update" to save the new settings.

Review Description of this Access Point:

- **IP Address**: Shows the current IP address, but cannot be changed from this screen.
- **MAC Addresses**: Shows the MAC addresses of Ethernet port, and cannot be changed.
- **Firmware Version**: Shows the current version of AP/Bridge firmware.
- **Location:** Enter a name that identifies where this AP/Bridge will be mounted.

Provide Network Settings:

- **Administrator Password**: The default is “vivato”. Enter a new password (twice) to use the next time that you access the VivatoVision interface. TO PROTECT YOUR NETWORK, DO NOT LEAVE THE DEFAULT PASSWORD UNCHANGED!
- **Primary Wireless Network Name (SSID)**: Enter a name (1 to 32 characters) for the default wireless signal that clients can always see in their list of available networks.

Settings:

- Select the “**Update**” button to start using these settings and enter the changes into the AP/Bridge’s configuration. Clicking **"Update"** on any of the VivatoVision web pages causes the current configuration to be changed and saved; settings are persistent through a reboot.

For a detailed description of these "Basic Settings" and how to properly configure them, see “Configuring Basic Settings” on page 38.

Default Configuration

If you follow the steps above and accept all the defaults, the AP/Bridge will have the default configuration described in “Default Settings” on page 21.

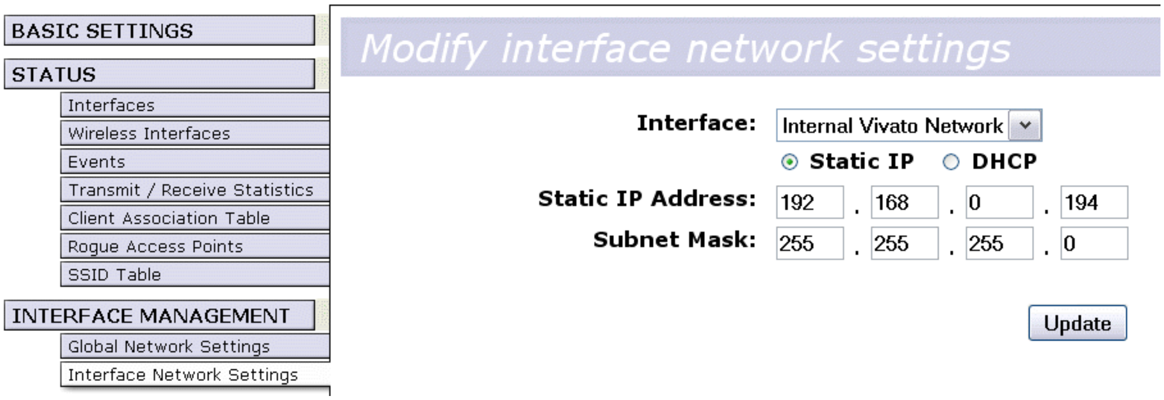
Step 5. Specify the IP Address and Security Settings for the Primary Wireless Network

The IP address of the AP/Bridge can be configured statically or dynamically to work on your wired network. Dynamic assignment requires a DHCP server on your wired network.

By default, the wireless network is unsecured. To prevent access to your network by undesired wireless clients, the highest level of security should be configured on the AP/Bridge and on the clients.

1. Select the **INTERFACE MANAGEMENT>Interface Network Settings** tab.

2. Select the **Interface** for the “Primary Wireless Network Name” that you entered on the Basic Settings screen.



Modify interface network settings

Interface: Internal Vivato Network

● Static IP ○ DHCP

Static IP Address: 192 . 168 . 0 . 194

Subnet Mask: 255 . 255 . 255 . 0

3. Set the IP Address to either **Static IP** or **DHCP**.

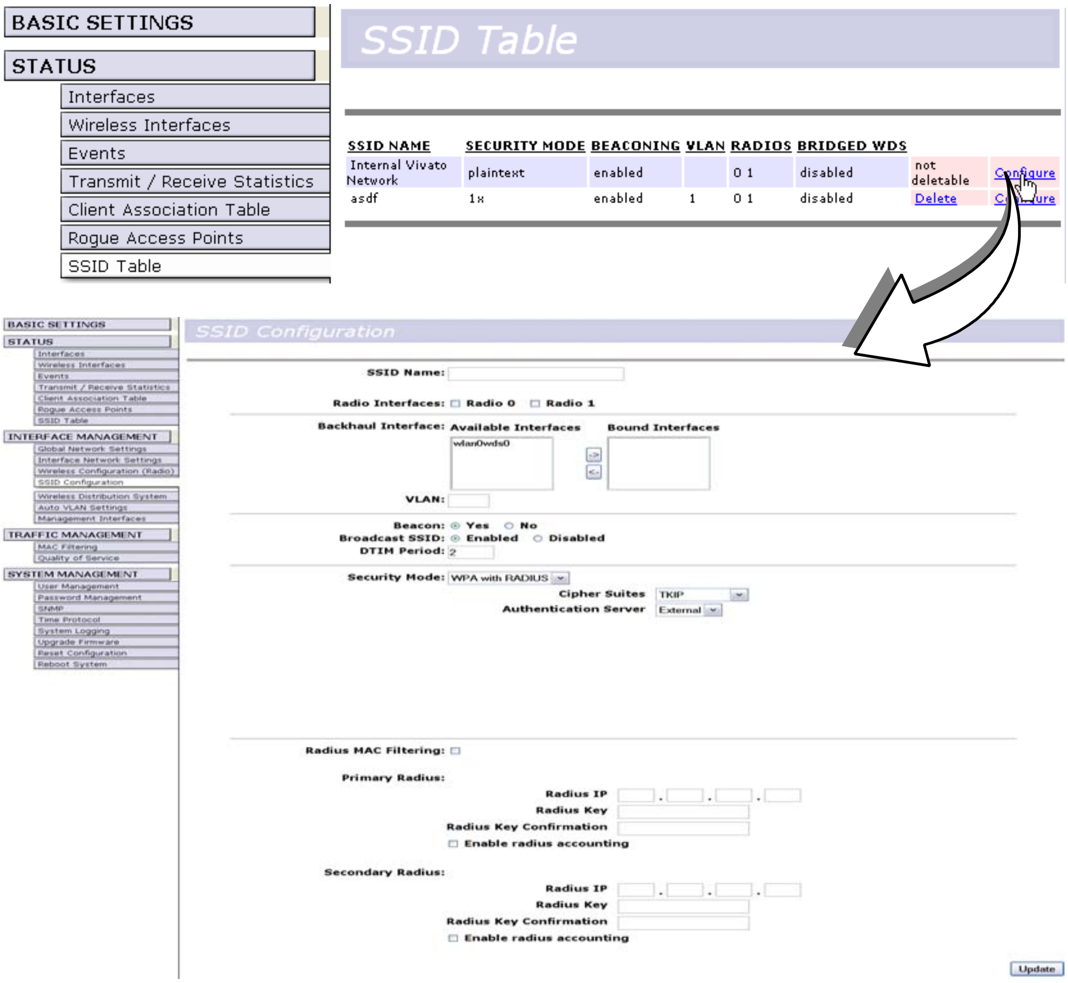
› If Static IP is used, enter the IP address and subnet mask.

› If DHCP is chosen, the AP/Bridge will request an IP address from your DHCP server when it is connected to your network.

› To restrict access to the AP/Bridge’s VivatoVision web interface to this IP address, select the checkbox next to **Management Interface**. When checked, no other IP address can be used to access the configuration settings.

4. Select **Update** to save your settings. If you selected to use DHCP, the IP address of the AP/Bridge remains 169.254.20.1 until it is connected to a network with a DHCP server. If you are using a static IP address, you must change the IP address of the NIC on your PC to be within that IP address range before you can access the VivatoVision configuration pages again.

5. Select the **STATUS>SSID Table** tab, and select the **Configure** link for the primary network name that you entered. This causes the **SSID Configuration** page for that network to be displayed.



SSID Table

SSID NAME	SECURITY MODE	BEACONING	VLAN	RADIOS	BRIDGED WDS		
Internal Vivato Network	plaintext	enabled		0 1	disabled	not deletable	Configure
asdf	1x	enabled	1	0 1	disabled	Delete	Configure

SSID Configuration

SSID Name:

Radio Interfaces: □ Radio 0 □ Radio 1

Backhaul Interface: Available Interfaces: wlan0wds0 -> <- Bound Interfaces

VLAN:

Beacon: ● Yes ○ No
Broadcast SSID: ● Enabled ○ Disabled
DTIM Period: 2

Security Mode: WPA with RADIUS
Cipher Suites: TKIP
Authentication Server: External

Radius MAC Filtering: □

Primary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

Secondary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

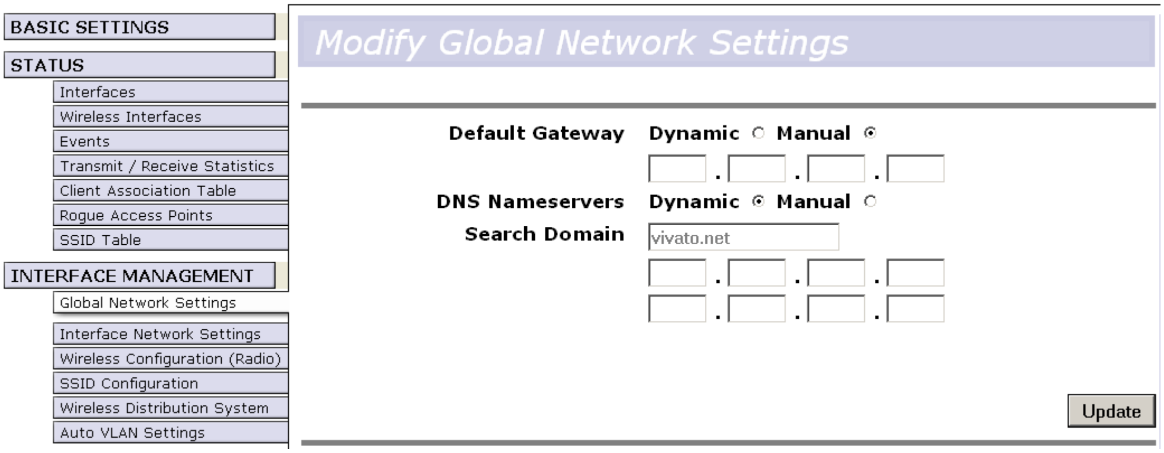
6. Select the type of security to use on the Primary Wireless Network to secure wireless connections, or leave the setting at "Open" to provide an unsecured network. Be sure to also configure your clients to work with that type of security. Refer to “Configuring Security” on page 91 for detailed descriptions of security settings.

7. Select **Update** to save your settings. Wireless clients must use the security configuration for that network in order to authenticate through it.

Step 6. Configure the Default Gateway and DNS Nameserver IP Addresses

The gateway in your wired network provides access to outside networks, allowing clients to do things like access the Internet. DNS nameservers convert host names, like "viviato.net", into IP addresses that may be on local or remote networks. The IP addresses of these devices need to be entered in order for the AP/Bridge to know where to send these types of network requests.

Select **INTERFACE MANAGEMENT>Global Network Settings** to bring up the default gateway and DNS nameserver fields.



Modify Global Network Settings

Default Gateway Dynamic ○ Manual ●

DNS Nameservers Dynamic ● Manual ○

Search Domain vivato.net

The Default Gateway and DNS Nameservers can be filled out automatically by a DHCP server that is configured to provide that information when these functions are set to Dynamic. When set to Manual, the user must enter the IP address of the device.

Select **Update** to save these settings.

Next Steps

1. If a PC was used to perform the initial configuration, disconnect the PC and connect the AP/Bridge directly to your wired network.

2. Connect to the AP/Bridge with your wireless client. Using the "available networks" function of your wireless client’s software, select the network name (SSID) that you specified. On MS Windows® clients, you will typically have to check the check-box that allows a connection to an unsecured network.

3. To verify LAN access, start an application on your wireless client that uses a service on your LAN (such as a web browser) to see if it can send and receive data.

   See “Wireless Client Computers” on page 23 for information on requirements for these clients.

4. After the wireless network is up and you have tested the AP/Bridge using some wireless clients, you can modify your security settings, add internal RADIUS server users, configure one or more virtual local area networks (VLANs), and fine-tune performance settings.

Installation

The VA4200 should be installed using the following steps:

1. Unpack the AP/Bridge.

2. Mount the AP/Bridge.

3. Run the network, power, and serial data lines to the AP/Bridge.

4. Configure the AP/Bridge. See “Quick Steps for Setup and Launch of Your Wireless Network” on page 26.

Shipping Contents

Quantity	Description
1	Vivato VA4200 AP/Bridge
1	Power supply
1	DB-9 null modem cable. Used for a direct "console" connection to the VA4200.
1	RJ45, CAT5, Ethernet cable, 6 ft.
2	RP-TNC (f) omnidirectional antennas (2 dBi @ 2.4 GHz)
1	Auto-running CD-ROM containing user documentation and other support files.

Environmental Considerations

The Vivato VA4200 AP/Bridge is designed for the following conditions:

- Operating temperature range: -0° C (32° F) to +55° C (+131° F)
- Storage temperature: -40° (-40° F) to +80° C (+176° F)
- Humidity: 20% to 90% non-condensing

Mounting Weight Considerations

- The VA4200 AP/Bridge weighs ~0.5 kg (1.1 lbs), excluding the AC/DC power supply.

Powering the VA4200

The VA4200 can be powered using its supplied AC/DC power supply or by using an IEEE 802.3af-compliant PoE device. If desired, both methods can be used simultaneously to power the VA4200 in order to provide a backup power supply if one of the supplies loses power.

Using the Provided AC/DC Power Supply

The AC/DC supply has an input voltage range of 90 to 260 VAC, 50-60 Hz. The output voltage to the VA4200 is +12 VDC at 1.5 A (18 watts).

Using a PoE Device

The VA4200 can be powered through its Ethernet port when connected to a 802.3af-compliant device.

Positioning The VA4200

Where you position the VA4200 depends on your intended application and the physical surroundings.

The following conditions must be considered regardless of your application:

- Availability of mains (AC) power and LAN connections. If a power over Ethernet (PoE) solution is used, only a LAN cable must be available.
- Wall construction materials and other wireless signal obstructions (elevator shafts, metal panels, water pipes...).
- Interfering signal sources (microwave ovens, 2.4 GHz cordless phones, other 802.11a, 802.11b, or 802.11g devices...).
- Temperature and humidity.

Antenna Polarization and Positioning

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

The VA4200’s antennas can be adjusted 90 degrees to allow transmission and reception of signals that are vertically or horizontally polarized. The Vivato Wi-Fi Base Station’s antenna is horizontally polarized, however this orientation can be affected somewhat by its signals being reflected off of hard surfaces. Whenever you are using the VA4200, especially with a Wi-Fi Base Station, you should always adjust the antennas on the VA4200 to obtain the strongest signal level at the receiving device(s).

When using a wireless distribution system (WDS) link between the VA4200 and a Vivato Wi-Fi Base Station, use the “wireless associations” function in the base station to monitor the signal strength of the WDS signal at the wireless interface used for the WDS link. Adjust the antenna on the VA4200 to maximum the received signal level at the base station.

Interfering Signal Sources

IEEE 802.11b devices share the same unlicensed frequency band as other common devices, such as some radio frequency identification (RFID) systems, many newer cordless telephones, and microwave ovens. These devices produce radio frequency (RF) energy that can interfere with the Wi-Fi VA4200's signal. Whenever possible, you should eliminate or minimize the use of these devices within the VA4200's operating area in order to maximize Wi-Fi data rates.

The Vivato Wi-Fi VA4200 also uses the same frequencies as conventional access points (APs). All 802.11b devices must use clear channel assessment, making sure that no other device is transmitting so that only one device is transmitting at a time. This prevents multiple devices on the same radio frequency (RF) channel in the area from interfering with each other, but requires these devices to take turns, reducing the overall available throughput for each device.

When using the VA4200 with a Vivato Wi-Fi Base Station, use the Wi-Fi Base Station's rogue access point detector (RAPD) to determine which channel has the least traffic and the least interference, and set the Wi-Fi Base Station to use that channel. Refer to the *Vivato Outdoor Wi-Fi Base Station Deployment Guide* on the Vivato Customer Support website for more information on the possible sources of interference and their effects on Wi-Fi operation.

Positioning for Access Point Operation

When used as a stand-alone access point, position the VA4200 to provide the greatest line-of-sight access to the most clients. Whenever possible, mount the VA4200 in a central location that is above cubicle walls or other obstacles.

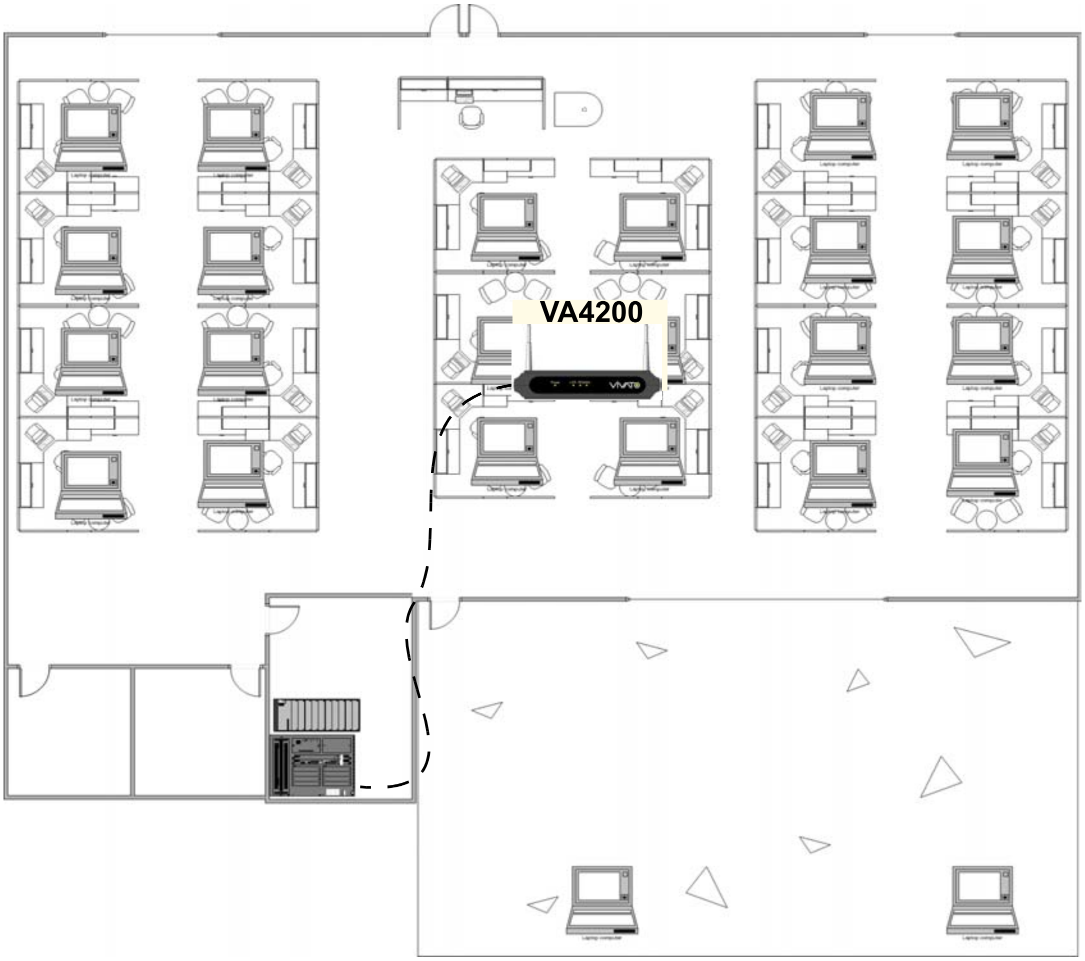


Figure 1—Access Point Location

Positioning for Coverage Filler Operation

When used with the Vivato Indoor Wi-Fi Base Station to fill a blocked area of Wi-Fi coverage, position the VA4200 where it has a good signal from the Wi-Fi Base Station (clear line-of-sight path when possible) and close to the clients that associate with it.

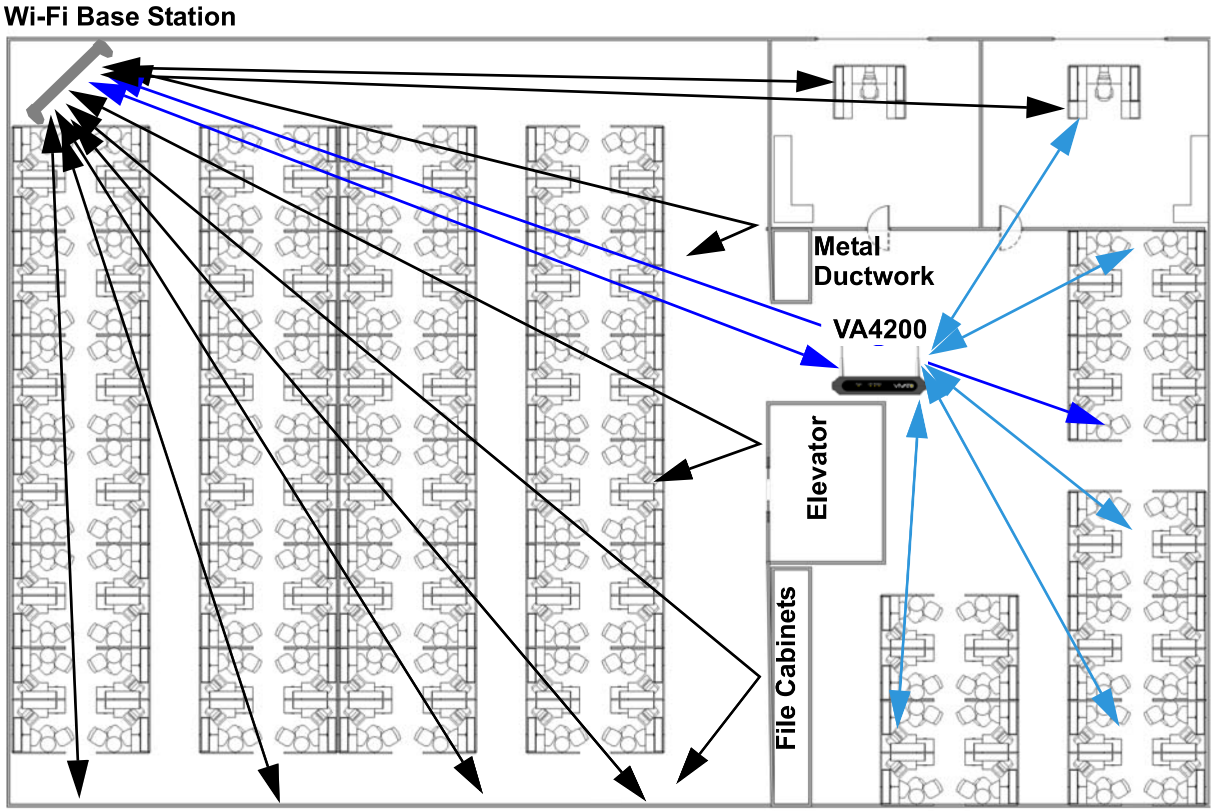


Figure 2—Hole Filler Location Example

Positioning for Wireless Backhaul Operation

When used to provide a wireless backhaul connection to a Vivato Wi-Fi Base Station that only has a power connection, position the VA4200 as close as possible to the Wi-Fi Base Station (clear line-of-sight path when possible). When used with an outdoor Wi-Fi Base Station, this is often achieved by putting the VA4200 next to a window with a clear view of the Base Station.

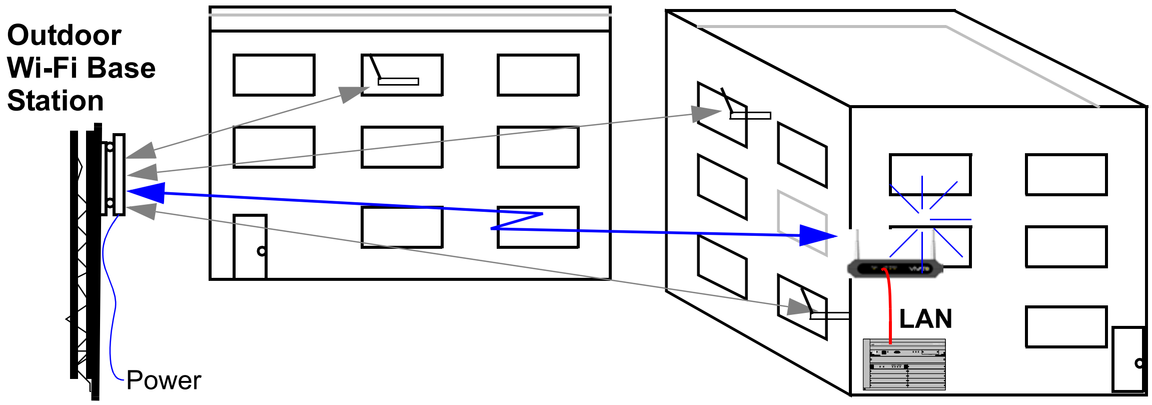


Figure 3—Wireless Backhaul to Base Station Example

Positioning for Range Extension Operation

When used to extend the range of a Vivato Wi-Fi Base Station's Wi-Fi area, position the VA4200 as close as possible to the Wi-Fi Base Station (clear line-of-sight path when possible). When used with an outdoor Wi-Fi Base Station, this is often achieved by putting the VA4200 next to a window with a clear view of the Base Station.

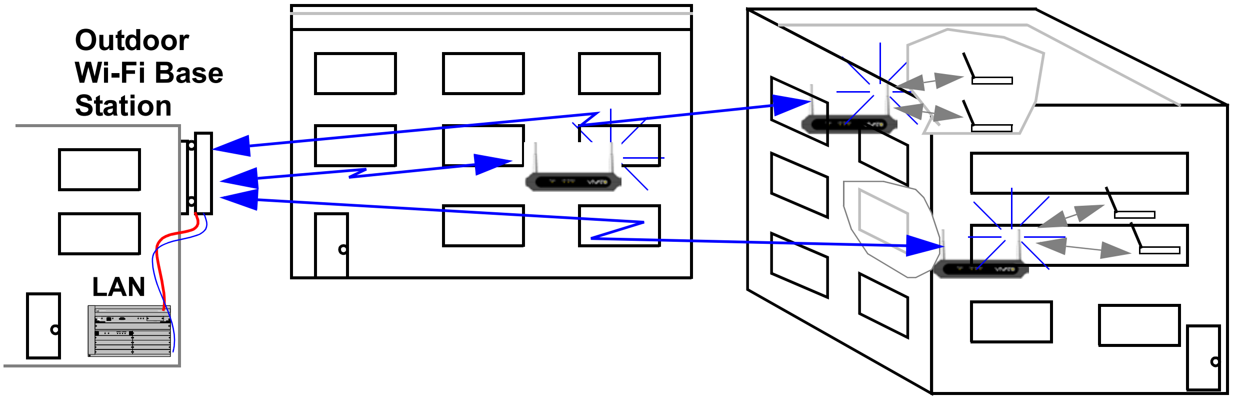
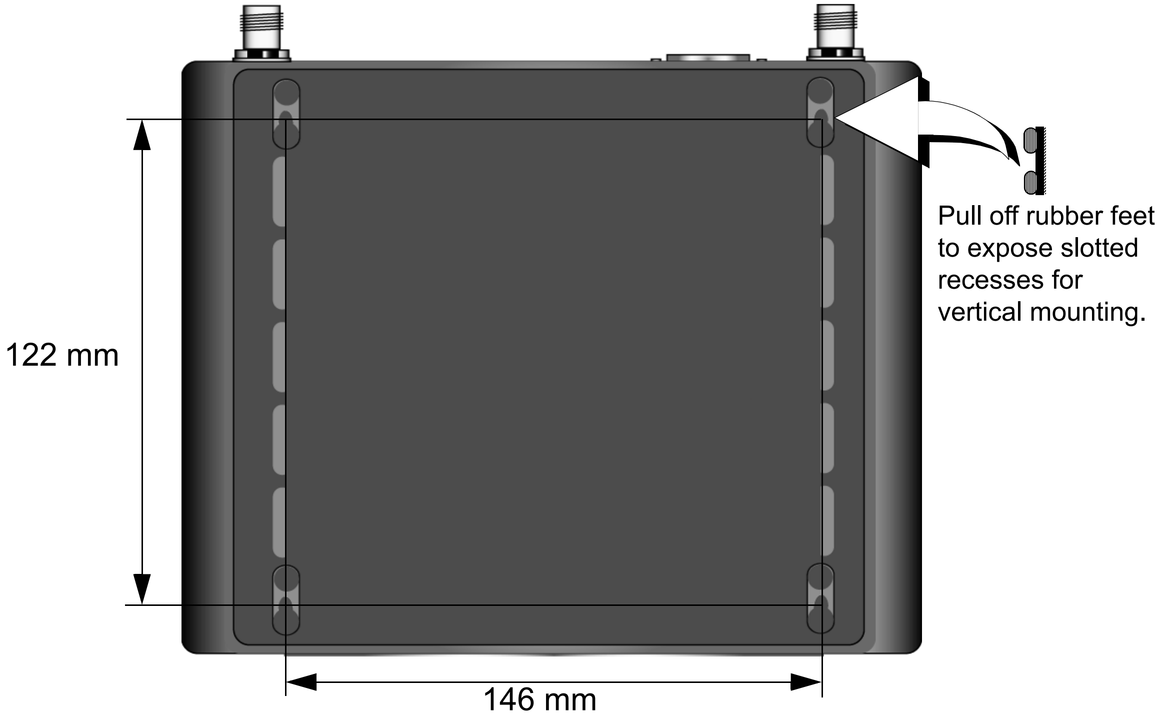


Figure 4—Wireless Backhaul to AP/Bridge Example

Mounting the VA4200

The VA4200 can be placed directly on a horizontal surface, or can be mounted vertically using user-supplied fasteners with exposed screw heads that recess into the slotted openings in its bottom cover.


122 mm
146 mm
Pull off rubber feet to expose slotted recesses for vertical mounting.

Preparing the VA4200 for Operation

To prepare the VA4200 for use:

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

2. Insert the AC power cord into the supplied power supply, then plug it into a wall outlet supplying a voltage within the voltage range labeled on the power supply. (Disregard this step if PoE is being used.)

3. Insert the power supply’s DC power plug into Power connector on the VA4200. (Disregard this step if PoE is being used.)

4. If not already done, configure the VA4200 using the built-in VivatoVision interface. Refer to “Quick Steps for Setup and Launch of Your Wireless Network” on page 26.

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

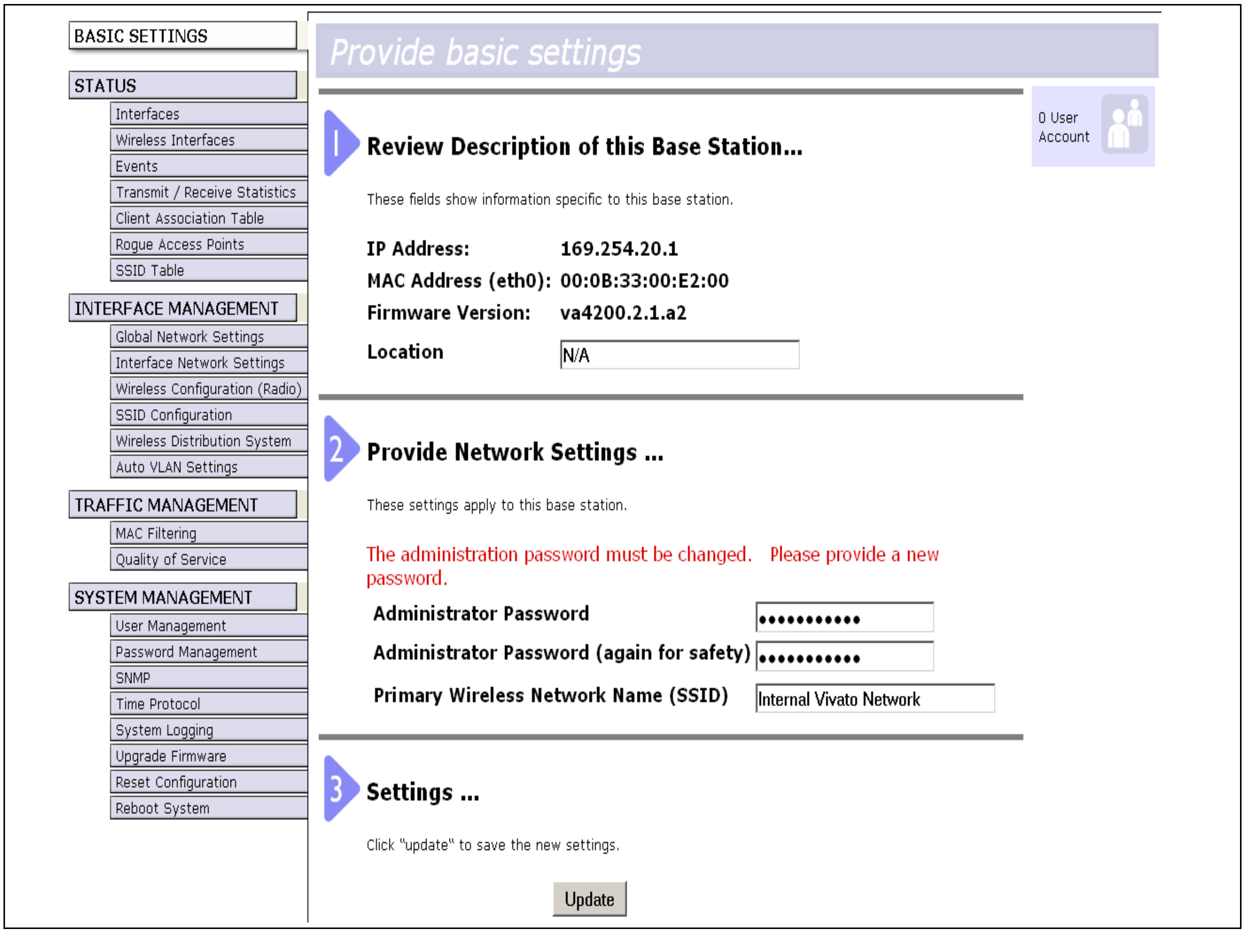
Configuring Basic Settings

The basic configuration tasks are described in the following sections:

- Navigating to Basic Settings
- Review / Describe the AP/Bridge
- Specify a New User Password and the Wireless Network Name
- Update Basic Settings
- At initial startup, no security is in place on the AP/Bridge. An important next step is to configure security, as described in “Configuring Security” on page 101.

Navigating to Basic Settings

To configure initial settings, click the **BASIC SETTINGS** tab.



Provide basic settings

1 Review Description of this Base Station...

These fields show information specific to this base station.

IP Address: 169.254.20.1
MAC Address (eth0): 00:0B:33:00:E2:00
Firmware Version: va4200.2.1.a2
Location: N/A

2 Provide Network Settings ...

These settings apply to this base station.

The administration password must be changed. Please provide a new password.

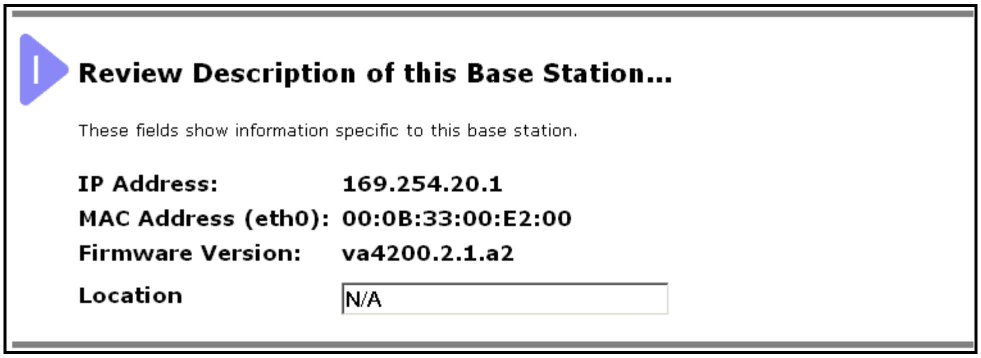
Administrator Password: •••••••••••
Administrator Password (again for safety): •••••••••••
Primary Wireless Network Name (SSID): Internal Vivato Network

3 Settings ...

Click "update" to save the new settings.

Fill in the fields on the BASIC SETTINGS screen as described below. The **User Account** icon shows the number of wireless client users that have been configured on the internal RADIUS server.

Review / Describe the AP/Bridge



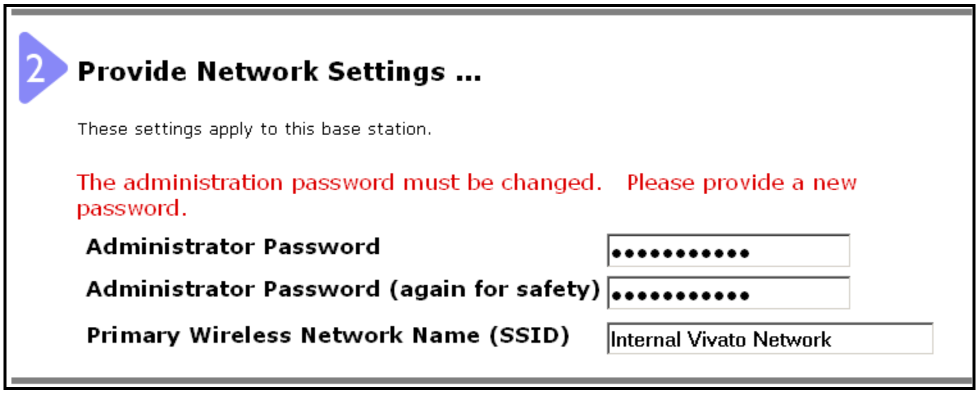
Review Description of this Base Station...

These fields show information specific to this base station.

IP Address: 169.254.20.1
MAC Address (eth0): 00:0B:33:00:E2:00
Firmware Version: va4200.2.1.a2
Location N/A

Field	Description
IP Address	Shows IP address assigned to this AP/Bridge. The address is not editable here, but can be changed on the Interface Network Settings screen. See “Setting Interface IP Addresses” on page 44.
MAC Addresses	Shows the MAC addresses of the Ethernet port: eth0 A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. To see MAC addresses for the wireless interfaces and the Guest and Internal interfaces on the VA4200, see the STATUS > INTERFACES tab.
Firmware Version	Version information about the firmware currently installed on the AP/Bridge. As new versions of the Vivato Wi-Fi AP/Bridge firmware become available, you can upgrade the firmware on your AP/Bridges to take advantages of new features. Firmware versions for the VA4200 AP/Bridge are identified by "spirit" at the start of the version name, and always end with ".bin". Whenever the firmware is updated, only use firmware with the file name beginning with "VA4200" (such as VA4200.2.0.bin). For instructions on how to upgrade the firmware, see “Upgrading the Firmware” on page 80.
Location	Specify a location description for this AP/Bridge to identify it in your network.

Specify a New User Password and the Wireless Network Name



2 Provide Network Settings ...

These settings apply to this base station.

The administration password must be changed. Please provide a new password.

Administrator Password: ●●●●●●●●●●●

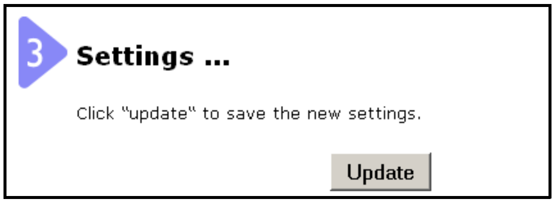
Administrator Password (again for safety): ●●●●●●●●●●●

Primary Wireless Network Name (SSID): Internal Vivato Network

Field	Description
Administrator Password	Enter a new administrator password. The characters you enter will be displayed as "*" characters to prevent others from seeing your password as you type. The password must be an alphanumeric strings of up to 32 characters. Do not use special characters or spaces. ▶ As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Administrator Password (again)	Re-enter the new administrator password to confirm that you typed it as intended.
Wireless Network Name (SSID)	Enter a name for the wireless network. This name will typically be used for all AP/Bridges on this network. The *Service Set Identifier* (SSID) is an alphanumeric character string of up to 32 characters. **Note:** If you are connected as a wireless client to the same VA4200 that you are administering, resetting the SSID will cause you to lose connectivity to the VA4200. You will need to reconnect to the new SSID after you save this new setting.
Wireless Guest Network Name (SSID)	Enter an alphanumeric character string of up to 32 characters to use for the wireless Guest network.

Note	The Vivato Wi-Fi AP/Bridge is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple AP/Bridges, and more than one administrator is logged on to the VivatoVision Web pages and making changes to the configuration, there is no guarantee that all configuration changes specified by multiple users will be applied.

Update Basic Settings



Settings ...

Click "update" to save the new settings.

When you have reviewed the new configuration, click **Update** to apply the settings and deploy the AP/Bridge as a wireless network.

At initial startup, no security is in place on the AP/Bridge. An important next step is to configure security, as described in “Configuring Security” on page 91.

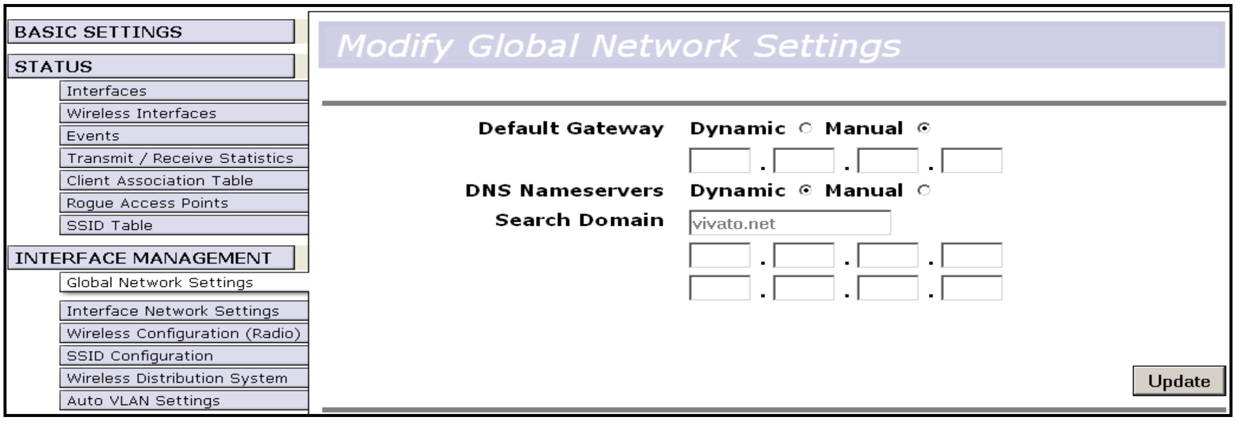
Global Network Settings

Global Network Settings specify the IP addresses for the default gateway and domain name server(s) (DNS) on your Ethernet local area network (LAN).

- Navigating to Global Network Settings
- Specifying the Default Gateway
- Specifying the DNS Nameservers
- Updating Settings

Navigating to Global Network Settings

To set the wired address for a AP/Bridge, navigate to the **INTERFACE MANAGEMENT > Global Network Settings** tab, and update the fields as described below.



Modify Global Network Settings

Default Gateway Dynamic ○ Manual ●

DNS Nameservers Dynamic ● Manual ○

Search Domain vivato.net

Specifying the Default Gateway

The default Gateway is the device on your wired network that is used to access other networks or subnets, including the Internet. The IP address of this device must be specified in order to send and receive packets to the other networks.

A DHCP server on your network can be configured to provide the default gateway address, even if the IP addresses of the interfaces on the AP/Bridge or not being provided by DHCP. To have the gateway IP address provided automatically, select "Dynamic".

To manually enter the default gateway, select "Manual" and enter the IP address in the standard format.

Specifying the DNS Nameservers

The DNS Nameserver associates domain names (like "vivato.net") with their IP addresses. This allows you to enter the domain name directly rather than having to know the actual IP address. Up to two IP addresses can be specified to provide for redundant nameserver operation.

A DHCP server on your network can be configured to provide the DNS nameserver addresses, even if the IP addresses of the interfaces on the AP/Bridge or not being provided by DHCP. To have the DNS server(s) address provided automatically, select "Dynamic".

To manually enter the DNS nameserver IP addresses, select "Manual" and enter the "Search Domain" and the IP addresses in the standard format.The Search Domain is the domain where the DNS nameserver(s) are located, such as "vivato.net". When a host name is used (such as "windmill"), the DNS servers will look for an entry within that domain; in this case "windmill.vivato.net".

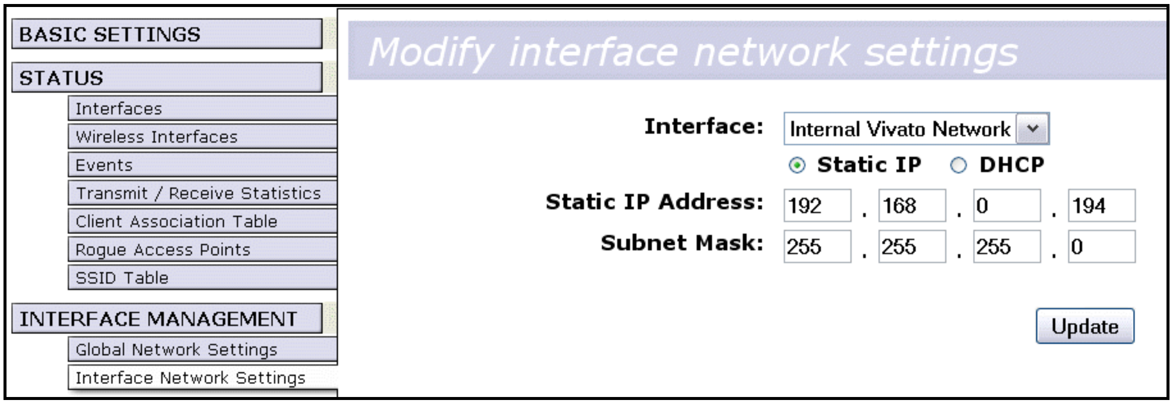
Updating Settings

To apply your changes, click **Update**.

Setting Interface IP Addresses

Each network within the VA4200 can have its own IP Address assigned to it. At least one interface must have an IP address assigned to it in order to provide access to the VivatoVision web user interlace. By default, a wireless network called "Internal Vivato Network" is configured on the VA4200 with an IP address of 169.254.20.1.

To view or change IP addresses, navigate to the **INTERFACE MANAGEMENT** > **Interface Network Settings.**



Modify interface network settings

Interface: Internal Vivato Network

● Static IP ○ DHCP

Static IP Address: 192 . 168 . 0 . 194

Subnet Mask: 255 . 255 . 255 . 0

Interface	The name assigned to this network. The first entry is always the name entered for the "Primary Wireless Network Name (SSID)" entered on the BASIC SETTINGS screen during initial configuration. This is the default wireless network and cannot be deleted. Additional SSIDs listed are those created on the SSID Configuration screen.
IP Address	An IP address can be statically or dynamically assigned to this network. • When "Static IP" is selected, the IP address and Subnet Mask must be manually entered. • When "DHCP" is selected, the IP address and Subnet Mask are provided by a DHCP server on the wired network.

Managing User Accounts

The Vivato Wi-Fi AP/Bridge includes a built-in remote authentication dial-in user service (RADIUS) server that is used to configure user accounts to provide secured wireless network access.

User management and authentication must always be used in conjunction with the following two security modes which require the use of a RADIUS server for user authentication and management.

- IEEE 802.1x mode (see “IEEE 802.1x” on page 102 in Configuring Security)
- WPA with RADIUS mode (see “WPA with RADIUS” on page 104 in Configuring Security)

You have the option of using either the internal RADIUS server embedded in the Vivato Wi-Fi AP/Bridge or an external RADIUS server that you provide. If you use the embedded RADIUS server, use this VivatoVision Web page on the AP/Bridge to set up and manage user accounts. If you are using an external RADIUS server, you will need to set up and manage user accounts on the Administrative interface for that server.

On the User Management page, you can create, edit, remove, and view client *user accounts*. Each user account consists of a user name and password. The set of users specified here represent approved *clients* that can log in and use one or more AP/Bridges to access local and possibly external networks via your wireless network.

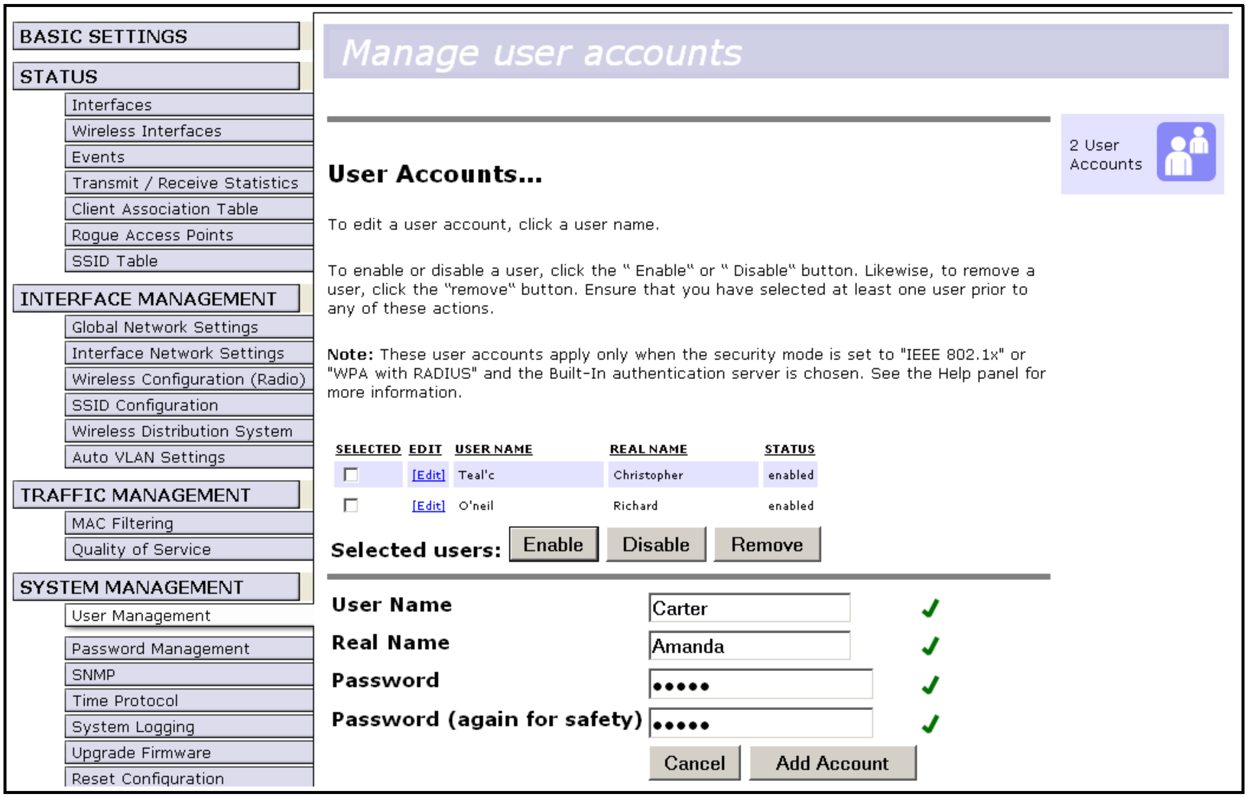
> **Note** Users specified here are clients of the AP/Bridge who use it as a connectivity hub, not administrators of the wireless network. Only those with the administrator username and password and knowledge of the VivatoVision URL can log in as an administrator and view or modify configuration settings.

The following topics are covered:

- Navigating to User Management
- Viewing User Accounts
- Adding a User
- Editing a User Account
- Enabling and Disabling User Accounts
- Removing a User Account

Navigating to User Management

To set up or modify user accounts, click the **SYSTEM MANAGEMENT>User Management** tab.



Manage user accounts

User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the " Enable" or " Disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
□	[Edit]	Teal'c	Christopher	enabled
□	[Edit]	O'neil	Richard	enabled

Selected users:

User Name	Carter ✓
Real Name	Amanda ✓
Password	●●●●● ✓
Password (again for safety)	●●●●● ✓

Viewing User Accounts

User accounts are shown at the top of the screen under "User Accounts". User name, real name, and status (enabled or disabled) are shown. You make modifications to an existing user account by first selecting the checkbox next to a user name and then choosing an action. (See “Editing a User Account” on page 47.)

Adding a User

To create a new user, do the following:

1. Under "Add a User", provide information in the following fields.

Field	Description
User Name	Provide a user name. User names are alphanumeric strings of up to 256 characters. Do not use special characters or spaces.

Field	Description
Real Name	For information purposes, provide the user’s full name. There is a 256 character limit on real names.
Password	Specify the password for this user. Enter the same password again for safety. Passwords are alphanumeric strings of up to 256 characters. Do not use special characters or spaces.

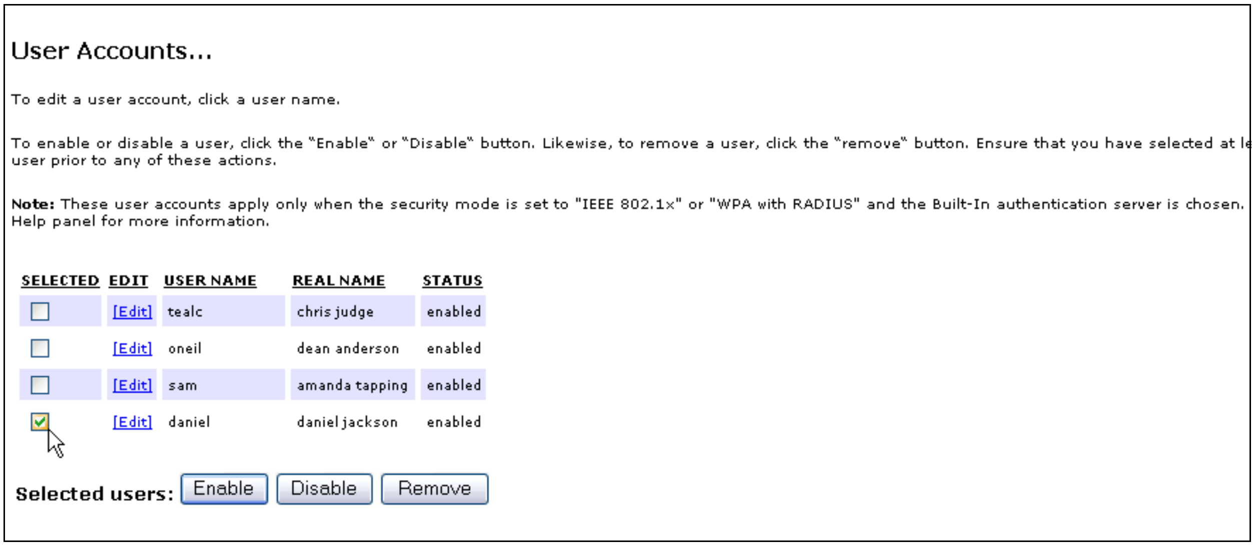
2. When you have filled in the fields, click **Add Account** to add the account.

   The new user is then displayed in the "User Accounts". The user account is *enabled* by default when you first create it.

Note	A limit of 100 user accounts per AP/Bridge is imposed by the VivatoVision user interface. Network usage may impose a more practical limit, depending upon the demand from each user.

Editing a User Account

Once you have created a user account, it is displayed under "User Accounts" at the top of the **User Management** VivatoVision Web page. To make modifications to an existing user account, first click the checkbox next to the user name so that the box is checked.



User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at le
user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen.
Help panel for more information.

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
☐	[Edit]	tealc	chris judge	enabled
☐	[Edit]	oneil	dean anderson	enabled
☐	[Edit]	sam	amanda tapping	enabled
☑	[Edit]	daniel	daniel jackson	enabled

Then, choose **Edit**, **Enable**, **Disable**, or **Remove**.

Enabling and Disabling User Accounts

A user account must be enabled for the user to log on as a client and use the AP/Bridge.

You can *enable* or *disable* any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or re-create accounts. This can come in handy in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

Enabling a User Account

To enable a user account, click the checkbox next to the user name and click **Enable**.

A user with an account that is *enabled* can log on to the wireless AP/Bridges in your network as a client.

Disabling a User Account

To disable a user account, click the checkbox next to the user name and click **Disable**.

A user with an account that is *disabled* cannot log on to the wireless AP/Bridges in your network as a client. However, the user remains in the database and can be enabled later as needed.

Removing a User Account

To remove a user account, click the checkbox next to the user name and click **Remove**.

If you think you might want to add this user back in at a later date, you might consider *disabling* the user rather than removing the account altogether.

Enabling the Network Time Protocol Server

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp will be used to indicate the date and time of each event in log messages.

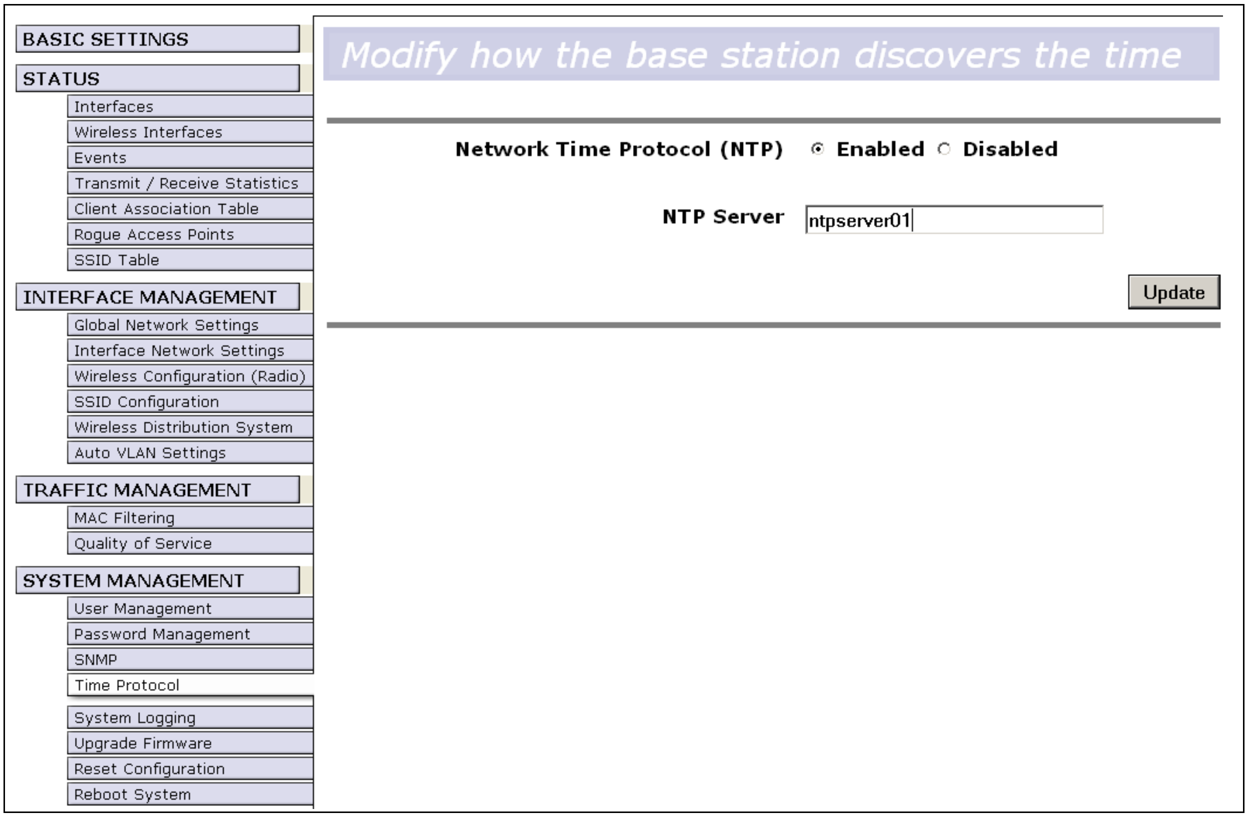
See http://www.ntp.org for more general information on NTP.

The following sections describe how to configure the Vivato Wi-Fi AP/Bridge to use a specified NTP server:

- Navigating to Time Protocol Settings
- Enabling or Disabling a Network Time Protocol (NTP) Server
- Updating Settings

Navigating to Time Protocol Settings

To enable an NTP server, navigate to the **SYSTEM MANAGEMENT > Time Protocol** tab, and update the fields as described below.



Modify how the base station discovers the time

Network Time Protocol (NTP) ● Enabled ○ Disabled

NTP Server ntpserver01

Enabling or Disabling a Network Time Protocol (NTP) Server

To configure your AP/Bridge to use a network time protocol (NTP) server, first *enable* the use of NTP, and then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the AP/Bridge.)

Field	Description
Network Time Protocol	NTP provides a way for the AP/Bridge to obtain and maintain its time from a server on the network. Using an NTP server gives your VA4200 the ability to provide the correct time of day in log messages and session information. (See http://www.ntp.org for more general information on NTP.) Choose to either enable or disable use of a network time protocol (NTP) server: • Enabled • Disabled
NTP Server	If NTP is enabled, select the NTP server you want to use. You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.

Updating Settings

To apply your changes, click **Update**.

Configuring Radio Settings

The following sections describe how to configure Radio Settings on the Vivato Wi-Fi AP/Bridge:

- Understanding Radio Settings
- Configuring Radio Settings
- Updating Settings

Understanding Radio Settings

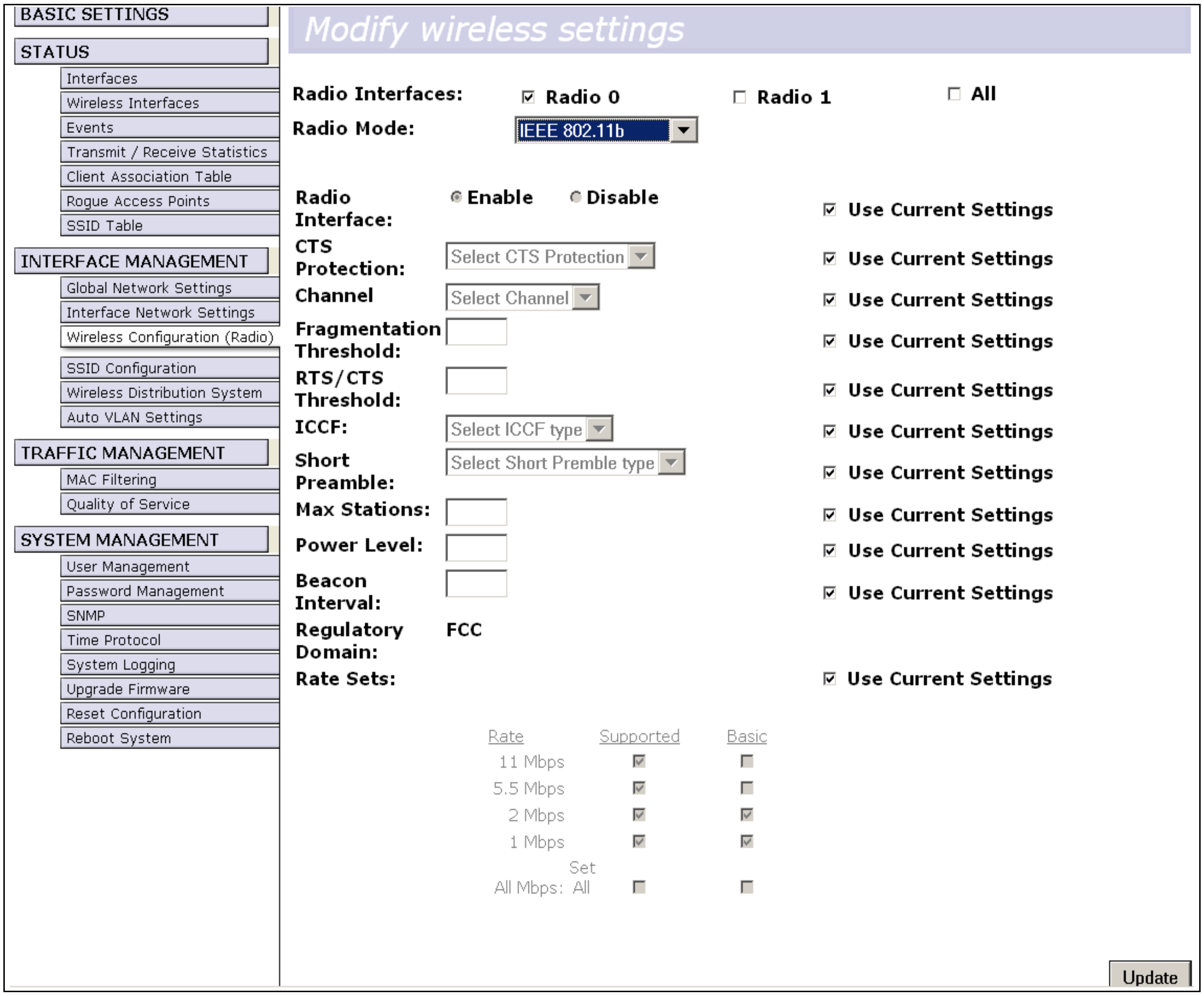
Radio settings on the Wireless Configuration (Radio) screen directly control the behavior of the two radio devices in the AP/Bridge. You can specify whether the radio is on or off, the transmit/receive frequency (channel), the beacon interval (amount of time between beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

The IEEE mode, along with other radio settings, are configured as described in ‘Navigating to Radio Settings’on page 51 and ‘Configuring Radio Settings’on page 52.

Navigating to Radio Settings

To specify radio settings, navigate to **INTERFACE MANAGEMENT > Wireless Configuration (Radio)** tab, and update the fields as described below.

Configuring Radio Settings



Modify wireless settings

Radio Interfaces: ☑ Radio 0 □ Radio 1 □ All

Radio Mode: IEEE 802.11b

Radio Interface: ● Enable ○ Disable ☑ Use Current Settings

CTS Protection: Select CTS Protection ☑ Use Current Settings

Channel Select Channel ☑ Use Current Settings

Fragmentation Threshold: ☑ Use Current Settings

RTS/CTS Threshold: ☑ Use Current Settings

ICCF: Select ICCF type ☑ Use Current Settings

Short Preamble: Select Short Premble type ☑ Use Current Settings

Max Stations: ☑ Use Current Settings

Power Level: ☑ Use Current Settings

Beacon Interval: ☑ Use Current Settings

Regulatory Domain: FCC

Rate Sets: ☑ Use Current Settings

Rate	Supported	Basic
11 Mbps	☑	□
5.5 Mbps	☑	□
2 Mbps	☑	☑
1 Mbps	☑	☑
Set All Mbps: All	□	□

To change an existing setting, de-select the corresponding "**Use Current Settings**" checkbox for that setting first, then change the setting. Be sure to leave the checkbox unchecked when you check **Update** button, otherwise the previous setting will continue to be used.

Field	Description
Radio Interfaces	The Vivato Wi-Fi AP/Bridge contains two radios. Select the check box next to the radio(s) to be configured, or select "All" to configure all radios at once.

Field(Continued)	Description(Continued)
Radio Mode	The *Mode* defines the *Physical Layer* (PHY) standard being used by the radio. Each radio can be set to operate only in IEEE 802.11a mode or in 802.11b mode, or allow simultaneous 802.11b and 802.11g operation (802.11b/g mode). To only allow 802.11g clients to associate with the AP/Bridge while in 802.11b/g mode, the radio's Supported Rates can be set to exclude those rates used by 802.11b clients (1, 2, 5.5, and 11 Mbps). See 'Rate Sets'on page 55.
Radio Interface	Specify whether you want one or both radios on or off by selecting `Enable` or `Disable.`
CTS Protection	CTS Protection is used to prevent data collisions when both 802.11b and 802.11g clients are present. When enabled, CTS Protection transmits a clear to send (CTS) message to itself at an 802.11b rate. This lets the 802.11b clients know that an 802.11g transmission is going to occur so that they will not transmit at the same time. This function is often called "CTS-to-self". Select between three available modes: • Auto - automatically uses CTS protection when an 802.11g client probe request is received. • Always Use - uses CTS-to-self before any clients are allowed to transmit. • Never Use - disables CTS-to-self protection.
Channel	The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. By default, the AP/Bridge uses channel 6 on all radios. When "Auto" is selected, the AP/Bridge analyzes signals in the area and sets the channel to the one anticipated to provide the best coverage.

Field(Continued)	Description(Continued)
Fragmentation Threshold	Specify an even number between 256 and 2,346 to set the frame size threshold in bytes. The *fragmentation threshold* is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation involves more overhead because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help *improve* network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens. By default, fragmentation is off. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.
RTS Threshold	Specify an RTS Threshold value, in bytes, between 0 and 2347. The RTS threshold specifies the frame size before a request to send (RTS) transmission is performed. This helps control traffic flow through the AP/Bridge, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
ICCF	Select `Enable` or `Disable`. When enabled, inter-client communication filtering (ICCF) prevents wireless clients associated on this radio from being able to communicate directly with other clients associating on this radio or on another radio on this AP/Bridge.
Short Preamble	Select `Enable` or `Disable`. When enabled, the short preamble uses fewer synchronization and CRC bits in order to allow additional data throughput. All 802.11g clients should support using a short preamble. However, 802.11b clients are not required to support short preamble operation and therefore using a short preamble may not work with them.
Max Stations	Specify the maximum number of stations allowed to access this AP/Bridge at any one time. You can enter a value between 0 and 2007.

Field(Continued)	Description(Continued)
Power Level	Provide a percentage value to set the transmit power for this AP/Bridge. The default is to have the AP/Bridge transmit using 100 percent of its power. ▶ Recommendations: • For most cases, we recommend keeping the default and having the transmit power set to 100 percent. This is more cost-efficient as it gives the AP/Bridge a maximum broadcast range, and reduces the number of VA4200s needed. • If a situation exists where clients outside the desired coverage area are able to access the wireless network, lowering the transmitted power will reduce the coverage area. However, reducing the power level may cause data throughput to some desired clients to be reduced below acceptable levels. Transmit power may also be reduced on one or more radios to reduce the effects of the AP/Bridge's signal on other 802.11 devices in that specific area.
Beacon Interval	Beacon frames are transmitted by a AP/Bridge at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 500 milliseconds (or 10 per second). The *Beacon Interval* value is set in milliseconds. Enter a value from 20 to 2000.
Rate Sets	Check the transmission rate sets you want the AP/Bridge to support and the basic rate sets you want the AP/Bridge to use when setting up communications. Rates are expressed in megabits per second. • **Supported Rate Sets** indicate rates that the AP/Bridge supports for data traffic to/from the client. These rates are advertised in the radio's beacons to let clients know what rates they can use. You can check multiple rates (click a checkbox to select or de-select a rate). The AP/Bridge will automatically choose the most efficient rate based on factors like error rates and signal strength. • **Basic Rate Sets** indicate rates that the AP/Bridge advertises to the network for the purposes of setting up communication with other VA4200s and client stations on the network. It is generally more efficient to have the radio broadcast a subset of its supported rate sets.

Updating Settings

To apply your changes, click **Update**. Any changes that were made to any of the radio settings are implemented at this time. If many changes were made, a progress bar is displayed to indicate that the changes are in the process of being made.

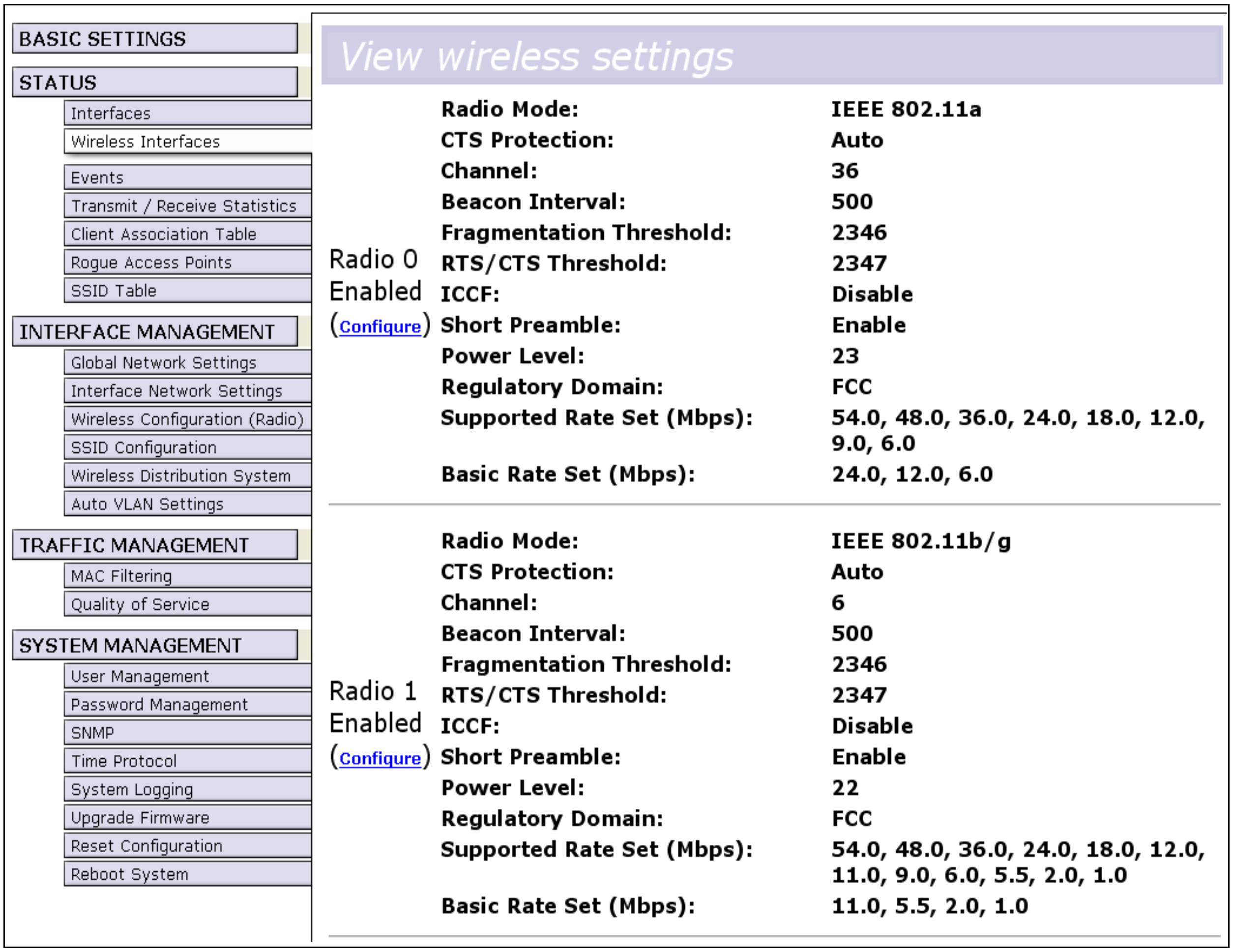
Viewing the Wireless Interface Settings

The Wireless Settings screen lists all of the wireless interfaces on the AP/Bridge and their current configuration.

Selecting "Configure" for any of the wireless interfaces displays the Radio screen. See Configuring Radio Settings for a description of what each parameter means and how to alter its current value.

Navigating to Wireless Settings

To view the current settings for each wireless interface in the AP/Bridge, select the **STATUS > Wireless Interfaces** tab.



View wireless settings

Radio 0 Enabled (Configure)

Radio Mode:	**IEEE 802.11a**
CTS Protection:	**Auto**
Channel:	**36**
Beacon Interval:	**500**
Fragmentation Threshold:	**2346**
RTS/CTS Threshold:	**2347**
ICCF:	**Disable**
Short Preamble:	**Enable**
Power Level:	**23**
Regulatory Domain:	**FCC**
Supported Rate Set (Mbps):	**54.0, 48.0, 36.0, 24.0, 18.0, 12.0, 9.0, 6.0**
Basic Rate Set (Mbps):	**24.0, 12.0, 6.0**

Radio 1 Enabled (Configure)

Radio Mode:	**IEEE 802.11b/g**
CTS Protection:	**Auto**
Channel:	**6**
Beacon Interval:	**500**
Fragmentation Threshold:	**2346**
RTS/CTS Threshold:	**2347**
ICCF:	**Disable**
Short Preamble:	**Enable**
Power Level:	**22**
Regulatory Domain:	**FCC**
Supported Rate Set (Mbps):	**54.0, 48.0, 36.0, 24.0, 18.0, 12.0, 11.0, 9.0, 6.0, 5.5, 2.0, 1.0**
Basic Rate Set (Mbps):	**11.0, 5.5, 2.0, 1.0**

Controlling Access by MAC Address Filtering

A *Media Access Control* (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example `FE:DC:BA:09:87:65`.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

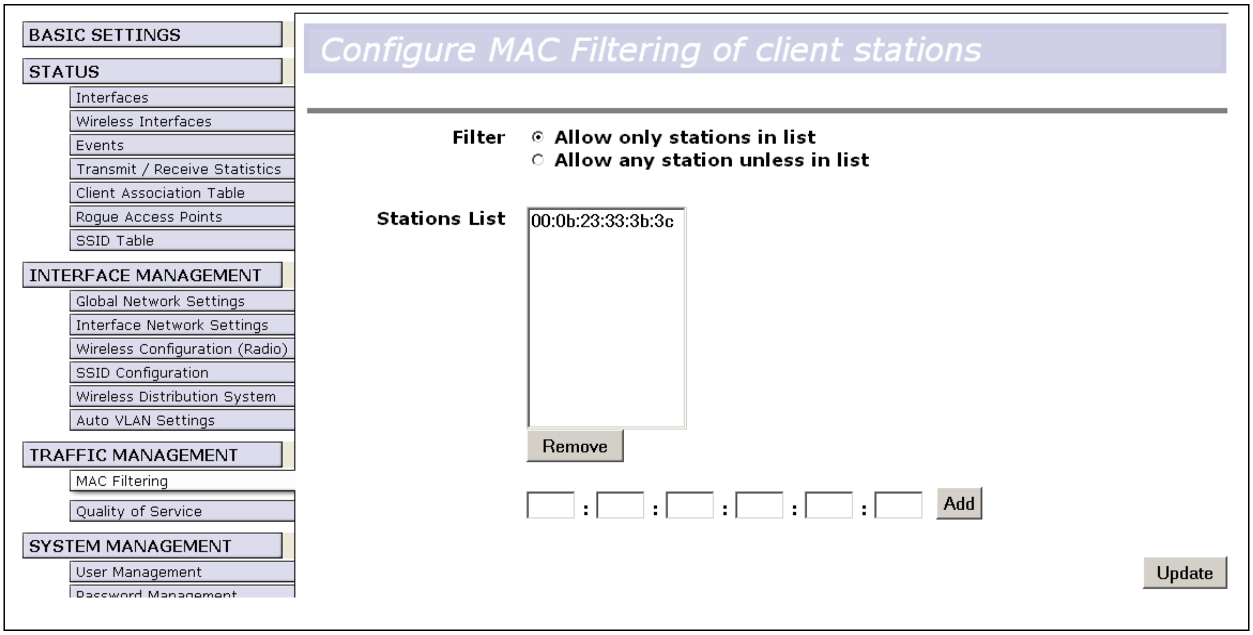
You can control client access to your wireless network by switching on "MAC Filtering" and specifying a list of MAC addresses. When MAC Filtering is on, clients are allowed or denied access based on their MAC address.

The following sections describe how to use MAC address filtering on the Vivato Wi-Fi AP/Bridge:

- Navigating to MAC Filtering Settings
- Using MAC Filtering
- Updating Settings

Navigating to MAC Filtering Settings

To enable filtering by MAC address, navigate to the **TRAFFIC MANAGEMENT > MAC Filtering** tab, and update the fields as described below.



Configure MAC Filtering of client stations

Filter ● Allow only stations in list
○ Allow any station unless in list

Stations List: 00:0b:23:33:3b:3c

Using MAC Filtering

This page allows you to control access to Vivato Wi-Fi AP/Bridge based on *Media Access Control* (MAC) addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed.

MAC Filtering settings apply to all radios.

Field	Description
Filter	To set the MAC Address **Filter**, click one of the following radio buttons: • **Allow only stations in the list.** In order for a client to gain access to the network, its MAC address must be entered into the Stations List. • **Allow any station unless in list.** Any station can gain access to the network unless its MAC address has been entered into the Stations List. This operation is typically used when a particular client is causing a problem of some kind and you want to exclude it from accessing the network.
Stations List	To add a MAC Address to Stations List, enter its 12 hexadecimal digits and click **Add**. The MAC Address is added to the Stations List. To remove a MAC Address from the Stations List, select the address and click **Remove**. The stations in the list will either be allowed or prevented from accessing the VA4200 based on how you set the Filter.

Updating Settings

To apply your changes, click **Update**.

Configuring Queues for Quality of Service (QoS)

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), video, and streaming media as well as traditional IP data over the Vivato Wi-Fi AP/Bridge.

The following sections describe how to configure Quality of Service queues on the Vivato Wi-Fi AP/Bridge:

- Understanding QoS
  - › 802.11e Standard
  - › 802.11e Standard
  - › QoS Queues and Parameters to Coordinate Traffic Flow
- Navigating to QoS Settings
- Configuring QoS Queues
- Updating Settings

Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to associate and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications like *Voice-over-IP* (VoIP) and streaming media.

Unlike typical data files which are less affected by variability in QoS, VoIP and streaming media must be sent in a specific order, at a consistent rate, and with minimum delay between Packet transmission. If the quality of service is compromised, the audio or video will be distorted.

802.11e Standard

QoS describes a range of technologies for controlling data streams on shared network connections. The task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting Jitter, Latency, and Packet Loss; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

As with all IEEE 802.11 working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable.

QoS Queues and Parameters to Coordinate Traffic Flow

Configuring QoS options on the Vivato Wi-Fi AP/Bridge consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for VoIP, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

For example, time-sensitive multimedia and VoIP are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

> Note: Regardless of the QoS settings, the AP/Bridge always prioritizes packets identified with the SpectraLink Radio Protocol type in the IPv4 header for SpectraLink® Voice Priority (SVP) operation.

The Vivato Wi-Fi AP/Bridge implements QoS with a custom extension to the traffic control mechanism in the Linux kernel. Our Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritization and routing based on the type of data being transmitted.

The VivatoVision UI provides a way for you to configure parameters on the queues.

QoS Queues and Type of Service (ToS) on Packets

QoS on the Vivato Wi-Fi AP/Bridge leverages existing information in the IP packet header related to Type of Service (ToS). Every IP packet sent over the network includes a ToS field in the header that indicates how the data should be prioritized and transmitted over the network. The ToS field consists of a 3 to 7 bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput since the critical consideration for FTP is the ability to transmit relatively large amounts of data in one go. Interactive feedback is a "nice-to-have" in this situation, but is less critical. VoIP data packets are set for minimum delay because that is a critical factor in quality and performance for that type of data.

The AP/Bridge examines the ToS field in the headers of all packets that pass through the VA4200. Based on the value in a packet’s ToS field, the VA4200 prioritizes the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- Data 0 (bulk). Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- Data 1 (best effort). Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 2 (interactive). Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- Data 3 (not used)

Using the QoS settings on the VivatoVision UI, you can configure parameters that determine how each queue is treated by the AP/Bridge.

> **Note**
>
> Wireless traffic travels:
>
> - Downstream from the AP/Bridge to the client station
> - Upstream from client station to AP/Bridge
> - Upstream from AP/Bridge to network
> - Downstream from network to AP/Bridge
>
> QoS settings on the Vivato Wi-Fi AP/Bridge affect only the first of these; *downstream* traffic flowing from the AP/Bridge to client station. The other phases of the traffic flow are not under control of the QoS settings on the VA4200.

DCF Control of Data Frames and Interframe Spaces

Data is transmitted over 802.11 wireless networks in *frames*. A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network.

> **Note**
>
> A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various *frame* types for management and control of the wireless infrastructure, and for data transmission. 802.11 frame types are (1) *management frames*, (2) *control frames*, and (3) *data frames*. Management and control frames (which manage and control the availability of the wireless infrastructure) automatically have higher priority for transmission.

802.11e uses *interframe spaces* to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

The Vivato Wi-Fi AP/Bridge supports the *Distribution Coordination Function* (DCF) as defined by the 802.11e standard. DCF, which is based on CSMA/CA protocol, defines the interframe space (IFS) between *data frames*. Data frames wait for an amount of time defined as the *DCF interframe space* (DIF) before transmitting.

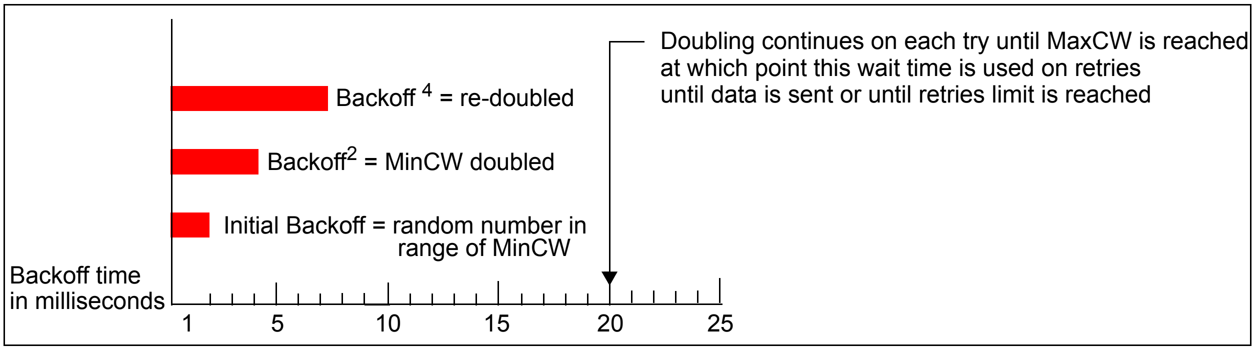
This parameter is configurable.

(Note that sending data frames in DIFs allows higher priority management and control frames to be sent in SIFs first.)

The DCF ensures that multiple AP/Bridges do not try sending data at the same time but instead wait until a channel is free.

Random Backoff and Minimum / Maximum Contention Windows

If a AP/Bridge detects that the medium is in use (busy), it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each AP/Bridge waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window*) increases exponentially up to a specified limit (*Maximum Contention Window*). The random delay avoids most of the collisions that would occur if multiple VA4200s got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.


Doubling continues on each try until MaxCW is reached at which point this wait time is used on retries until data is sent or until retries limit is reached
Backoff ^{4} = re-doubled
Backoff^2 = MinCW doubled
Initial Backoff = random number in range of MinCW
Backoff time in milliseconds
1
5
10
15
20
25

The random backoff used by the AP/Bridge is a configurable parameter. To describe the random delay, a "Minimum Contention Window" (MinCW) and a "Maximum Contention Window" (MaxCW) is defined.

- The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.

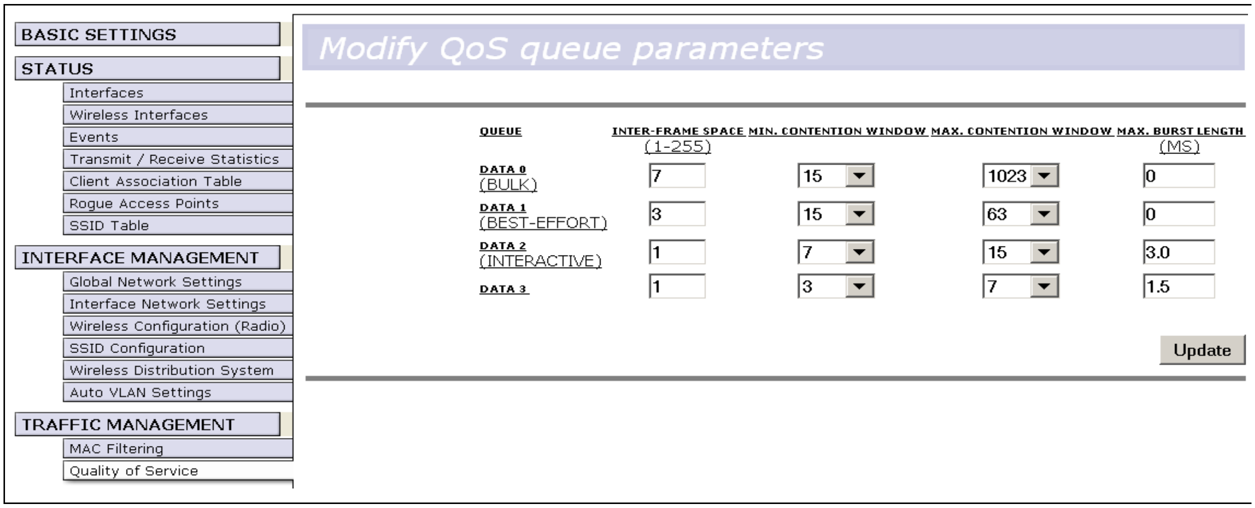
- If the first random backoff time ends before successful transmission of the data frame, the AP/Bridge increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

Packet Bursting for Better Performance

The Vivato Wi-Fi AP/Bridge includes 802.11e based *packet bursting* technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

Navigating to QoS Settings

To set up queues for QoS, navigate to the **TRAFFIC MANAGEMENT > Quality of Service** tab, and configure settings as described below.



Modify QoS queue parameters

QUEUE	INTER-FRAME SPACE (1-255)	MIN. CONTENTION WINDOW	MAX. CONTENTION WINDOW	MAX. BURST LENGTH (MS)
DATA 0 (BULK)	7	15	1023	0
DATA 1 (BEST-EFFORT)	3	15	63	0
DATA 2 (INTERACTIVE)	1	7	15	3.0
DATA 3	1	3	7	1.5

Configuring QoS Queues

Configuring Quality of Service (QoS) on the Vivato Wi-Fi AP/Bridge consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via *Contention Windows*) for transmission. The settings described here apply to data transmission behavior on the AP/Bridge only, not to that of the client stations.

Note	These settings apply to all radios, but the traffic for each radio is queued independently.

Field	Description
Queue	Queues are defined for different types of data transmitted from VA4200-to-station: **Data 0 (bulk)** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For information purposes, the hexadecimal values to describe this queue are in the following ranges: 0X02 - 0X03 0X08 - 0X0F **Data 1 (best effort)** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. For information purposes, the hexadecimal values to describe this queue are in the following ranges: 0x00 - 0X01 0X04 - 0X07 0X18 - 0X1F **Data 2 (interactive)** Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. For information purposes, the hexadecimal values to describe this queue are in the following ranges: 0x10 - 0X17 **Data 3 (not used)** For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 59.
Inter-Frame Space	The Interframe Space specifies a wait time (in milliseconds) for *data frames*. For more information, see “DCF Control of Data Frames and Interframe Spaces” on page 61.

Field	Description
Min. Contention Window	This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the *Minimum Contention Window* is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 61.
Max. Contention Window	The value specified here in the *Maximum Contention Window* is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 61.
Max. Burst Length	This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A *packet burst* is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. For more information, see “Packet Bursting for Better Performance” on page 62.

Updating Settings

To apply your changes, click **Update**.

Configuring the Wireless Distribution System (WDS)

The Vivato Wi-Fi AP/Bridge lets you connect multiple AP/Bridges and AP/Bridges together using a Wireless Distribution System (WDS). WDS allows AP/Bridges and AP/Bridges to communicate with one another wirelessly in a standardized way. This capability is critical in providing an uninterrupted experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The following sections describe how to configure the WDS on the Vivato Wi-Fi AP/Bridge:

- Understanding the Wireless Distribution System
  - › Using WDS to Bridge Distant Wired LANs
  - › Using WDS to Extend the Network Beyond the Wired Coverage Area
  - › Backup Links and Unwanted Loops in WDS Bridges
  - › Security Considerations Related to WDS Bridges
- Navigating to WDS Settings
- Configuring WDS Settings
  - › Example of Configuring a WDS Link
- Updating Settings

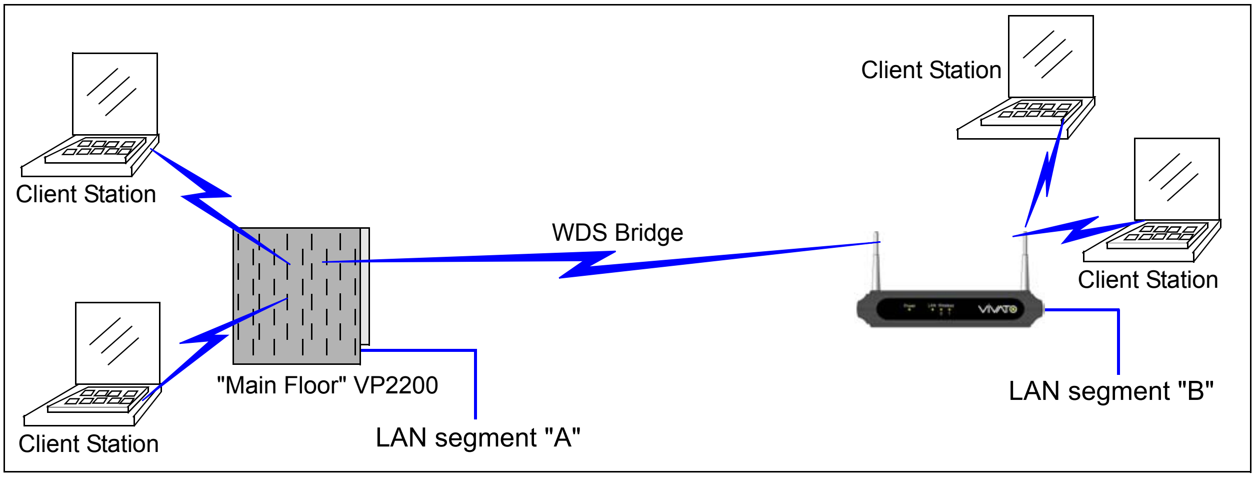
Understanding the Wireless Distribution System

A *Wireless Distribution System* (WDS) connects AP/Bridges, known as Basic Service Sets (BSS), to form what is known as an *Extended Service Set* (ESS).

Note	A BSS generally equates to a AP/Bridge (deployed as a single-VA4200 wireless "network"), except in cases where multi-BSSID features make a single AP/Bridge look like two or more AP/Bridges to the network. In such cases, the AP/Bridge has multiple unique BSSIDs.

Using WDS to Bridge Distant Wired LANs

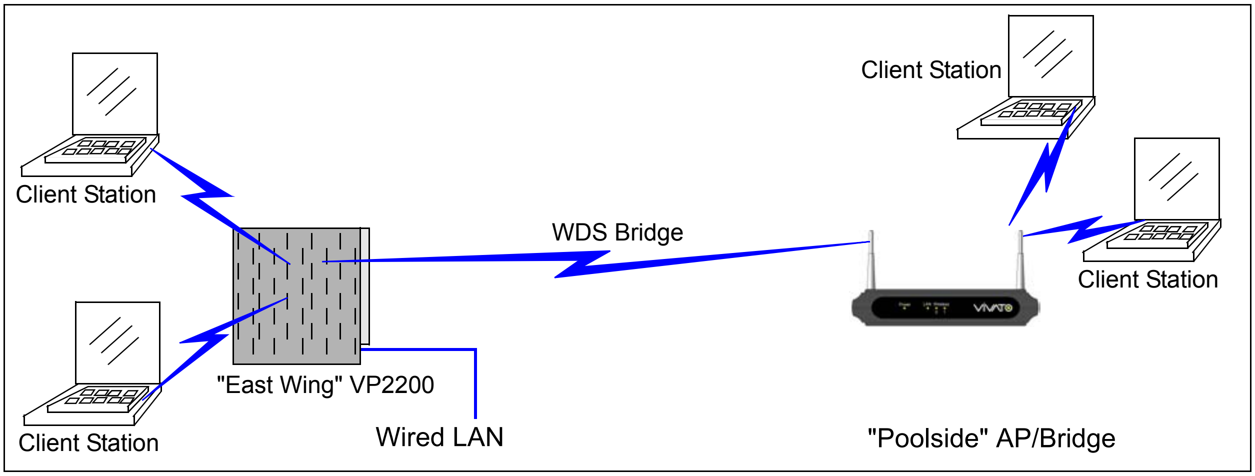
In an ESS, each AP/Bridge or AP/Bridge serves part of an extended wireless coverage area. You can use WDS to bridge distant Ethernets to create a single LAN. For example, suppose you have a AP/Bridge that is connected to LAN segment "A" by Ethernet and is serving multiple client stations on the main floor of a building, and an AP/Bridge that is connected to LAN segment "B" and is serving stations in conference area behind the main floor. You can bridge the AP/Bridge and the AP/Bridge using a WDS link between them to create a single network in both areas.



Using WDS to Extend the Network Beyond the Wired Coverage Area

An ESS can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have a AP/Bridge which is connected to the network by Ethernet and serving multiple client stations in one area ("East Wing" in our example) but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling. You can solve this problem by placing an AP/Bridge closer to second group of stations ("Poolside" in our example) and bridge the two VA4200s with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations.



Backup Links and Unwanted Loops in WDS Bridges

Another use for WDS bridging, the creation of backup links, is not supported on the VA4200. The topic is included here to emphasize that you should not try to use WDS in this way; backup links will result in unwanted, endless loops of data traffic.

The VA4200 does not provide *Spanning Tree Protocol* (STP). Without STP, it is possible that both connections (paths) may be active at the same time, and result in an endless loop of traffic on the LAN.

Therefore, never create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see the "Do not create loops" note under “Configuring WDS Settings” on page 69.

Security Considerations Related to WDS Bridges

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both AP/Bridges in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

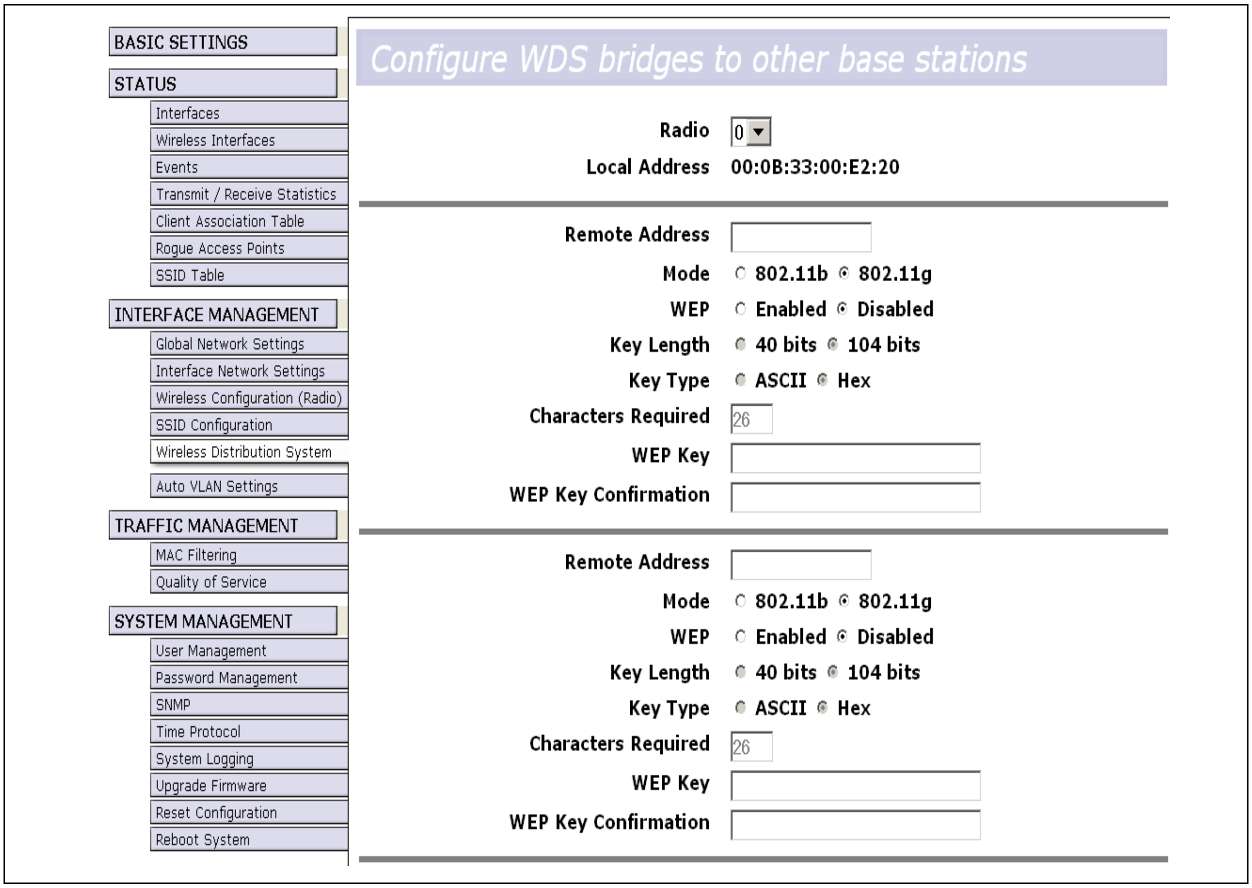
You can enable Static WEP on the WDS link (bridge). When WEP is enabled, all data exchanged between the two AP/Bridges in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP is the only security mode available for the WDS link, and it does not provide effective data protection to the level of other security modes available for service to client stations. If you use WDS on a LAN intended for secure wireless traffic you are putting your network at risk. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge AP/Bridges on the Internal network unless you are not concerned about the security risk for data traffic on that network.

For more information about the effectiveness of different security modes, see “Configuring Security” on page 91. This topic also covers use of plain text security mode for VA4200-to-station traffic on the Guest network, which is intended for less sensitive data traffic.

Navigating to WDS Settings

To specify the details of traffic exchange from this AP/Bridge to others, navigate to the **INTERFACE MANAGEMENT > Wireless Distribution System** tab, and update the fields as described below.



Configure WDS bridges to other base stations

Radio 0

Local Address 00:0B:33:00:E2:20

Remote Address

Mode ○ 802.11b ● 802.11g

WEP ○ Enabled ● Disabled

Key Length ○ 40 bits ● 104 bits

Key Type ○ ASCII ● Hex

Characters Required 26

WEP Key

WEP Key Confirmation

Remote Address

Mode ○ 802.11b ● 802.11g

WEP ○ Enabled ● Disabled

Key Length ○ 40 bits ● 104 bits

Key Type ○ ASCII ● Hex

Characters Required 26

WEP Key

WEP Key Confirmation

Configuring WDS Settings

The following notes summarize some critical guidelines regarding WDS configuration. Please read all the notes before proceeding with WDS configuration.

Notes	
	• The only security mode available on the WDS link is Static WEP, which is not particularly secure. Do not use WDS to bridge AP/Bridges on the Internal network unless you are not concerned about the security risk for data traffic on that network. • When using WDS, be sure to configure WDS settings on *both* AP/Bridges participating in the WDS link. • You can have only one WDS link between any pair of AP/Bridges or to an AP/Bridge. That is, a remote MAC (peer) address may appear only once on the WDS page for a particular AP/Bridge. • Both devices participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See "Configuring Radio Settings" on page 51 for information on configuring the Radio mode and channel.) • **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevents unwanted loops, is not provided on the VA4200. Keep these rules in mind when working with WDS on this release of the Vivato Wi-Fi AP/Bridge: • Only one path should exist between two AP/Bridges or a AP/Bridge and an AP/Bridge; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both. • Do not create "backup" links. • If you can trace more than one path between any pair of VA4200s going through any combination of Ethernet or WDS links, you have a loop..

Up to four WDS links can be configured on each radio (a total of 8 WDS links). The following information must be entered to configure each link:

Table 1 WDS Interface Settings

Field	Description
Radio	**Select the radio:** Select the Radio for each WDS link. The rest of the settings for the link apply to the radio selected in this field. The read-only "Local Address" will change depending on which Radio you select here.
Local Address	Indicates the Media Access Control (MAC) addresses for this radio. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the AP/Bridge or interface. For each WDS link on the VA4200, the Local Address reflects the MAC address for the Internal interface on the selected radio (Radio One on `WLAN0` or Radio Two `WLAN1, ...etc`).
Remote Address	Specify the MAC address of the radio on the AP/Bridge or AP/Bridge used for the other end of the WDS link. This is sometimes known as the "peer" address.

Field(Continued)	Description(Continued)
Mode	Select 802.11b or 802.11g. Be sure to use the same mode on the device at the other end of the WDS link.
WEP	Specify whether you want *Wired Equivalent Privacy* (WEP) encryption enabled for the WDS link. • Enabled • Disabled *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both AP/Bridges on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.
Key Length	If WEP is enabled, specify the length of the WEP key: • 40 bits • 104 bits
Key Type	If WEP is enabled, specify the WEP key type: • ASCII • Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Key	Enter the WEP key using the required number and type of characters. Enter the same key a second time (**WEP Key Confirmation**). If you selected "ASCII", enter any combination of `0-9` and `a-z` or `A-Z`. If you selected "HEX", enter hexadecimal digits (any combination of `0-9` and `a-f` or `A-F`). These are the RC4 encryption keys shared with the stations using the AP/Bridge.

Example of Configuring a WDS Link

When using WDS, be sure to configure WDS settings on both devices on the WDS link.

For example, to create a WDS link between a pair of AP/Bridges "**MyVBS1**" and "**MyVBS2**" do the following:

1. Open the VivatoVision Web pages for MyVBS1 by entering the IP address for MyVBS1 as a URL in the Web browser address bar in the following form:

   `https://`*IPAddressOfAP/Bridge*

   where *IPAddressOfAP/Bridge* is the address of MyVBS1.

2. Navigate to the Wireless Distribution System tab on MyVBS1 VivatoVision Web pages.

   The MAC address for MyVBS1 (the AP/Bridge you are currently viewing) will show as the "Local

Address" at the top of the page.

3. Configure a WDS interface for data exchange with MyVBS2.

   Start by entering the Local Address of the radio used for the WDS link on MyVBS2 as the "Remote Address". Fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings (click Update).

4. Navigate to the radio settings on the VivatoVision Web pages (**INTERFACE MAANGEMENT > Wireless Configuration (Radio)**) to verify or set the mode and the radio channel on which you want MyVBS1 to broadcast.

   Remember that the two AP/Bridges participating in the link, MyVBS1 and MyVBS2, must be set to the same Mode and be transmitting on the same channel.

   For our example, let's say we're using IEEE 802.11b Mode and broadcasting on Channel 6.

5. Now repeat the same steps for MyVBS2:

   - Open VivatoVision Web pages for MyVBS2 by using MyVBS2's IP address in a URL.

   - Navigate to the WDS tab on MyVBS2 VivatoVision Web pages. (MyVBS2's MAC address will show as the "Local Address".)

   - Configure a WDS interface for data exchange with MyVBS1, starting with the Local Address of the radio used for the WDS link on MyVBS1.

   - Navigate to the radio settings for MyVBS2 to verify that it is using the same mode and broadcasting on the same channel as MyVBS1. (For our example Mode is 802.11b and the channel is 6.)

   - Be sure to save the settings by clicking **Update**.

Updating Settings

To apply your changes, click **Update**.

Setting the User Password

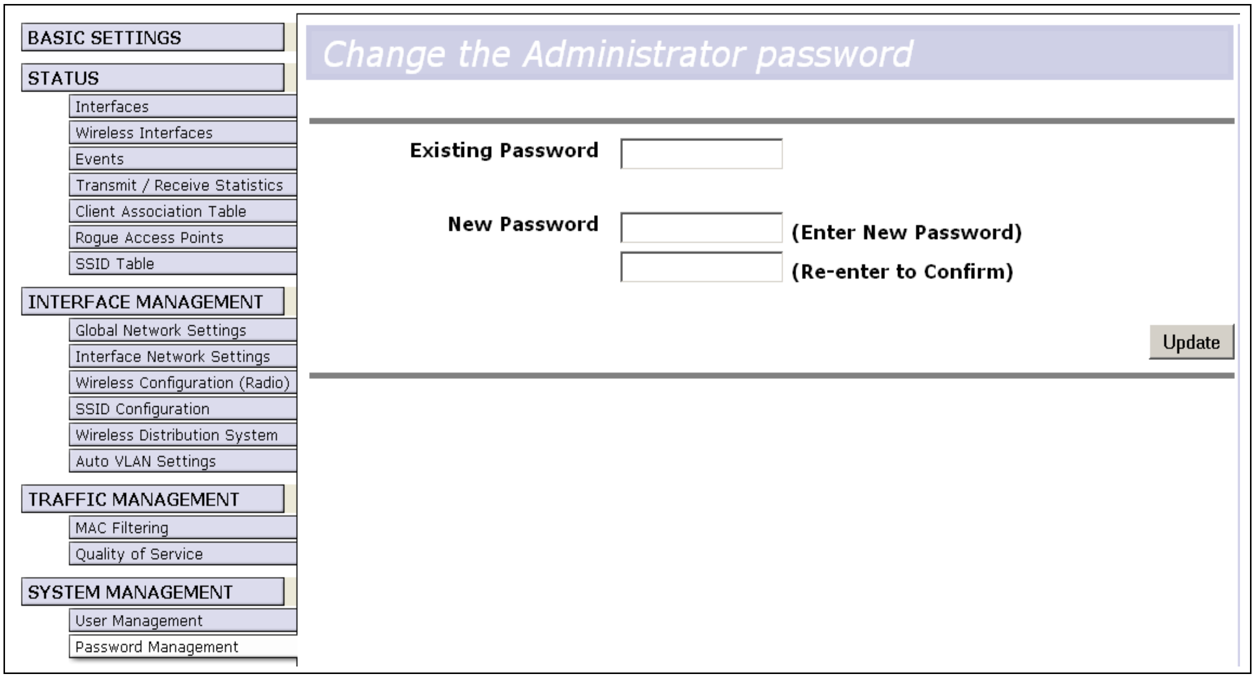
The administrator password controls access to the VivatoVision Web pages for the Vivato Wi-Fi AP/Bridge. This setting is also available on the Network > Basic Settings VivatoVision page. The new password is updated when you set the administration password in either place and apply the change.

The following sections describe how to configure the Administrator password on the Vivato Wi-Fi AP/Bridge:

- Navigating to Administrator Password Setting
- Setting the User Password
- Updating Settings

Navigating to Administrator Password Setting

To set the administrator password, navigate to the **SYSTEM MANAGEMENT > Password Management** tab, and update the fields as described below.



Change the Administrator password

Existing Password

New Password (Enter New Password)

(Re-enter to Confirm)

Setting the User Password

To set a new administrator password, enter the existing password and the new password (twice). The password setting requires that you know the existing password before you can change it. This is to prevent an unauthorized person from changing the password in a case where you leave an open browser unattended.

Field	Description
Existing Password	Enter the existing password.
New Password	Enter a new administrator password. The text you enter will be displayed as "*" characters to prevent others from seeing your password as you type. The User password must be an alphanumeric strings of up to 32 characters. Do not use special characters or spaces. Re-enter the new administrator password to confirm that you typed it as intended.

Updating Settings

To apply your changes, click **Update**.

Maintenance and Monitoring

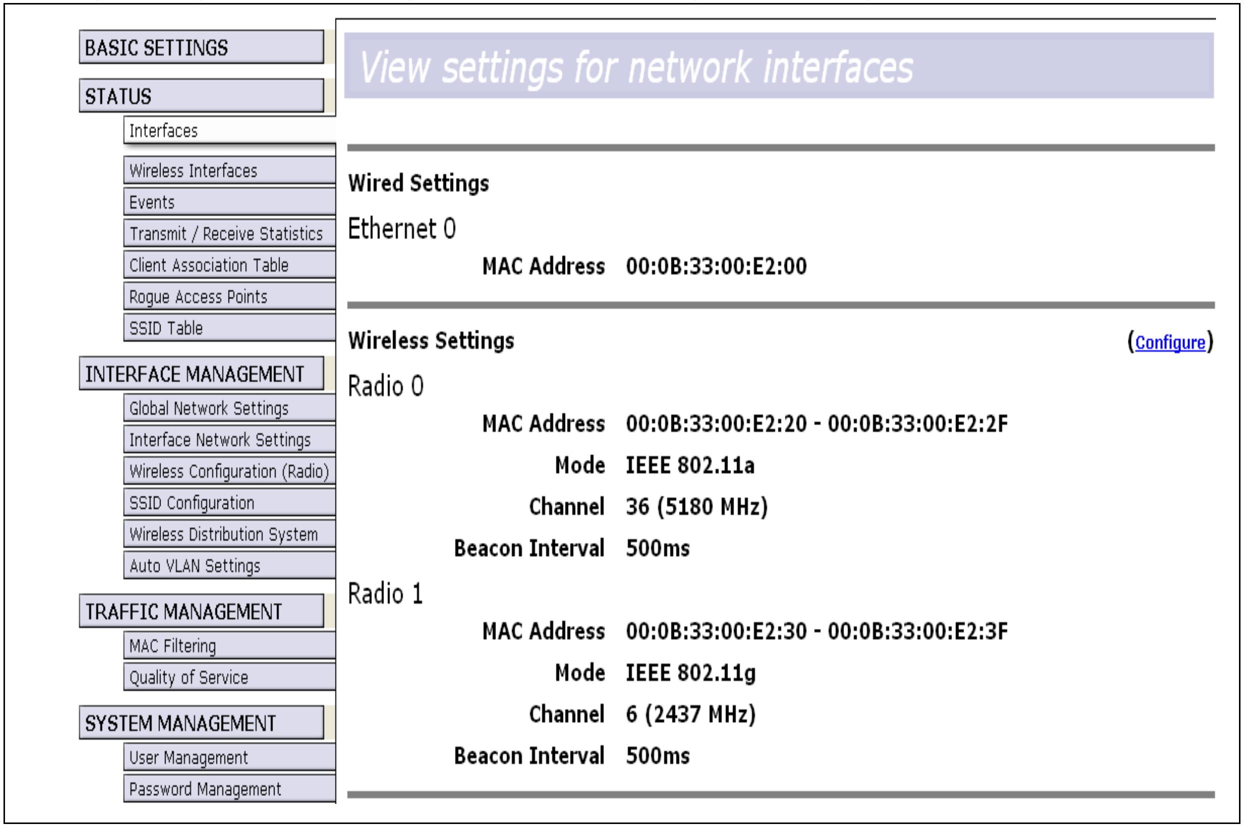
The following maintenance and monitoring topics are covered.

- Interfaces
- Event Log
- Transmit/Receive Statistics
- Associated Wireless Clients
- Resetting the Configuration
- Upgrading the Firmware
- Rogue Access Points

Interfaces

To view wired (Ethernet) and wireless (WLAN) settings, navigate to **STATUS > Interfaces**.

This page displays the **Wired Settings** and the **Wireless Settings** for the AP/Bridge.



Wired Settings

Ethernet 0

MAC Address	00:0B:33:00:E2:00

Wireless Settings

Radio 0

MAC Address	00:0B:33:00:E2:20 - 00:0B:33:00:E2:2F
Mode	IEEE 802.11a
Channel	36 (5180 MHz)
Beacon Interval	500ms

Radio 1

MAC Address	00:0B:33:00:E2:30 - 00:0B:33:00:E2:3F
Mode	IEEE 802.11g
Channel	6 (2437 MHz)
Beacon Interval	500ms

Wired Settings

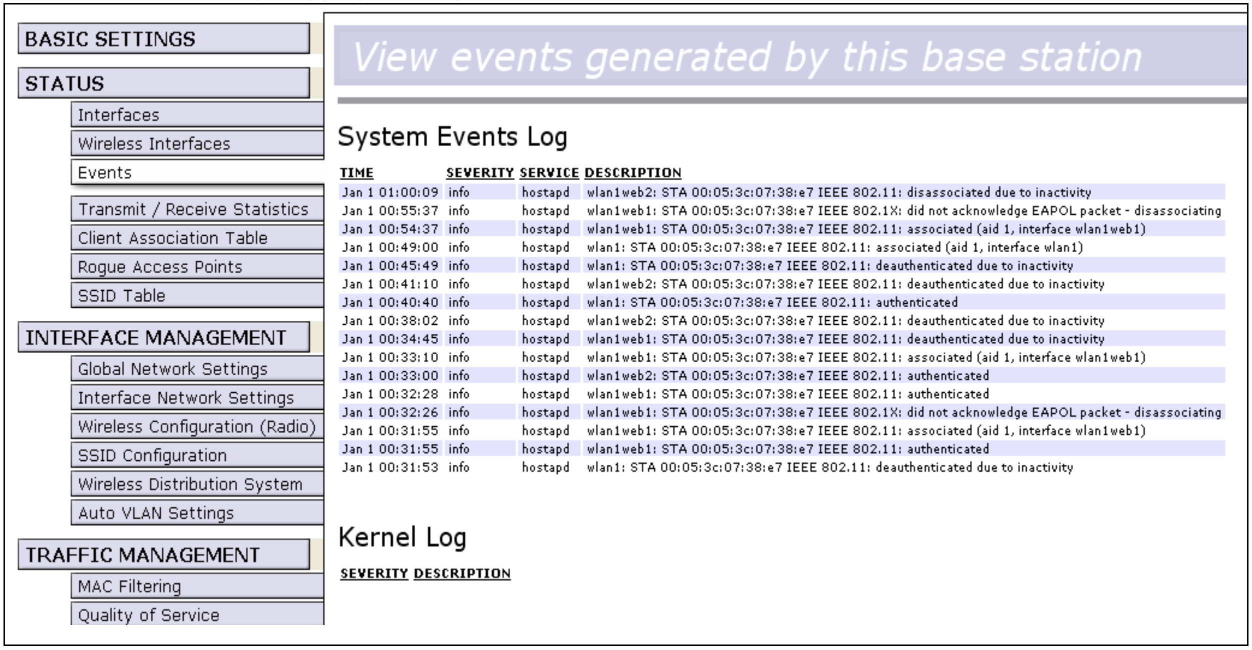
The MAC addresses for the Ethernet port are displayed. These are assigned at the time of manufacture, and cannot be changed.

Wireless Settings

The current Wireless Interface settings include the MAC addresses (read-only), the Mode (802.11a, 802.11b, or 802.11g) and the channel number, and the beacon Interval. See “Configuring Radio Settings” on page 51 for more information.)

Event Log

To view a list of the AP/Bridge’s system operating message, navigate to **STATUS > Events** on the VivatoVision Web pages. Event logging is enabled/disabled on the **SYSTEM MANAGEMENT> System Logging** screen. See “Enabling Logging” on page 112.



View events generated by this base station

System Events Log

TIME	SEVERITY	SERVICE	DESCRIPTION
Jan 1 01:00:09	info	hostapd	wlan1web2: STA 00:05:3c:07:38:e7 IEEE 802.11: disassociated due to inactivity
Jan 1 00:55:37	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.1X: did not acknowledge EAPOL packet - disassociating
Jan 1 00:54:37	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: associated (aid 1, interface wlan1web1)
Jan 1 00:49:00	info	hostapd	wlan1: STA 00:05:3c:07:38:e7 IEEE 802.11: associated (aid 1, interface wlan1)
Jan 1 00:45:49	info	hostapd	wlan1: STA 00:05:3c:07:38:e7 IEEE 802.11: deauthenticated due to inactivity
Jan 1 00:41:10	info	hostapd	wlan1web2: STA 00:05:3c:07:38:e7 IEEE 802.11: deauthenticated due to inactivity
Jan 1 00:40:40	info	hostapd	wlan1: STA 00:05:3c:07:38:e7 IEEE 802.11: authenticated
Jan 1 00:38:02	info	hostapd	wlan1web2: STA 00:05:3c:07:38:e7 IEEE 802.11: deauthenticated due to inactivity
Jan 1 00:34:45	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: deauthenticated due to inactivity
Jan 1 00:33:10	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: associated (aid 1, interface wlan1web1)
Jan 1 00:33:00	info	hostapd	wlan1web2: STA 00:05:3c:07:38:e7 IEEE 802.11: authenticated
Jan 1 00:32:28	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: authenticated
Jan 1 00:32:26	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.1X: did not acknowledge EAPOL packet - disassociating
Jan 1 00:31:55	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: associated (aid 1, interface wlan1web1)
Jan 1 00:31:55	info	hostapd	wlan1web1: STA 00:05:3c:07:38:e7 IEEE 802.11: authenticated
Jan 1 00:31:53	info	hostapd	wlan1: STA 00:05:3c:07:38:e7 IEEE 802.11: deauthenticated due to inactivity

Kernel Log

SEVERITY	DESCRIPTION

The **Events** page lists the most recent events generated by this AP/Bridge.

The System Events Log lists stations associating, being authenticated, and other occurrences.

The Kernel Log lists error conditions, such as dropped frames.

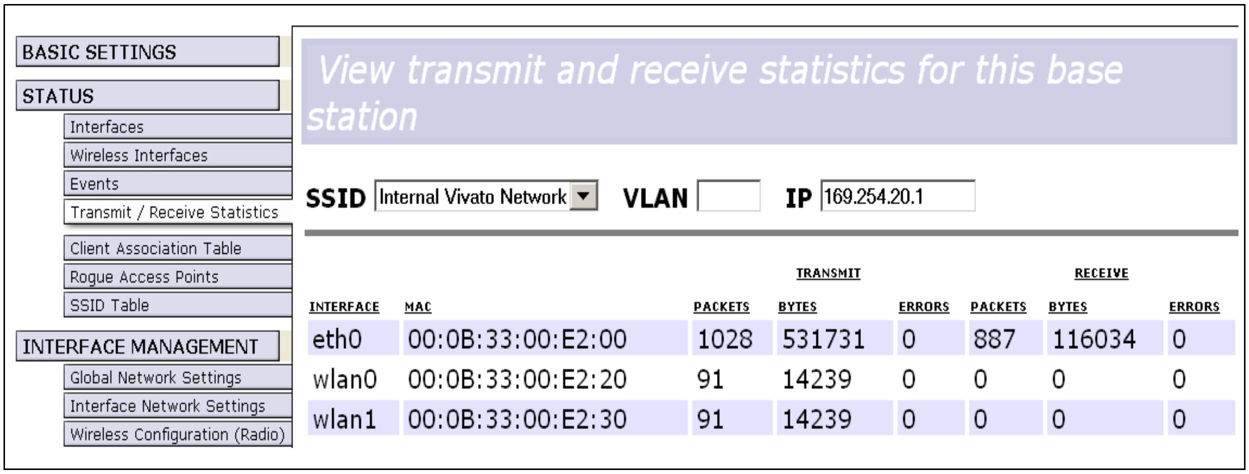
Note

The Vivato Wi-Fi AP/Bridge acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as *Greenwich Mean Time*). You need to convert the reported time to your local time.

For information on setting the network time protocol, see “Enabling the Network Time Protocol Server” on page 49.

Transmit/Receive Statistics

To view transmit/receive statistics for a particular SSID, navigate to **STATUS > Transmit/Receive Statistics** on the VivatoVision Web pages and select the SSID that you want to monitor.



View transmit and receive statistics for this base station

SSID Internal Vivato Network VLAN IP 169.254.20.1

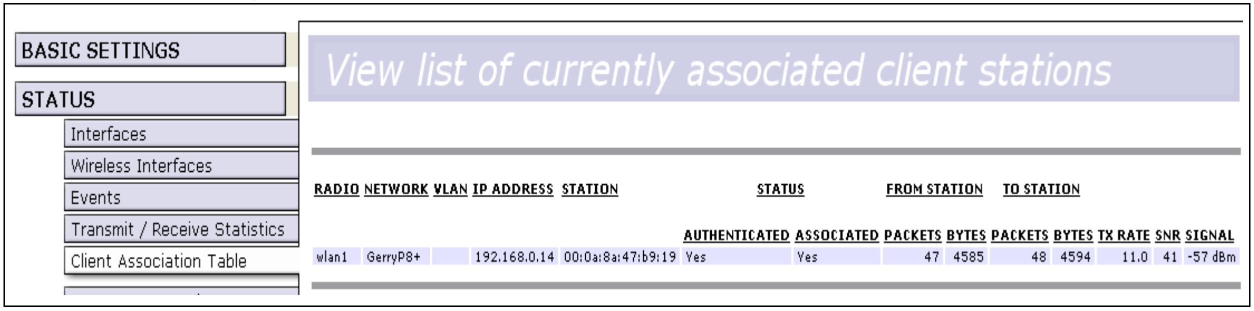
		TRANSMIT			RECEIVE		
INTERFACE	MAC	PACKETS	BYTES	ERRORS	PACKETS	BYTES	ERRORS
eth0	00:0B:33:00:E2:00	1028	531731	0	887	116034	0
wlan0	00:0B:33:00:E2:20	91	14239	0	0	0	0
wlan1	00:0B:33:00:E2:30	91	14239	0	0	0	0

This page provides some basic information about the SSID and a real-time display of the transmit and receive statistics for this AP/Bridge as described in the following table. All transmit and receive statistics shown are totals since the AP/Bridge was last started. If the AP/Bridge is rebooted, these figures indicate transmit/receive totals since the re-boot.

Field	Description
SSID	Select the SSID to monitor. The VLAN ID number and IP address of that SSID are also displayed if they have been previously assigned.
VLAN	This is the VLAN ID associated with this SSID. Only the primary wireless network does not require a VLAN ID to be specified..
IP	The IP address assigned to this SSID (when used).
INTERFACE	These are the interfaces that are members of the selected SSID.
MAC Address	Media Access Control (MAC) address for the specified interface. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. The Vivato Wi-Fi AP/Bridge has a unique MAC address for each interface, including a different MAC address for each interface on each of its radios.
Transmit and Receive Information	
Packets	Indicates the total number of packets sent (in the Transmit table) or received (in the Received table) by this AP/Bridge.
Bytes	Indicates total number of bytes sent (in the Transmit table) or received (in the Received table) by this AP/Bridge.
Errors	Indicates total errors related to sending and receiving data through this interface.

Associated Wireless Clients

To view the client stations associated with the AP/Bridge, navigate to **STATUS > Client Association Table** on the VivatoVision Web pages..



View list of currently associated client stations

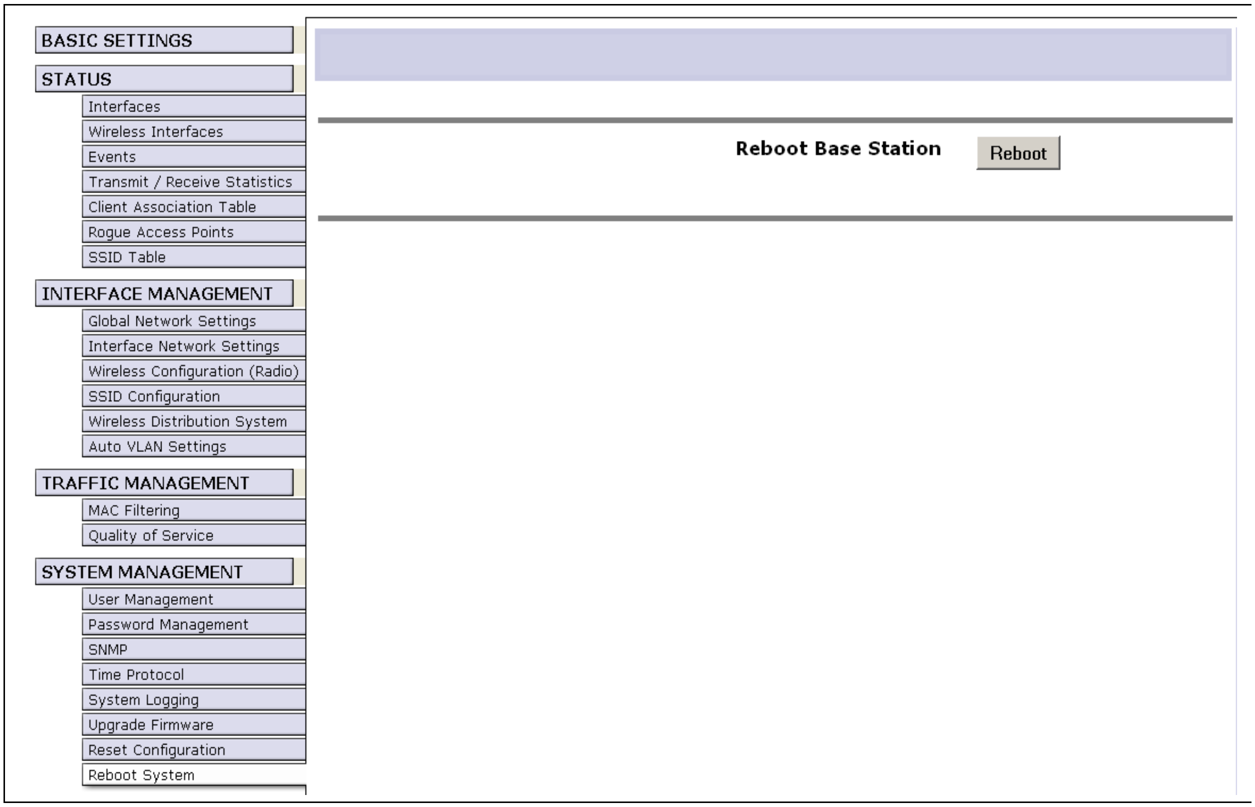
RADIO	NETWORK	VLAN	IP ADDRESS	STATION	STATUS		FROM STATION		TO STATION				
					AUTHENTICATED	ASSOCIATED	PACKETS	BYTES	PACKETS	BYTES	TX RATE	SNR	SIGNAL
wlan1	GerryP8+		192.168.0.14	00:0a:8a:47:b9:19	Yes	Yes	47	4585	48	4594	11.0	41	-57 dBm

Field	Description
RADIO	This is the wireless interface that the client is associating through.
NETWORK	This is the SSID to which the client is associated.
VLAN	The is the VLAN ID number used for this network.
IP ADDRESS	The associated client's IP address.
STATION	The MAC address of the client.
AUTHENTICATED	Shows if the client has authenticated ("Yes") or has not authenticated ("No").
ASSOCIATED	Shows if the client is associated ("Yes") or is not associated ("No").
FROM STATION	The number of packets and bytes from the client.
TO STATION	The number of packets and bytes to the client.
SNR	The signal to noise ratio (SNR) of the signal from the client. The higher the ratio, the "cleaner" the signal. An minimum SNR of 12 is typically required to provide 11 Mbps operation in 802.11b mode.
SIGNAL	The strength of the signal from the client in dBm. This value can be used to track the relative signal strength while the client moves from one location to another.

Rebooting the AP/Bridge

For maintenance purposes or as a troubleshooting measure, you can reboot the Vivato Wi-Fi AP/Bridge as follows.

Click the **SYSTEM MANAGEMENT > Reboot** tab.



Reboot Base Station

6. Click the **Reboot** button.

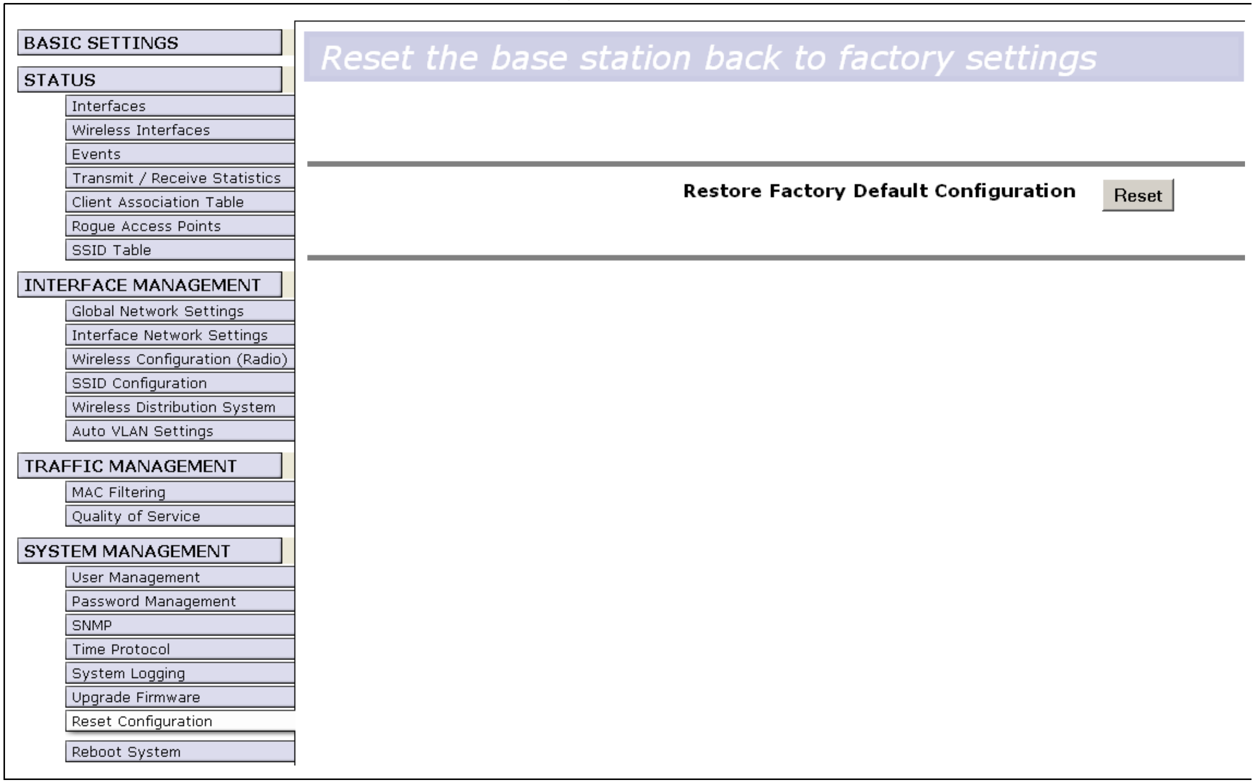
The VA4200 reboots. See also “Resetting the Configuration”.

Resetting the Configuration

If you are experiencing extreme problems with the Vivato Wi-Fi AP/Bridge and have tried all other troubleshooting measures, use the **Reset Configuration** function. This will restore factory defaults and clear all settings, including the static IP address (if one was assigned), new passwords, wireless interface settings, WDS connections, and SSID and VLAN configurations.

NOTE: After resetting the AP/Bridge, the VivatoVision web pages must be accessed using the default IP address of 169.254.20.1. For information on the factory default settings, see “Default Settings for the Vivato Wi-Fi AP/Bridge” on page 21.

1. Click the **SYSTEM MANAGEMENT > Reset Configuration** tab.



Reset the base station back to factory settings

Restore Factory Default Configuration

2. Click the **Reset** button.

   Factory defaults are restored.

Upgrading the Firmware

As new versions of the Vivato Wi-Fi AP/Bridge firmware become available, you can upgrade the firmware on your devices to take advantages of new features and enhancements.

1. Set Up a User Account on the Vivato Customer Support Website

   The latest firmware is available from the Vivato Customer Support site at www.vivato.net/access_cs.html.

   To receive a password to access the Knowledge Base and firmware downloads, enter and submit the required account information on the Customer Support entry page. Once your information is verified, a password is e-mailed to you (typically within one working day) that is used with your e-mail address to access the support information. The support site also includes a wide variety of troubleshooting and informative documents.

2. Search the Knowledge Base For the Latest Firmware

   Search the Customer Support Knowledge Base for the keyword "firmware", and select the latest entry for the VA4200 Indoor AP/Bridge.

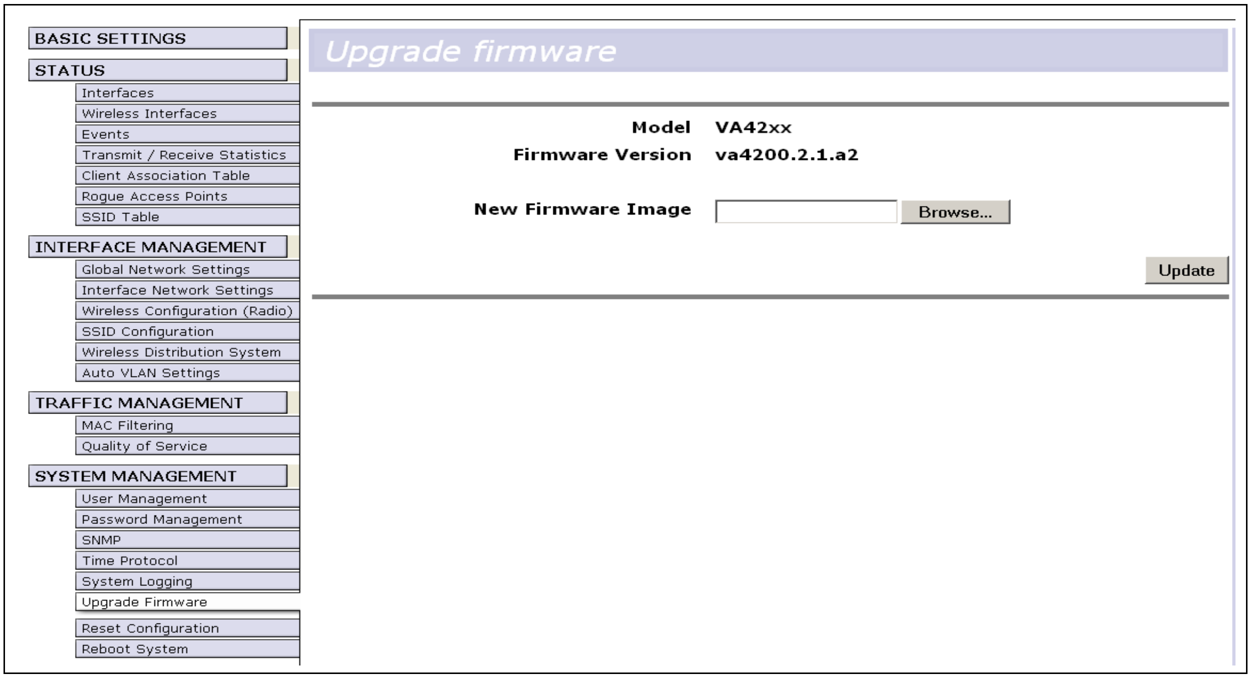
3. Click on the firmware file listed under "File Attachments", and select to "Save" the file to your local PC.

Note The firmware upgrade file must be in the format `VA4200<version>.bin`

4. Navigate to **SYSTEM MANAGEMENT > Upgrade Firmware** on the VivatoVision Web pages. Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

5. Click on **Browse,** and select the downloaded firmware file on your local PC.

6. Select **Update** button to begin the update process.



Upgrade firmware

Model VA42xx

Firmware Version va4200.2.1.a2

New Firmware Image

Upon clicking **Update**, a popup confirmation window is displayed that describes the upgrade process.

Click **OK** to confirm the upgrade, and start the process.

Caution	The firmware upgrade process begins once you click Update and then OK in the popup confirmation window. The upgrade process may take several minutes during which time the AP/Bridge will be unavailable. Do not power down the AP/Bridge while the upgrade is in process. When the upgrade is complete, the AP/Bridge will restart and resume normal operation using your existing configuration settings.

Verifying the Firmware Upgrade

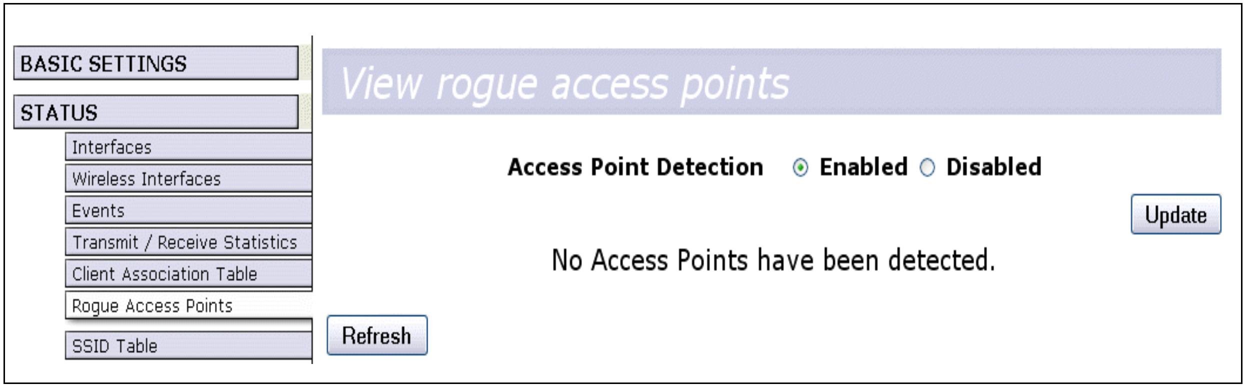
To verify that the firmware upgrade completed successfully, check the firmware version shown on the **SYSTEM MANAGEMENT > Upgrade** tab (and also on the Basic Settings tab). If the upgrade was successful, the updated version name or number will be indicated.

Rogue Access Points

The status page for rogue access points provides real-time statistics for all AP/Bridges, Wi-Fi base stations, and access points within range of the AP/Bridge on which you are viewing the VivatoVision Web pages. This information can be extremely helpful in identifying possible sources of interference from devices that are sharing the 802.11 frequency bands..

> **Note** When enabled, the Rogue Access Point feature uses each wireless interface’s receiver to detect other devices. This can cause some loss in throughput to wireless clients. Therefore, DO NOT LEAVE THIS FUNCTION ENABLED WHEN NOT NEEDED.

Navigate to **STATUS > Rogue Access Points**



Access Point Detection ● **Enabled** ○ **Disabled**

No Access Points have been detected.

Information provided on neighboring AP/Bridges is described in the following table.

Field	Description
MAC Address	Shows the MAC address of a neighboring AP/Bridge or access point. A MAC address is a hardware address that uniquely identifies each node of a network.
RADIO	This is the radio that received this signal..
Beacon Interval	Shows the Beacon interval being used by this AP/Bridge. Beacon frames are transmitted by a AP/Bridge at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on the INTERFACE MANAGEMENT > Wireless Configuration Radio screen. (See “Configuring Radio Settings” on page 51.)

Field(Continued)	Description(Continued)
Type	Indicates the type of device: • **AP** indicates the neighboring device is a AP/Bridge or access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. • **Ad hoc** indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP/Bridge. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as *peer-to-peer* mode or an *Independent Basic Service Set* (IBSS).
SSID	The *Service Set Identifier* (SSID) for the AP/Bridge. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. The default SSID is set on the Basic Settings page. See “Configuring Basic Settings” on page 38. New SSIDS are created on the INTERFACE MANAGEMENT> SSID Configuration settings. See “Creating and Managing Multiple Networks (SSIDs)” on page 85.
Privacy	This indicates if the "privacy" bit is set in the beacon. If it is, then some type of security is being used and "on" is displayed. If no security is used, the privacy bit is not set and "off" is displayed.
WPA	Indicates whether WPA security is "on" or "off" for this AP/Bridge.
Band	This indicates the frequency band (in GHz) that this radio is using. 802.11b and 802.11g use the 2.4 GHz band, while 802.11a uses the 5 GHz band.
Channel	Shows the channel on which the AP/Bridge is currently broadcasting. The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set in INTERFACE MANAGEMENT > Wireless Configuration (Radio) screen. (See “Configuring Radio Settings” on page 51.)
Rate	Shows the rate (in megabits per second) at which this AP/Bridge is currently transmitting. The current rate will always be one of the rates shown in Supported Rates.
Signal	Indicates the strength of the radio signal emitting from this AP/Bridge as measured in dBm units.
# of Beacons	Shows the total number of beacons transmitted by this AP/Bridge since it was last booted.
Last Beacon	Shows the date and time of the most recent beacon was transmitted from the AP/Bridge.

Field(Continued)	Description(Continued)
Rates	Shows supported and basic (advertised) rate sets for the neighboring AP/ Bridge. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the INTERFACE MANAGEMENT > Wireless Configuration (Radio) screen. (See “Configuring Radio Settings” on page 51.) The rates shown for a AP/Bridge will always be the rates currently specified for that VA4200 in its Radio Settings.

Creating and Managing Multiple Networks (SSIDs)

Each time an SSID is created, the AP/Bridge creates a new bridge that connects all of the selected interfaces. The AP/Bridge comes with a default bridge (SSID) that cannot be deleted, which is referred to as the "Primary Wireless Network" on the **Basic Settings** page. The IP address on that bridge is used to access the VivatoVision web interfaces. Additional SSIDs are created and edited on the **SSID Configuration** VivatoVision page.

Radio interfaces can be shared by all bridges (SSIDs). However, an Ethernet port can only belong to one bridge unless each SSID using that port is assigned to a different VLAN in order to differentiate the network traffic from each SSID.Therefore, because the AP/Bridge has one Ethernet port, *only one SSID can be created that does not use VLAN tagging*.

Using SSIDs with VLANs to Create Logically Separate Networks

VLANs provide a way to separate traffic from two or more SSIDs that share the same Ethernet port. Each SSID is assigned a unique VLAN ID that a router or a switch configured for VLAN operation uses to classify that traffic into a specific network.

In the following figure, two SSIDs were created that are assigned to VLANs. One SSID is called "Guest", and is assigned to VLAN 2. The second SSID is called "Private", and is assigned to VLAN 3. Both SSIDs are configured to use both radio interfaces and the same Ethernet port (Eth0). The network administrator configures the router or switch to direct all packets tagged with VLAN 2 to an unsecured portal, whereas packets tagged for VLAN 3 are forwarded to secure network servers..

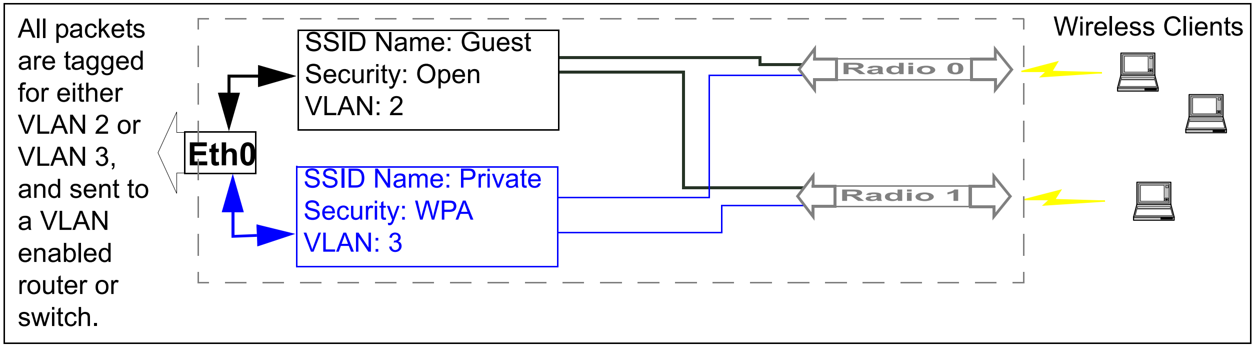
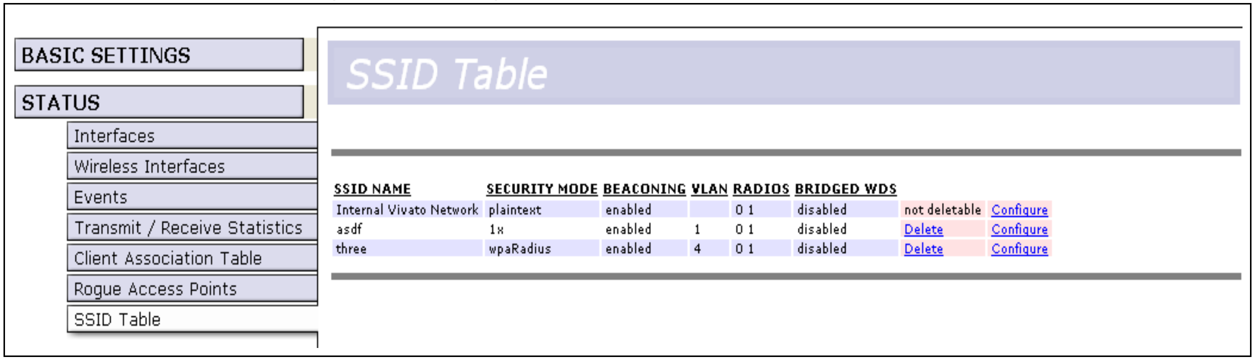


Figure 5 Creating Two Separate Networks Using VLANs

Navigating to Current SSID Settings

To view the status of existing SSIDs, navigate to the **STATUS > SSID Table** tab.



SSID Table

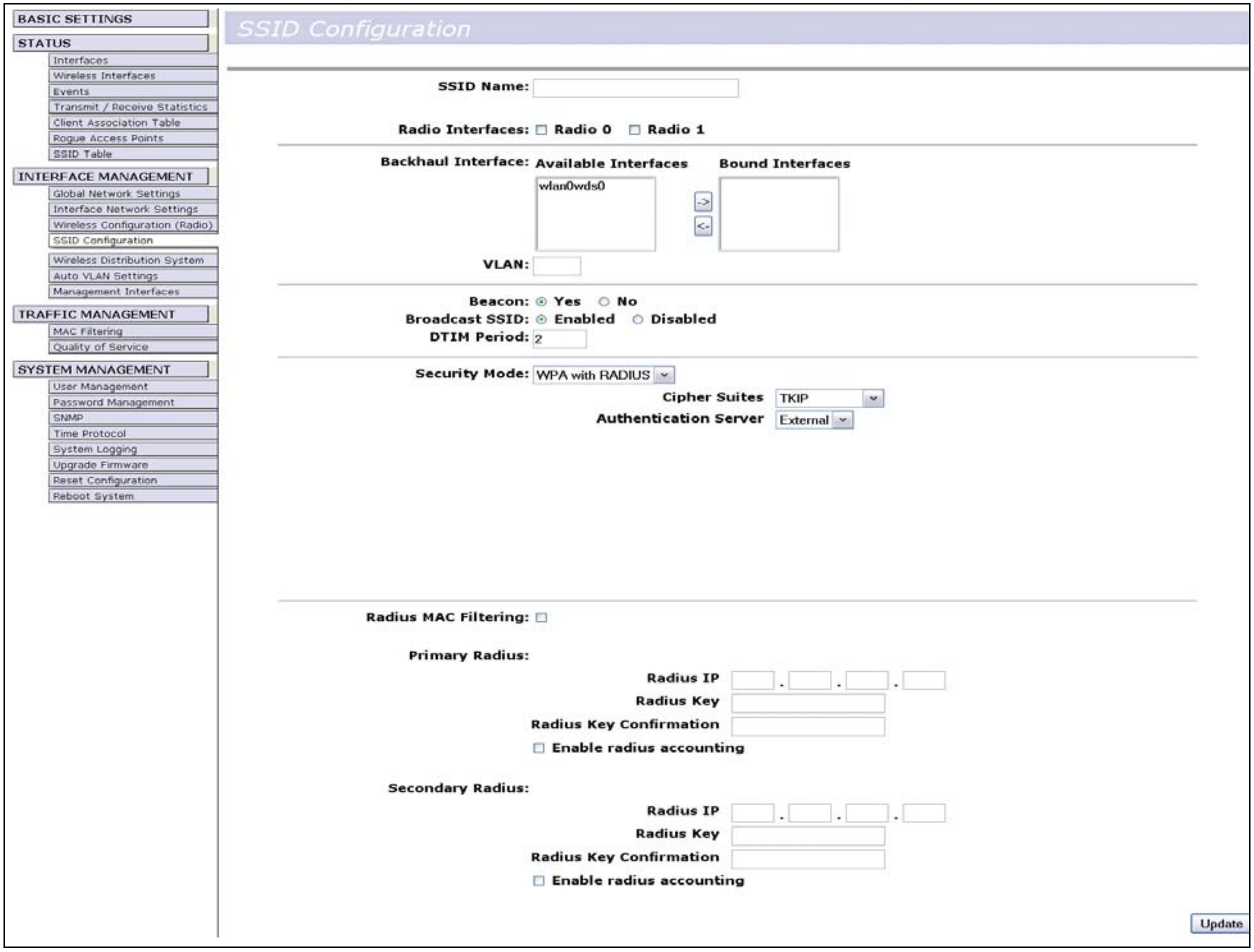
SSID NAME	SECURITY MODE	BEACONING	VLAN	RADIOS	BRIDGED WDS		
Internal Vivato Network	plaintext	enabled		0 1	disabled	not deletable	Configure
asdf	1x	enabled	1	0 1	disabled	Delete	Configure
three	wpaRadius	enabled	4	0 1	disabled	Delete	Configure

Field*	Description
SSID NAME	The name assigned to this network. The first entry is always the name entered for the "Primary Wireless Network Name (SSID)" entered on the BASIC SETTINGS screen during initial configuration. This is the default wireless network and cannot be deleted. Additional SSIDs listed are those created on the SSID Configuration screen.
SECURITY MODE	Lists the type of security being used by this network.
BEACONING	Shows if beacons are enabled or disabled on this network.
VLAN	Lists the VLAN ID for that network if it was assigned.
RADIOS	Lists which radios are being used by this network.
BRIDGED WDS	Shows if this network is being used with a wireless distribution system (WDS) link to another AP/Bridge or to an AP/Bridge.
Delete	Deletes this network. (The primary network cannot be deleted.)
Configure	Navigates to the SSID Configuration screen with the current settings for the selected network in order to change the configuration.

*See Table 2 “SSID Configuration Settings” on page 87 for descriptions of each SSID feature.

Creating and Editing SSIDs

To create or edit SSIDs, navigate to the **INTERFACE MANAGEMENT > SSID Configuration** tab.



SSID Name:

Radio Interfaces: □ Radio 0 □ Radio 1

Backhaul Interface: Available Interfaces: wlan0wds0 Bound Interfaces:

VLAN:

Beacon: ● Yes ○ No
Broadcast SSID: ● Enabled ○ Disabled
DTIM Period: 2

Security Mode: WPA with RADIUS
Cipher Suites: TKIP
Authentication Server: External

Radius MAC Filtering: □

Primary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

Secondary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

Table 2 SSID Configuration Settings

Field	Description
SSID Name	Enter a name of up to 32 characters in length to identify this network.
Radio Interfaces	Select which radios to use in this network.
Ethernet Interface	Select which Ethernet interface(s) (if any) to use with this network. If an Ethernet interface is not selected, traffic through this network is limited to communication between wireless clients and for WDS links.
VLAN	Enter the VLAN ID number for this network (if VLANs are being used). This is a numeric value in the range of 1 to 4094.

Field(Continued)	Description(Continued)
Beacon	Select whether or not to send beacons for this network. Beacons identify this network to other devices with several types of information, such as the BSSID (MAC address) of the wireless radio sending the beacon and the SSID name (Broadcast SSID) that clients see in there list of available wireless networks. • If "Yes" is selected, the beacon is sent on a regular basis so clients can detect it and request an association with that network. The SSID name may or may not be "advertised" in the client's available networks list, depending on the Broadcast SSID setting. If this network is listed first in the client's list of preferred networks, the client will automatically attempt to associate with this network when it sees this beacon. • If "No" is selected, the beacon for this network is not sent. In this case, clients must initiate the association to the network by sending a probe request that contains the SSID to which it is trying to connect. Some clients may not have this capability, and therefore will not operate in a network where beacons are not being sent.
Broadcast SSID	If beacons are enabled, you can select whether or not to sent the SSID's name in the beacon to "advertise" itself to wireless clients. • If "Yes" is selected, clients will see the SSID name in their list of available wireless networks. • If "No" is selected, clients will not see the SSID name in their list of available wireless networks. In this case, the SSID name must be manually entered into the client's configuration before it can access the network.
DTIM Period	The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the AP/Bridge awaiting pick-up. The DTIM you specify here indicates how often the clients served by this AP/Bridge should check for buffered data still on the VA4200 awaiting pickup. Specify a DTIM in the range of 1 - 255. The measurement is in beacons. For example, if you set this to "1" clients will check for buffered data on the VA4200 at every beacon. If you set this to "2", clients will check on every other beacon. If you set this to 10, clients will check on every 10th beacon.
Security Mode	Select the type of wireless security to use with this network. See "Configuring Security Settings" on page 97 for a description of each security mode, including the configuration of an external RADIUS authentication and accounting server.

Updating Settings

To apply your changes, click **Update**.

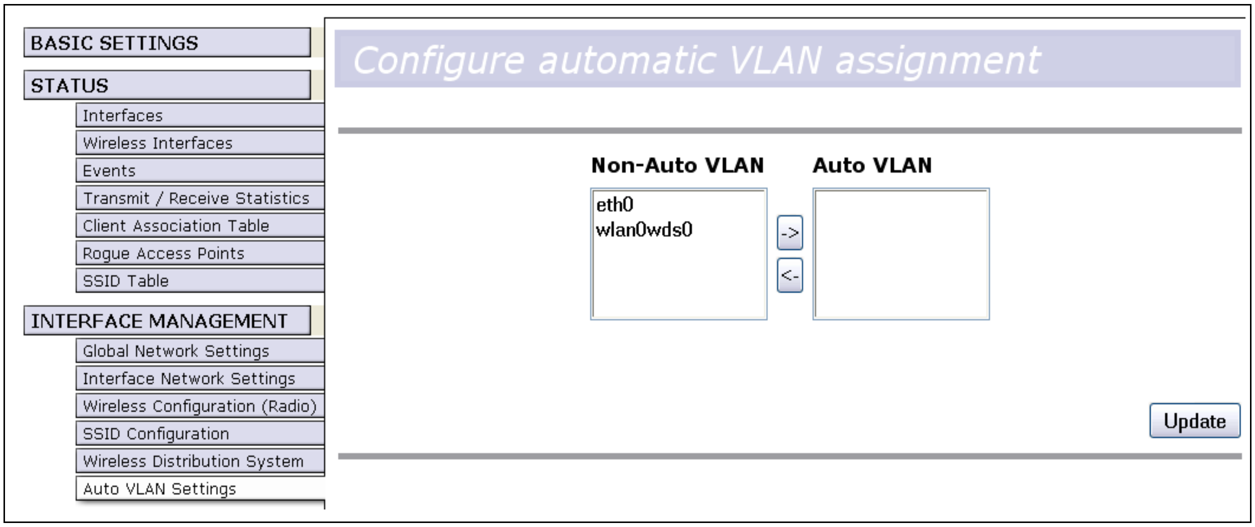
Automatic VLAN Assignment

When a new SSID interface is created, it is assigned a VLAN ID number. This number is used to create an IEEE 802.1Q tag that is appended to packets sent out of the Ethernet or WDS interface used by that SSID for a backhaul connection. VLANs can also be created dynamically on the AP/Bridge when an external RADIUS server is used for client authentication (using 802.1x or WPA security).

The network switch or router providing the backhaul connection must be configured to use 802.1Q tags in order to route the packets to the appropriate device on the local network.

If the MAC address of the client has been entered into the RADIUS server as being part of an existing VLAN on a network, a VLAN with the same ID number can be automatically created on the AP/Bridge. This is done by enabling the Auto VLAN feature on the backhaul interface (Ethernet or WDS) of the AP/Bridge. If the client successfully authenticates, the RADIUS server provides the VLAN assignment for that client to the base station, which in turn creates a VLAN of the same ID for the client to use while associating with the AP/Bridge. After the VLAN is dynamically created, all packets from that client are passed through that VLAN, along with the appropriate 802.1Q tag when sent from the selected interface.

To view and set the Auto VLAN feature, navigate to **INTERFACE MANAGEMENT** > **Auto VLAN Settings**.



To enable Auto VLAN operation on an interface, click on the interface entry to highlight it, then click the **->** arrow to move the entry into the "**Auto VLAN**" box. Select **Update**.

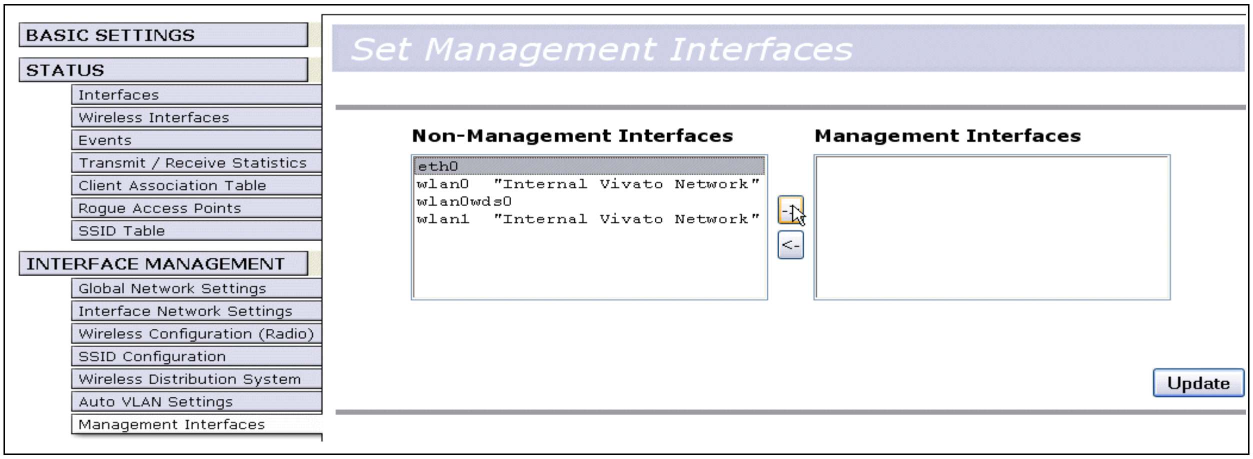
To disable Auto VLAN operation on an interface, click on the interface entry to highlight it, then click the **<-** arrow to move the entry into the "**Non-Auto VLAN**" box. Select **Update**.

Specifying the Management Interface(s)

Access to the VivatoVision configuration web pages can be restricted to one or more interfaces. This is typically done to prevent unauthorized access to the VA4200's configuration.

Navigating to the Management Interfaces Settings

To access the Management Interfaces settings, navigate to the **INTERFACE MANAGEMENT > Management Interfaces** tab.



```
eth0
wlan0   "Internal Vivato Network"
wlan0wds0
wlan1   "Internal Vivato Network"
```

To assign one or more interfaces to be used for management, highlight the desired interface(s) under the **Non-Management Interface** heading and select the -> arrow to move them under the **Management Interface** heading.

Updating Settings

To apply your changes, click **Update**.

Configuring Security

Each SSID network that you configure on the AP/Bridge has its own Security Mode associated with it that clients must be configured to use in order to access that network. For information on creating and editing SSIDs, see “Creating and Editing SSIDs” on page 87.

The following sections describe how to configure Security settings:

- Understanding Security Issues on Wireless Networks
  - How Do I Know Which Security Mode to Use?
  - Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms
  - Does Prohibiting the Broadcast SSID Enhance Security?
- Navigating to Security Settings
- Configuring Security Settings
  - Plain-text
  - Static WEP
  - IEEE 802.1x
  - WPA with RADIUS
  - WPA-PSK
- Updating Settings

Understanding Security Issues on Wireless Networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet NIC transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals over the air, allowing a wireless LAN’s signal to be received without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can attempt to compromise your wireless network. Using a higher gain antenna on the client, a hacker may be able to connect to the network from many miles away.

The Vivato Wi-Fi AP/Bridge provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described in the sections below.

For a more detailed explanation of security concepts, including a comparison of the advantages and disadvantages of using different security modes and suggestions on which mode to use; see Understanding Security Issues on Wireless Networks in the Users Guide.

See also the related topic, Appendix A:“Configuring Security Settings on Wireless Clients” in the User Guide.

See also the related topic, “Appendix A. Configuring Security Settings on Wireless Clients” on page 120.

How Do I Know Which Security Mode to Use?

It is recommended you use the most robust security mode that is feasible in your environment. When configuring security on the AP/Bridge, you first must choose the security mode, then in some modes an authentication algorithm, and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) using the CCMP (AES) encryption algorithm provides the best data protection available and is the best choice if all client stations are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

However, security may not be as much of a priority on some types of networks. If you are simply providing Internet and printer access, as on a guest network, plain text mode (no security) may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID for the Internal network so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations. (See “Does Prohibiting the Broadcast SSID Enhance Security?” on page 97)

Following is a brief discussion of what factors make one mode more secure than another, a description of each mode offered, and when to use each mode.

Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms

Three major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys
- Presence or absence of integrated user authentication in the protocol
- Encryption algorithm or formula the protocol uses to encode/decode the data

Following is a list of the security modes available on the Vivato VA4200, along with a description of the key management, authentication, and encryption algorithms used in each mode. We include some suggestions as to when one mode might be more appropriate than another.

- When to Use Plain Text
- When to Use Static WEP
- When to Use IEEE 802.1x
- When to Use WPA with RADIUS
- When to Use WPA-PSK

When to Use Plain Text

Plain text mode provides no security. The data is not encrypted, rather it is sent as "plain text" across the network. No key management, data encryption or user authentication is used. Any client should be able to access the network.

Recommendations

Plain text mode is **not recommended** for regular use on the Internal network because it is not secure. Therefore, only use plain text mode for a guest network or when performing the initial AP/Bridge setup, or during testing or problem solving.

See Also

For information on how to configure plain text mode, see “Plain-text” on page 98 under “Configuring Security Settings” on page 97.

When to Use Static WEP

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and AP/Bridges on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption

Key Management	Encryption Algorithm	User Authentication
Static WEP uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the Vivato Wi-Fi AP/Bridge). The client stations must have the same key indexed in the same slot to access data on the AP/Bridge.	An RC4 stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	If you set the Authentication Algorithm to Shared Key, this protocol provides a rudimentary form of user authentication. However, if the Authentication Algorithm is set to "Open System", no authentication is performed. If the algorithm is set to "Both", only WEP clients are authenticated.

Recommendations

Static WEP was designed to provide security equivalent of sending unencrypted data through an Ethernet connection, however it has some flaws and it does not provide even this intended level of security.

Therefore, **Static WEP is not recommended** as a secure mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

See Also

For information on how to configure Static WEP security mode, see “Static WEP” on page 98 under “Configuring Security Settings” on page 97.

When to Use IEEE 802.1x

IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP.

Key Management	Encryption Algorithm	User Authentication
IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	An RC4 stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server. You have a choice of using the Vivato Wi-Fi AP/Bridge embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as TKIP and CCMP (AES) used in *Wi-Fi Protected Access* (WPA).

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method.

Therefore, IEEE 802.1x mode is not as secure a solution as *Wi-Fi Protected Access* (WPA). If you cannot use WPA because some of your client stations do not have WPA, then a better solution than using IEEE 802.1x mode is to **use WPA with RADIUS mode instead and check the "Allow non-WPA IEEE 802.1x clients" checkbox** to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

If you have an external RADIUS server on your network, we recommend using it rather than the using the embedded RADIUS server on the VA4200. An external RADIUS server will provide better security than the local authentication server.

For information on how to configure IEEE 802.1x security mode, see “IEEE 802.1x” on page 102 under “Configuring Security Settings” on page 97.

When to Use WPA with RADIUS

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Counter mode/CBC-MAC Protocol* (CCMP), and *Advanced Encryption Standard* (AES) mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA with RADIUS provides the best security available for wireless networks.

Key Management	Encryption Algorithms	User Authentication
WPA with RADIUS provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• *Temporal Key Integrity Protocol* (TKIP) • *Counter mode/CBC-MAC Protocol* (CCMP) *Advanced Encryption Standard* (AES)	*Remote Authentication Dial-In User Service* (RADIUS) You have a choice of using the Vivato Wi-Fi AP/Bridge embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

WPA with RADIUS mode is the **recommended mode**. The CCMP (AES) and TKIP encryption algorithms used with WPA modes are far superior to the RC4 algorithm used for Static WEP or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option.

Additionally, this mode (WPA with RADIUS) incorporates a RADIUS server for user authentication which is more effective than WPA-PSK.

If you have an external RADIUS server on your network, we recommend using it rather than the using the embedded RADIUS server on the AP/Bridge. An external RADIUS server will provide better security than the local authentication server.

Use the following guidelines for choosing options within the WPA with RADIUS security mode:

1. The best security you can have to date on a wireless network is WPA with RADIUS using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other VA4200s on the network are WPA/CCMP compatible, use this encryption algorithm.

2. The second best choice is WPA with RADIUS with the encryption algorithm set to "Both" (that is, both TKIP and CCMP). This lets WPA client stations without CCMP associate, uses TKIP for encrypting Multicast and Broadcast frames, and allows clients to select whether to use CCMP or TKIP for Unicast (VA4200-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Client stations that support CCMP can use it for their Unicast frames. If you encounter VA4200-to-station interoperability problems with the "Both" encryption algorithm setting, then you will need to select TKIP instead. (See next bullet.)

3. The third best choice is WPA with RADIUS with the encryption algorithm set to TKIP. Some clients have interoperability issues with CCMP and TKIP enabled at same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client Wireless software security features. TKIP is the only encryption algorithm that is being tested in Wi-Fi WPA certification.

> **Note**
>
> If there are older client stations on your network that do not support WPA, you can configure WPA with RADIUS (with Both, CCMP, or TKIP) and check the "Allow non-WPA IEEE 802.1x clients" checkbox to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.
>
> A typical scenario is when upgrading a current 802.1x network to use WPA. You might have a mix of clients; some new clients that support WPA and some older ones that do not support WPA. You might even have other AP/Bridges on the network that support only 802.1x and some that support WPA with RADIUS. For as long as this mix persists, use the "Allow non-WPA IEEE 802.1x clients" option
>
> When all the stations have been upgraded to use WPA, you should disable the "Allow non-WPA IEEE 802.1x clients" option.

See Also

For information on how to configure WPA with RADIUS security mode, see “WPA with RADIUS” on page 104 under “Configuring Security Settings” on page 97.

When to Use WPA-PSK

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP) *Advanced Encryption Algorithm* (AES), and *Counter mode/CBC-MAC Protocol* (CCMP) mechanisms. This mode offers the same encryption algorithms as WPA with RADIUS but without the ability to integrate a RADIUS server for user authentication.

Key Management	Encryption Algorithms	User Authentication
WPA-PSK provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• *Temporal Key Integrity Protocol* (TKIP) • *Counter mode/CBC-MAC Protocol* (CCMP) *Advanced Encryption Standard* (AES)	The use of a Pre-Shared (PSK) key provides user authentication similar to that of shared keys in WEP.

Recommendations

WPA w/PSK is not recommended for use with the Vivato VA4200 when WPA with RADIUS is an option.

We recommend that you use WPA with RADIUS mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA with EAP talking to a RADIUS server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, we recommend that you use WPA-PSK.

See Also

For information on how to configure WPA-PSK security mode, see “WPA-PSK” on page 108 under “Configuring Security Settings” on page 97.

Does Prohibiting the Broadcast SSID Enhance Security?

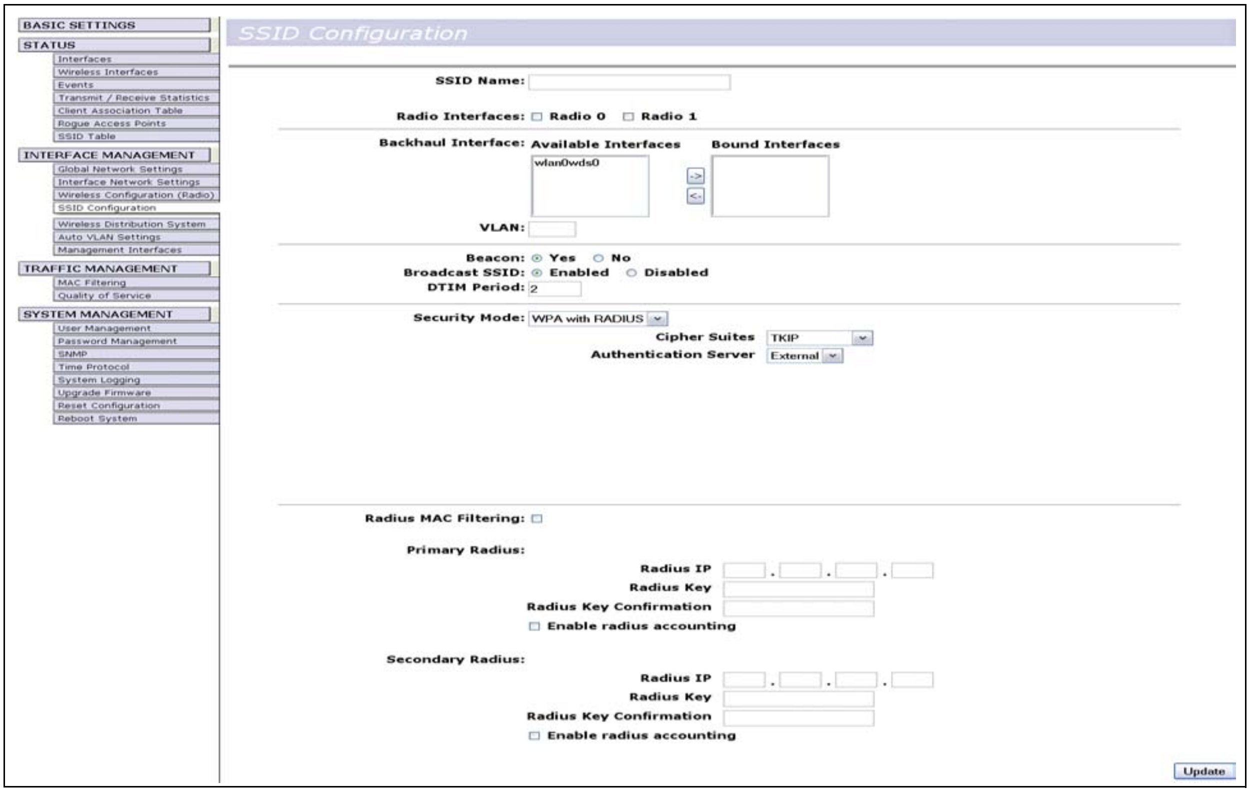
You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your AP/ Bridge (see “Broadcast SSID” on page 88). When the VA4200’s broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.

Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor plain text traffic.

This offers a very minimal level of protection on an otherwise exposed network, where the priority is making it easy for clients to get a connection and where no sensitive information is available.

Navigating to Security Settings

Security is first configured when creating an SSID. To edit the security mode for an existing SSID, navigate to the **STATUS > SSID Table** tab, select "Configure" for that SSID, and modify the existing settings. See “Creating and Managing Multiple Networks (SSIDs)” on page 85 .



SSID Configuration

SSID Name:

Radio Interfaces: □ Radio 0 □ Radio 1

Backhaul Interface: Available Interfaces: wlan0wds0 Bound Interfaces:

VLAN:

Beacon: ● Yes ○ No
Broadcast SSID: ● Enabled ○ Disabled
DTIM Period: 2

Security Mode: WPA with RADIUS
Cipher Suites: TKIP
Authentication Server: External

Radius MAC Filtering: □

Primary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

Secondary Radius:
Radius IP . . .
Radius Key
Radius Key Confirmation
□ Enable radius accounting

Configuring Security Settings

The following configuration information explains how to configure security modes on the AP/Bridge. Keep in mind that each wireless client that wants to exchange data with the AP/Bridge must be configured with the proper security settings as well.

Field	Description
Security Mode	Select the **Security Mode**. Select one of the following: • Plain-text • Static WEP • IEEE 802.1x • WPA with RADIUS • WPA-PSK

Plain-text

Plain Text means any data transferred to and from the Vivato Wi-Fi AP/Bridge is not encrypted.

There are no further options for "Plain-text" mode.

Plain text mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and AP/Bridges on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

You cannot mix 64-bit and 128-bit WEP keys between the AP/Bridge and its client stations.

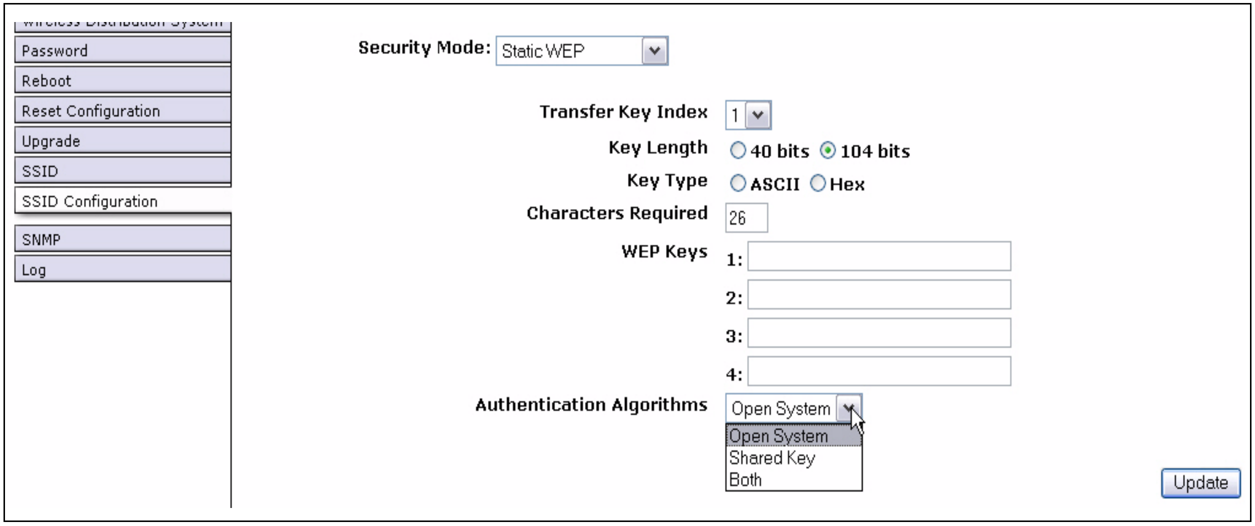
Static WEP is not the most secure mode available, but it offers more protection than plain-text mode as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see the sections on “IEEE 802.1x” on page 102, “WPA with RADIUS” on page 104, or “WPA-PSK” on page 108.)

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a "stream" cipher called RC4.)

The AP/Bridge uses a key to transmit data to the client stations. Each client station must use that same key to decrypt data it receives from the AP/Bridge.

Client stations can use different keys to transmit data to the AP/Bridge. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you selected "Static WEP" Security Mode, provide the following on the AP/Bridge settings:



Security Mode: Static WEP

Transfer Key Index: 1

Key Length: ○ 40 bits ● 104 bits

Key Type: ○ ASCII ○ Hex

Characters Required: 26

WEP Keys 1: 2: 3: 4:

Authentication Algorithms: Open System

.

Field	Description
Transfer Key Index	Select a key index from the drop-down menu. Key indexes 1 through 4 are available. The default is 1. The Transfer Key Index indicates which WEP key the AP/Bridge will use to encrypt the data it transmits.
Key Length	Specify the length of the key by clicking one of the radio buttons: • 64 bits • 128 bits
Key Type	Select the key type by clicking one of the radio buttons: • ASCII • Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for each key. If you selected "ASCII", enter any combination of integers and letters `0-9`, `a-z`, and `A-Z`. If you selected "HEX", enter hexadecimal digits (any combination of `0-9` and `a-f` or `A-F`). Use the same number of characters for each key as specified in the "Characters Required" field. These are the RC4 WEP keys shared with the stations using the AP/Bridge. Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the VA4200. (See “Rules to Remember for Static WEP” on page 100.)

Field(Continued)	Description(Continued)
Authentication Algorithm	The authentication algorithm defines the method used to determine whether a client station is allowed to associate with a AP/Bridge when static WEP is the security mode. Specify the authentication algorithm you want to use by choosing one of the following from the drop-down menu: • Open System • Shared Key • Both **Open System** authentication allows any client station to associate with the AP/Bridge whether that client station has the correct WEP key or not. This algorithm is also used in plaintext, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to "Open System", any client can associate with the AP/Bridge. Note that just because a client station is allowed to *associate* does not ensure it can exchange traffic with a AP/Bridge. A station must have the correct WEP key to be able to successfully access and decrypt data from a AP/Bridge, and to transmit readable data to the AP/Bridge. **Shared Key** authentication requires the client station to have the correct WEP key in order to associate with the AP/Bridge. When the authentication algorithm is set to "Shared Key", a station with an incorrect WEP key will not be able to associate with the AP/Bridge. **Both** is the default. When the authentication algorithm is set to "Both": • Client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the AP/Bridge. • Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the AP/Bridge even if they do not have the correct WEP key.

Rules to Remember for Static WEP

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the VA4200 in order to de-code VA4200-to-station data transmissions.

- The VA4200 must have all keys used by clients for station-to-VA4200 transmit so that it can de-code the station transmissions.

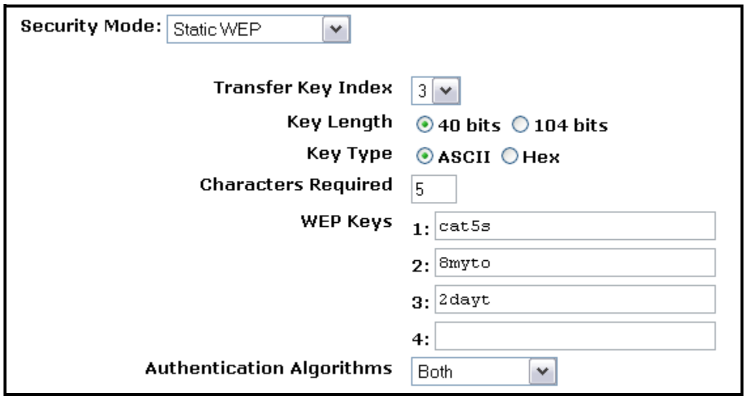
- The same key must occupy the same slot on all nodes (VA4200 and clients). For example if the VA4200 defines `abc123` key as WEP key 3, then the client stations must define that same string as WEP key 3.

- On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client station "transfer key index", and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring VA4200s cannot decode each other’s transmissions.

Example of Using Static WEP

For a simple example, suppose you configure three WEP keys on the AP/Bridge. In our example, the Transfer Key Index for the VA4200 is set to"3". This means that the WEP key in slot "3" is the key the AP/Bridge will use to encrypt the data it sends.

Figure 6 Setting the **Transfer Key** on the AP/Bridge



Security Mode: Static WEP

Transfer Key Index: 3

Key Length: ● 40 bits ○ 104 bits

Key Type: ● ASCII ○ Hex

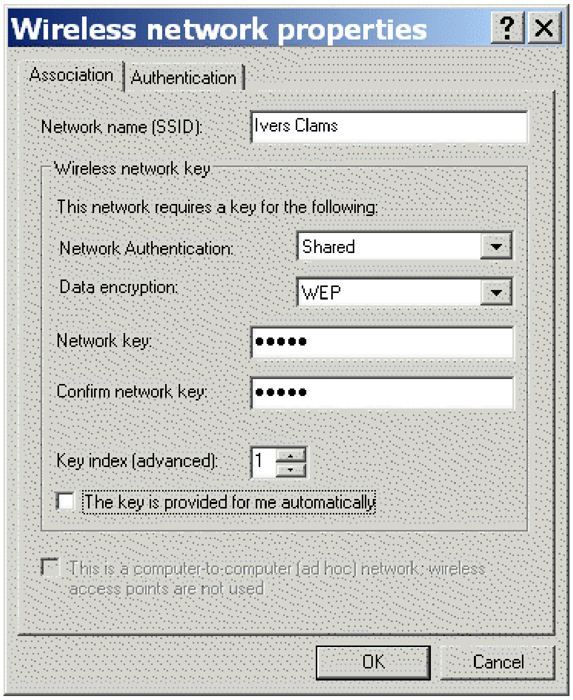
Characters Required: 5

WEP Keys
1: cat5s
2: 8myto
3: 2dayt
4:

Authentication Algorithms: Both

You must then set all client stations to use WEP and provide each client with one of the slot/key combinations you defined on the VA4200. For this example, we'll set WEP key 1 on a Windows client.

Figure 7 Providing a Wireless Client with a WEP Key



Network name (SSID): Ivers Clams

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key: •••••

Confirm network key: •••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

If you have a second client station, that station also needs to have one of the WEP keys defined on the VA4200. You could give it the same WEP key you gave to the first station. Or for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

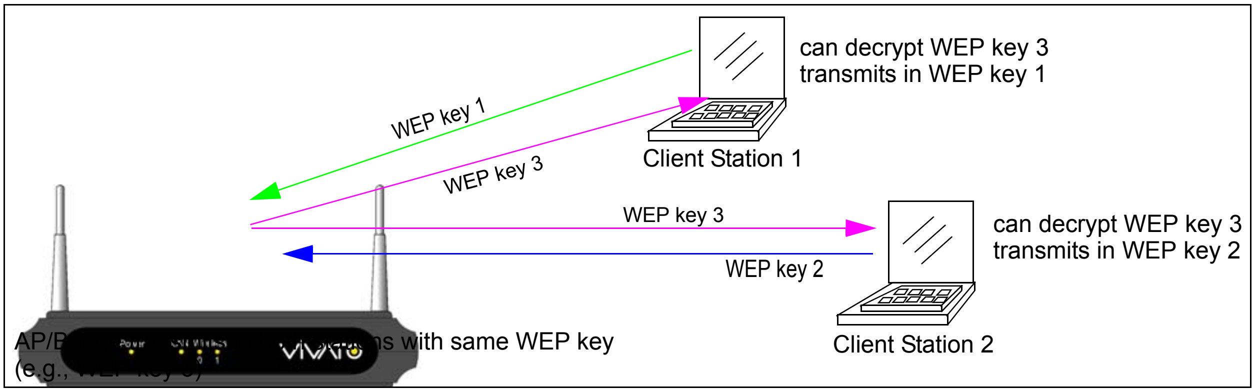
Static WEP with Transfer Key Indexes on Client Stations

Some Wireless client software (like Funk Odyssey) lets you configure multiple WEP keys and set a transfer index on the client station, then you can specify different keys to be used for station-to-VA4200 transmissions. (The standard Windows wireless client software does not allow you to do this.)

To build on our example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the VA4200 transmissions with that key and also give client 1 WEP key 1 and set this as its transfer key. You could then give client 2 WEP key 2 and set this as its transfer key index.

The following figure illustrates the dynamics of the VA4200 and two client stations using multiple WEP keys and a transfer key index.

Figure 8 Example of Using Multiple WEP Keys and Transfer Key Index on Client Stations



IEEE 802.1x

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

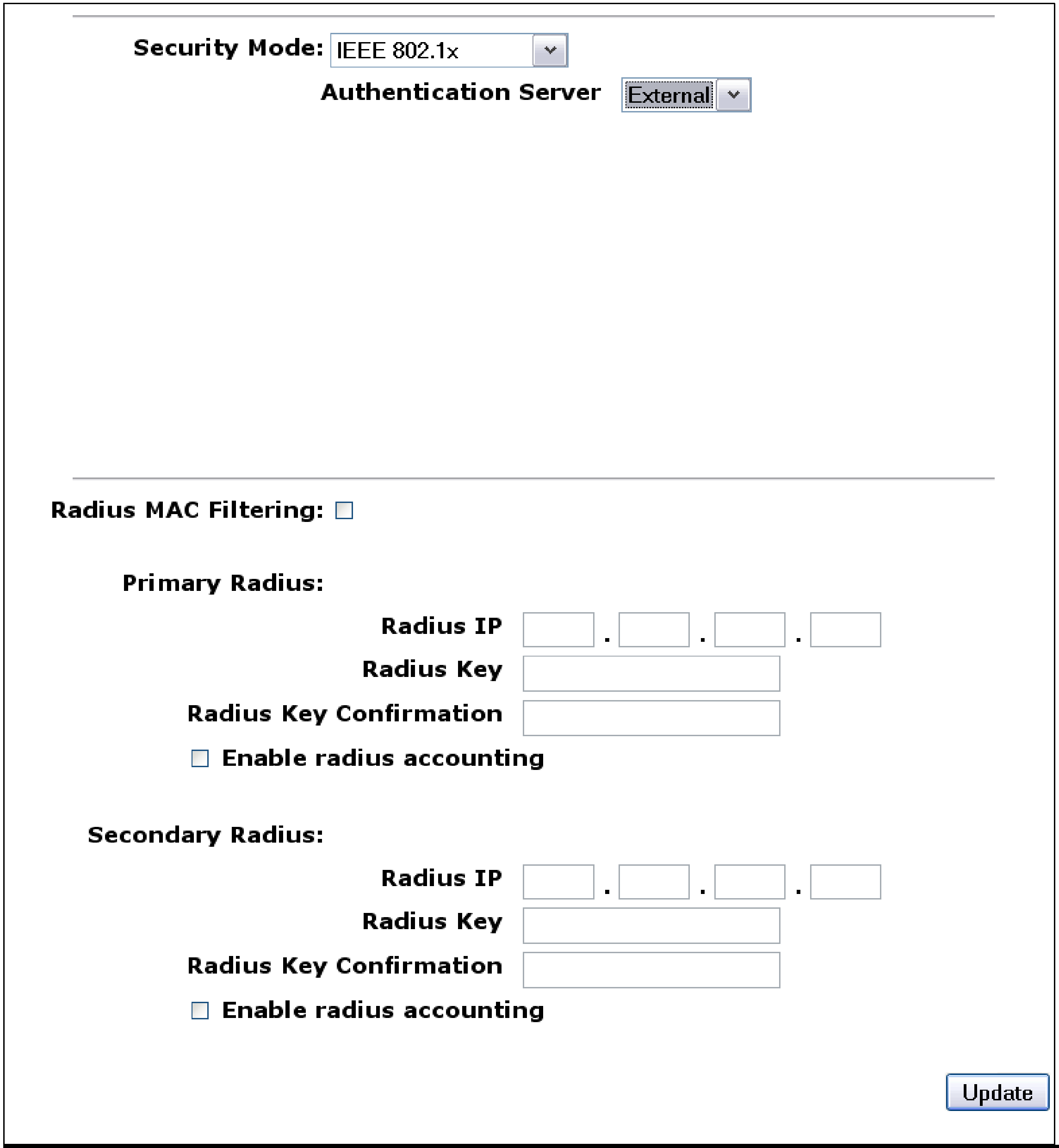
This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the Network > User Management tab.

The AP/Bridge requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the Vivato Wi-Fi AP/Bridge internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

When configuring IEEE 802.1x mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The Vivato Wi-Fi AP/Bridge embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you have the option of using any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the client stations must be configured to use the same authentication method being used by the AP/Bridge.

If you selected "IEEE 802.1x" Security Mode, provide the following:



Security Mode: IEEE 802.1x

Authentication Server External

Radius MAC Filtering: □

Primary Radius:

Radius IP . . .

Radius Key

Radius Key Confirmation

□ Enable radius accounting

Secondary Radius:

Radius IP . . .

Radius Key

Radius Key Confirmation

□ Enable radius accounting

Field	Description
Authentication Server	Select one of the following from the drop-down menu: • **Built-in** - To use the authentication server provided with the Vivato Wi-Fi AP/ Bridge. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • **External** - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server(s) that you want to use. **Note:** The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the Vivato Wi-Fi AP/ Bridge, the RADIUS server User Datagram Protocol (UDP) ports used by the AP/ Bridge are not configurable. (The Vivato Wi-Fi AP/Bridge is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.

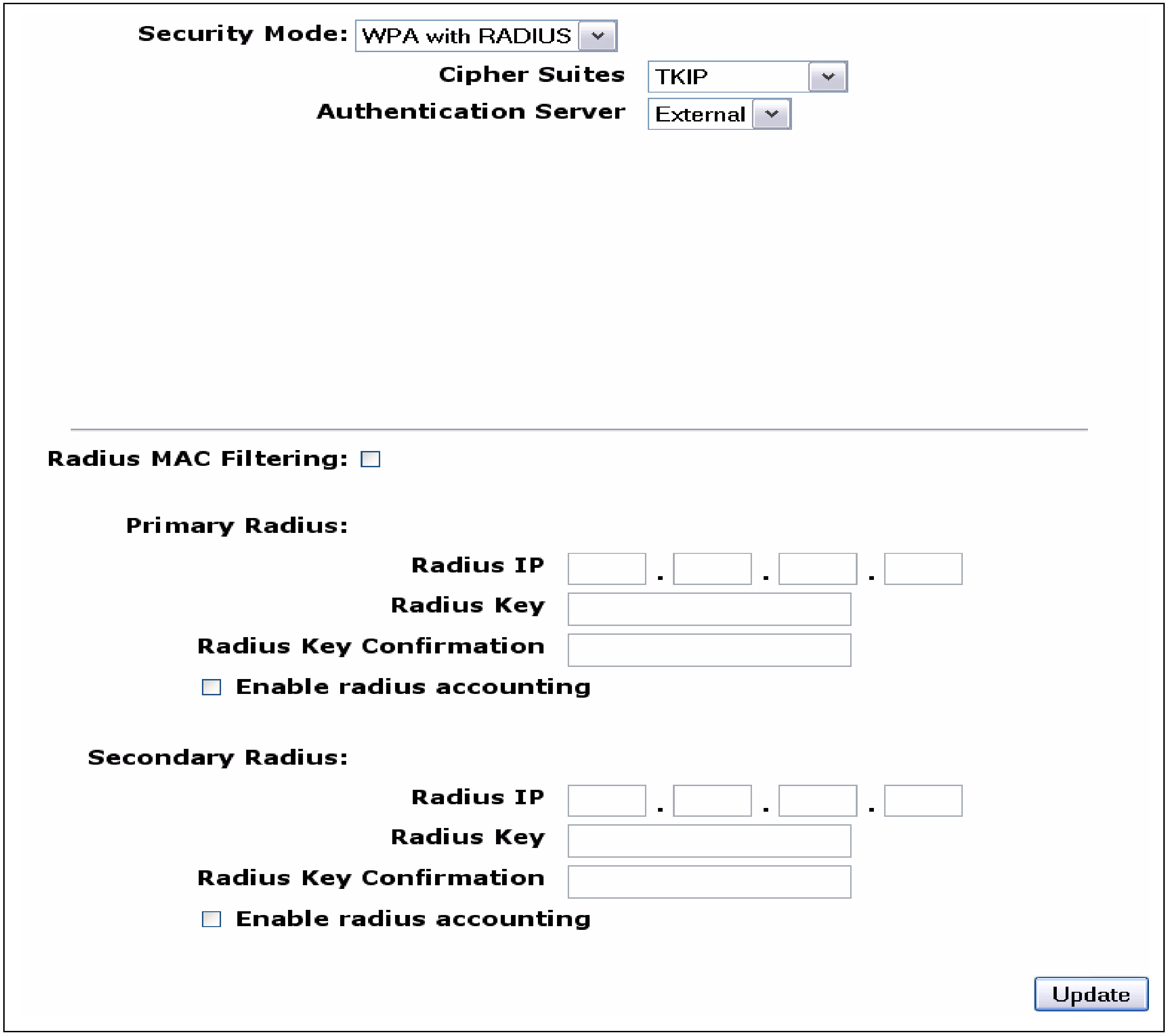
Field(Continued)	Description(Continued)
Radius MAC Filtering	When unchecked, client (station) authentication requests are passed directly to the specified RADIUS server(s). Checking this box causes the VA4200 to first use the MAC Filtering settings on the VA4200 to filter clients that are specifically allowed or denied authentication. See “Navigating to MAC Filtering Settings” on page 57. If a client’s MAC address is in the active Stations List of allowed or denied clients, they are authenticated or denied authentication at that point; their authentication request is not forwarded to the RADIUS server(s). If a client’s MAC address has not been entered into the active Station List, the client’s authentication request is passed to the specified RADIUS server(s). The RADIUS server must be configured with an account that uses the MAC address for both a username and a password, and formatted as a string of 12 hex digits without separating colons, such as 002c31e4161f. MAC authentication uses PAP instead of PEAP for the Authentication-type, so the Authenticator must be configured accordingly. On Windows IAS, PAP is disabled by default
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the RADIUS server. (The Vivato Wi-Fi AP/Bridge internal authentication server is `127.0.0.1`.) For information on setting up user accounts, see “Managing User Accounts” on page 45.
Radius Key	Enter the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. (The Vivato Wi-Fi AP/Bridge internal authentication server key is `secret`.) This value is never sent over the network.
Radius Key Confirmation	Re-enter the same Radius Key.
Enable RADIUS Accounting	Click "Enable RADIUS Accounting" to send client information to the RADIUS accounting server, including the client login time, logout time, and the duration that the client was logged in. By default, accounting information is sent to port 1813 on the RADIUS server.

WPA with RADIUS

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Counter mode/ CBC-MAC Protocol* (CCMP), and *Advanced Encryption Standard* (AES) mechanisms. This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the Network > User Management tab.

When configuring WPA with RADIUS mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The Vivato Wi-Fi AP/Bridge embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you selected "WPA with RADIUS" **Security Mode**, provide the following:



Security Mode: WPA with RADIUS

Cipher Suites TKIP

Authentication Server External

Radius MAC Filtering: □

Primary Radius:

Radius IP . . .

Radius Key

Radius Key Confirmation

□ Enable radius accounting

Secondary Radius:

Radius IP . . .

Radius Key

Radius Key Confirmation

□ Enable radius accounting

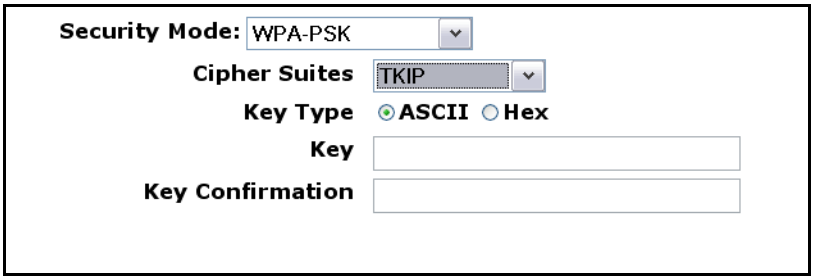
Field	Description
Cipher Suites	Select the cipher you want to use from the drop-down menu: • TKIP • CCMP (AES) • Both **Temporal Key Integrity Protocol** (TKIP) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit "temporal key" shared by clients and AP/Bridges. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (CCMP) is an encryption method for IEEE 802.11 that uses the **Advanced Encryption Algorithm** (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the AP/Bridge. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the VA4200: • A valid TKIP RADIUS IP address and valid shared Key • A valid CCMP (AES) IP address and valid shared Key Clients not configured to use WPA with RADIUS will not be able to associate with VA4200. **Both** is the default. When the authentication algorithm is set to "Both", client stations configured to use WPA with RADIUS must have one of the following: • A valid TKIP RADIUS IP address and RADIUS Key • A valid CCMP (AES) IP address and RADIUS Key
Authentication Server	Select one of the following from the drop-down menu: • **Built-in** - To use the authentication server provided with the Vivato Wi-Fi AP/Bridge. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • **External** - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use. **Note:** The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the Vivato Wi-Fi AP/Bridge, the RADIUS server User Datagram Protocol (UDP) ports used by the AP/Bridge are not configurable. (The Vivato Wi-Fi AP/Bridge is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.

Field(Continued)	Description(Continued)
Radius MAC Filtering	When unchecked, client (station) authentication requests are passed directly to the specified RADIUS server(s). Checking this box causes the VA4200 to first use the MAC Filtering settings on the VA4200 to filter clients that are specifically allowed or denied authentication. See “Navigating to MAC Filtering Settings” on page 57. If a client’s MAC address is in the active Stations List of allowed or denied clients, they are authenticated or denied authentication at that point; their authentication request is not forwarded to the RADIUS server(s). If a client’s MAC address has not been entered into the active Station List, the client’s authentication request is past to the specified RADIUS server(s). The RADIUS server must be configured with an account that uses the MAC address for both a username and a password, and formatted as a string of 12 hex digits without separating colons, such as 002c31e4161f. MAC authentication uses PAP instead of PEAP for the Authentication-type, so the Authenticator must be configured accordingly. On Windows IAS, PAP is disabled by default.
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the RADIUS server. (The Vivato Wi-Fi AP/Bridge internal authentication server is `127.0.0.1`.) For information on setting up user accounts, see “Managing User Accounts” on page 45.
Radius Key	Enter the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. (The Vivato Wi-Fi AP/Bridge internal authentication server key is `secret`.) This value is never sent over the network.
Radius Key Confirmation	Re-enter the same Radius Key.
Enable RADIUS Accounting	Click "Enable RADIUS Accounting" to send client information to the RADIUS accounting server, including the client login time, logout time, and the duration that the client was logged in. By default, accounting information is sent to port 1813 on the RADIUS server.

WPA-PSK

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Algorithm* (AES), and *Counter mode/CBC-MAC Protocol* (CCMP) mechanisms. PSK employs a pre-shared key. This is used for an initial check of credentials only.

If you selected "WPA-PSK" **Security Mode**, provide the following:



Security Mode:	WPA-PSK
Cipher Suites	TKIP
Key Type	● ASCII ○ Hex
Key	
Key Confirmation	

Field	Description
Cipher Suites	Select the cipher you want to use from the drop-down menu: • TKIP • CCMP (AES) • Both **Temporal Key Integrity Protocol** (TKIP) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit "temporal key" shared by clients and AP/Bridges. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (CCMP) is an encryption method for IEEE 802.11i that uses the **Advanced Encryption Algorithm** (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. When the authentication algorithm is set to "**Both**", both TKIP and AES clients can associate with the AP/Bridge. WPA clients must have one of the following to be able to associate with the VA4200: • A valid TKIP key • A valid CCMP (AES) key Clients not configured to use WPA-PSK will not be able to associate with VA4200.
Key Type	Select the character format for the pre-shared key: ASCII or Hex. • **ASCII** - Enter any combination of 8 to 63 characters. • **Hex** - Enter 64 hexidecimal characters (a-f, 0-9).

Field	Description
Key	The *Pre-shared Key* is the shared secret key for WPA-PSK. Enter the proper number and type of characters for the selected **Key Type**.
Key Confirmation	Re-enter the same pre-shared key.

Updating Settings

To apply your changes, click **Update**.

Simple Network Management Protocol (SNMP)

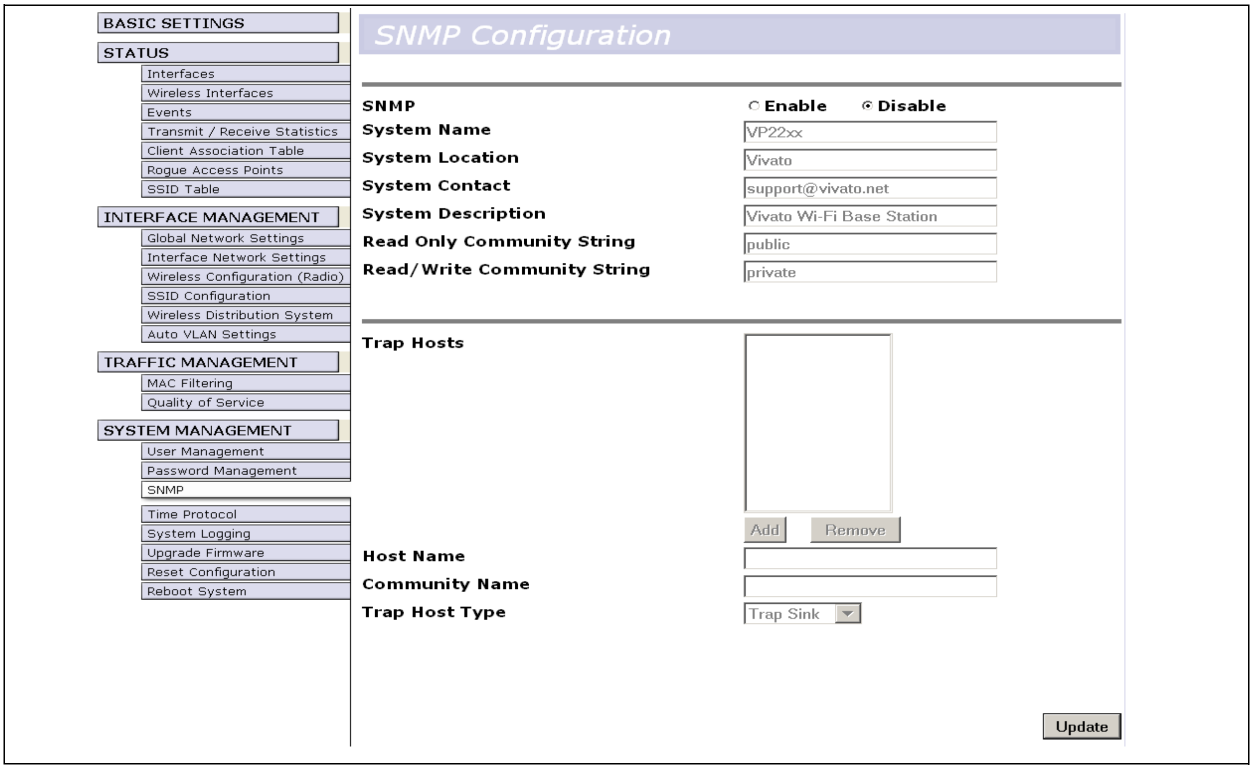
Simple Network Management Protocol (SNMP) is a network management and monitoring system that can be used to change[2] and monitor settings within the AP/Bridge. The AP/Bridge contains program routines called "agents" that monitor the state of settings and network conditions and send that information to management information bases (MIBs). Many available network management software packages are available that can use the MIBs to manage the AP/Bridge in your network.

Several standard MIBs are supported that are used to monitor 802.11 networks:

- BRIDGE-MIB.txt
- IEEE802dot11-MIB.txt
- IF-MIB.txt
- IP-FORWARD-MIB.txt
- IP-MIB.txt
- SNMPv2-MIB.txt
- TCP-MIB.txt
- UDP-MIB.txt
- VIVATO-BASE-STATION-MIB.txt
- VIVATO-CLIENT-MIB.txt
- VIVATO-CLIENT-PERF-MIB.txt
- VIVATO-MIB.txt
- VIVATO-SSID-MIB.txt
- VIVATO-TC-MIB.txt
- VIVATO-VA4200-AGT-CAP-MIB.txt
- VIVATO-VA4210-AGT-CAP-MIB.txt

Navigating to SNMP Settings

To access the SNMP settings, navigate to the **SYSTEM MANAGEMENT > SNMP** tab.



SNMP Configuration

SNMP	○ Enable ● Disable
System Name	VP22xx
System Location	Vivato
System Contact	support@vivato.net
System Description	Vivato Wi-Fi Base Station
Read Only Community String	public
Read/Write Community String	private
Trap Hosts	
Host Name	
Community Name	
Trap Host Type	Trap Sink

[2] The VA4200 does not currently support SNMP write (set) operations; only read (get) operations are supported.

Field	Description
SNMP	Enable or Disable SNMP operation.
System Name	What you call this AP/Bridge in your network.
System Location	Enter the physical location of this AP/Bridge. This may be used to distinguish it from another AP/Bridge located in the same area.
System Contact	Enter the name of the person who is responsible for maintaining the configuration of the AP/Bridge.
System Description	Enter a description of the system that this AP/Bridge is part of.
Read Only Community String	Enter the read only community string.
Read/Write Community String	Enter the read/write community string.
Trap Hosts	Lists the traps that have been created. After entering the **Community Name** and **Trap Host Type**, select **Add** to add it. To remove an existing trap, select the trap and click on **Remove**.
Host Name	Enter the IP address or host name of the device where the trap report is to be sent. Using a host name requires a DNS nameserver on the network.
Community Name	Enter the community name (password) for the host where the trap report is being sent.
Trap Host Type	Select whether to create a Trap Sink, Trap2 Sink, or an Inform Sink.

Updating Settings

To apply your changes, click **Update**.

Enabling Logging

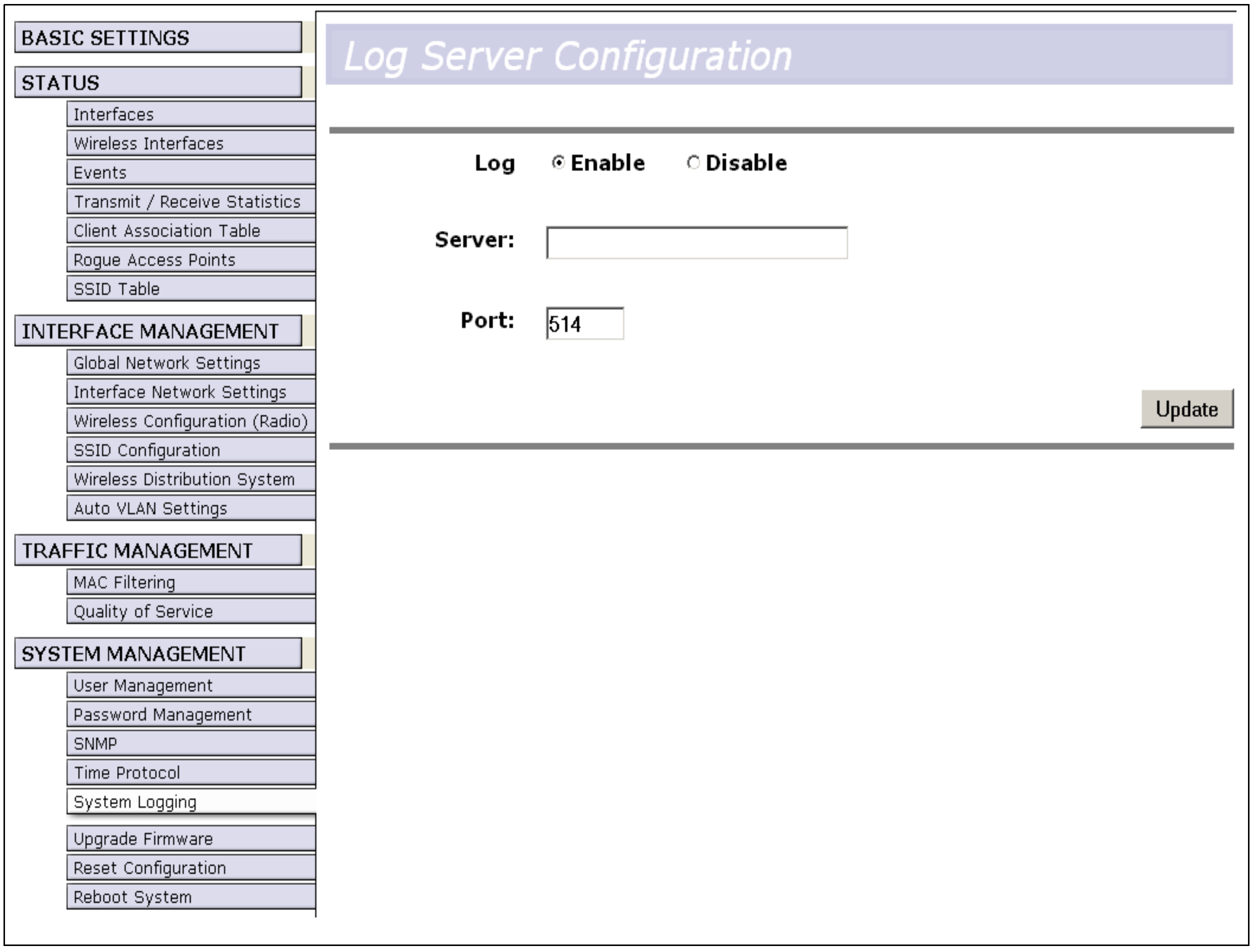
System messages can be displayed on the VivatoVision **Events** page, and can also be sent to a remote system logging (syslog) server to maintain a record of system conditions.

The following sections describe how to configure event logging:

- Navigating to Log Server Configuration Settings
- Updating Settings

Navigating to Log Server Configuration Settings

To access the Log Server Configuration settings, navigate to the **SYSTEM MANAGEMENT > System Logging** tab.



Log Server Configuration

Log ● Enable ○ Disable

Server:

Port: 514

Field	Description
Log	Select **`Enable`** or **`Disable`** to turn logging on or off, respectively. This control effects logging to both the **`Events`** VivatoVision web page and to a remote syslog server (if configured).
Server	Enter the IP address of the remote syslog server. A host name can be entered if a DNS nameserver is on the network with an entry for that host.
Port	Enter the UDP port number for syslog operation on the remote host. The default is 514, and is typically used by syslog servers.

Updating Settings

To apply your changes, click **Update**.

System Recovery and File System Commands

The VA4200 uses the Linux operating system, consisting of a bootloader routine (called "Redboot") and a Linux kernel ("shell"). After the bootloader loads and runs the kernel, the configuration of the AP/Bridge is loaded from a file called "apconfig.xml". The configuration file contains all of the settings made by the user. If the configuration file is deleted, the AP/Bridge returns to using its factory default settings.

The Linux operating system can be accessed directly by using a terminal emulator and a null modem serial connection.

If the administrator password is unknown, the only way to regain control of the AP/Bridge is by connecting a PC to the AP/Bridge's serial port, interrupting the bootloader, and issuing the default password recovery command. This causes the AP/Bridge to be rebooted using the default password: vivato. If you know the AP/Bridge's IP address, you can then use the default password to access the VivatoVision web interface to create and save a new password.

If IP access to the AP/Bridge is lost, the configuration can be restored to the factory defaults to regain access, or commands can be issued to view the currently assigned IP address and specify a new address.

Restoring the Default Administrator Password

A null modem connection and terminal emulator program (such as HyperTerminal™ or Tera Term Pro™) are used to access the Linux "Redboot" bootloader and shell.

1. Connect a null modem serial cable between the VA4200's DB-9(m) port and the your PC's COM port.

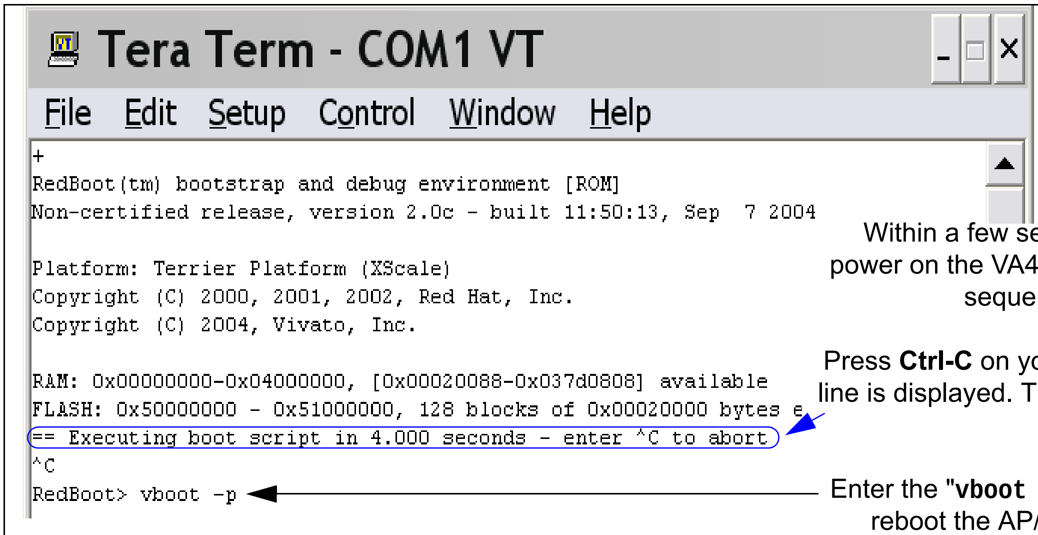
2. Configure a terminal emulator on your PC with the following communication settings:

   - Baud: 9600
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: none
   - Flow Control: none

3. Disconnect power to the VA4200 for 5 seconds, and then reconnect power to begin the boot-up process.

4. Press **Ctrl-C** on the PC when prompted to abort the boot-up sequence. See Figure 9—"Accessing the Bootloader by Interrupting the Boot Sequence" on page 115.

5. Enter "**`vboot -p`**" to reboot the AP/Bridge using the default password.



```
+
RedBoot(tm) bootstrap and debug environment [ROM]
Non-certified release, version 2.0c - built 11:50:13, Sep  7 2004

Platform: Terrier Platform (XScale)
Copyright (C) 2000, 2001, 2002, Red Hat, Inc.
Copyright (C) 2004, Vivato, Inc.

RAM: 0x00000000-0x04000000, [0x00020088-0x037d0808] available
FLASH: 0x50000000 - 0x51000000, 128 blocks of 0x00020000 bytes e
== Executing boot script in 4.000 seconds - enter ^C to abort
^C
RedBoot> vboot -p
```

Within a few seconds of cycling power on the VA4200, the boot-up sequence is displayed.

Press **Ctrl-C** on your PC when this line is displayed. This interrupts the boot-up.

Enter the "`vboot -p`" command to reboot the AP/Bridge using the default password: vivato.

Figure 9—Accessing the Bootloader by Interrupting the Boot Sequence

After the boot-up sequence has completed (~1 minute), you can enter the AP/Bridge's IP address in a web browser (http**s**://<IP address>) and use the default password to access the VivatoVision web interface and reconfigure the AP/Bridge. If the IP address has been changed from the default (169.254.20.1) and is unknown, you can restore the factory default address (see below) or use Linux shell commands to read/set the IP address. See "Linux Commands" on page 117.

Restoring the Default AP/Bridge Configuration

If the administrator password is known, the Linux shell can be accessed using the same null modem serial connection used to access the bootloader. The AP/Bridge's configuration file can then be deleted in order to restore the factory default settings.

> *IMPORTANT! — Deleting the configuration file causes all previous configuration information to be lost, including lists of internal RADIUS server users, MAC filtering lists, SSID configurations, security configurations, WDS link settings, and any other settings that have have been changed.*

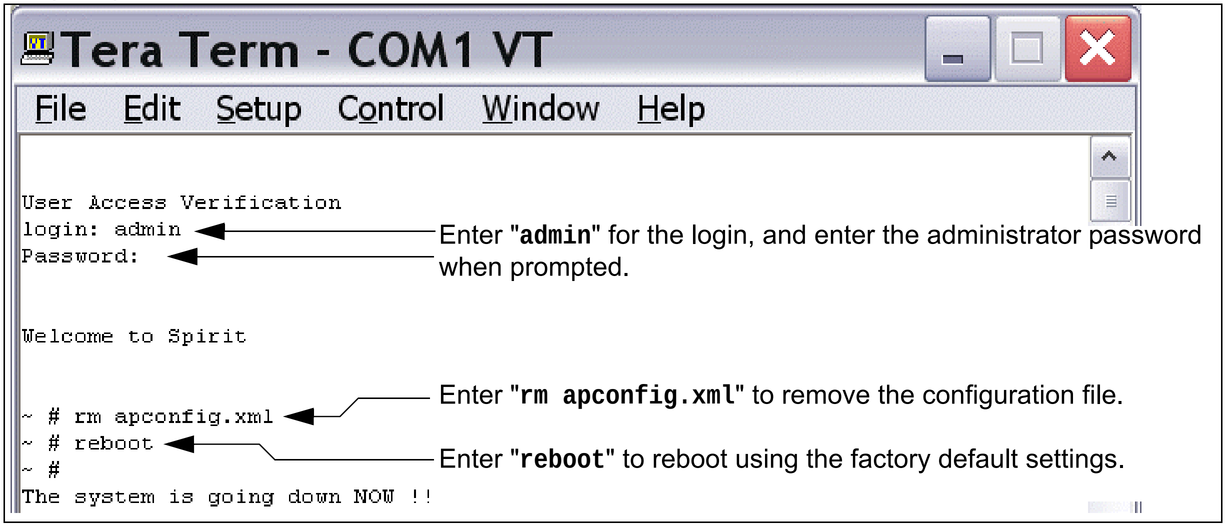
Use the following steps to access the Linux shell command prompt and delete the configuration file:

1. Make the serial connection described in "Restoring the Default Administrator Password" on page 114.

2. Press the **Enter** key on the PC to receive the shell login prompt.

3. Enter "**`admin`**" for the login, then enter the administrator password to access the shell command

prompt and enter Linux commands. *All commands are case sensitive*.



```
User Access Verification
login: admin
Password:


Welcome to Spirit


~ # rm apconfig.xml
~ # reboot
~ #
The system is going down NOW !!
```

Enter "**`admin`**" for the login, and enter the administrator password when prompted.

Enter "**`rm apconfig.xml`**" to remove the configuration file.

Enter "**`reboot`**" to reboot using the factory default settings.

4. Enter "**`rm apconfig.xml`**" to remove the configuration file.

5. Enter "**`reboot`**" to reboot the AP/Bridge using the factory default settings. After the reboot has completed (~1 minute) the AP/Bridge can be accessed using the default password ("vivato") and the default IP address and netmask (169.254.20.1, 255.255.0.0). In order to reconfigure the AP/Bridge, the network interface on the computer communicating with the AP/Bridge must be configured within the same IP subnet as this IP address.

Linux Commands

The following table lists some Linux commands and their use, and are listed for users who are experienced in configuring network devices using the Linux operating system.

Command	Operation
ls <opt -l>	List files in the current directory. Specifying the "-l" option displays the listing with additional file size and permissions information: ~ # ls apconfig.xml spirit.bin.bak ssh_host_rsa_key apconfig.xml.bak ssh_host_dsa_key ssh_host_rsa_key.pub newconfig.xml ssh_host_dsa_key.pub vision redboot_VA4200_20c.bin ssh_host_key spirit.bin ssh_host_key.pub ~ # ls -l -rw-r--r-- 1 root root 24170 Jan 1 00:03 apconfig.xml -rw-r--r-- 1 root root 24189 Jan 1 00:03 apconfig.xml.bak -rw-r--r-- 1 root root 24170 Jan 1 00:18 newconfig.xml -rw-r--r-- 1 root root 334364 Sep 15 2004 redboot_VA4200_20c.bin -rw------- 1 root root 4361263 Jan 1 00:03 spirit.bin -rw------- 1 root root 4360739 Jan 1 00:02 spirit.bin.bak -rw------- 1 root root 668 Jan 1 1970 ssh_host_dsa_key -rw-r--r-- 1 root root 601 Jan 1 1970 ssh_host_dsa_key.pub -rw------- 1 root root 526 Jan 1 1970 ssh_host_key -rw-r--r-- 1 root root 330 Jan 1 1970 ssh_host_key.pub -rw------- 1 root root 887 Jan 1 1970 ssh_host_rsa_key -rw-r--r-- 1 root root 221 Jan 1 1970 ssh_host_rsa_key.pub drwxr-xr-x 1 nobody root 0 Jan 1 1970 vision ~ #

rm <file name>	Remove the specified file. For example, to remove the AP/Bridge's configuration file called "apconfig.xml" (shown in the "ls" command example above) enter **`rm apconfig.xml`**:
	
	`~ # rm apconfig.xml`
	`~ # ls`
	`apconfig.xml.bak        spirit.bin.bak          ssh_host_key.pub`
	`newconfig.xml           ssh_host_dsa_key        ssh_host_rsa_key`
	`redboot_VA4200_20c.bin  ssh_host_dsa_key.pub    ssh_host_rsa_key.pub`
	`spirit.bin              ssh_host_key            vision`
	`~ #`

cp <current file name> <copy file name>	Create a copy of a file in the same directory using a different name. For example, **`cp apconfig.xml newconfig.xml`** makes a copy of the current configuration file (apconfig.xml) and saves it as "newconfig.xml".

<table>
<tr><th>Command(Continued)</th><th>Operation(Continued)</th></tr>
<tr><td><b>ps</b></td><td>

Displays a list of processes that are currently running on the AP/Bridge. This information may be helpful in some support situations.

```
~ # ps
  PID  Uid     VmSize Stat Command
    1 root        352 S   init
    2 root            SW  [keventd]
    3 root            SWN [ksoftirqd_CPU0]
    4 root            SW  [kswapd]
    5 root            SW  [bdflush]
    6 root            SW  [kupdated]
    7 root            SW  [mtdblockd]
   15 root            SWN [jffs2_gcd_mtd1]
   78 root            SW  [ixp425 eth0]
146 root       1316 S   /sbin/apconfd
  147 root        448 S   -sh
  150 root       1052 S   /usr/sbin/sshd -D -f /etc/sshd.conf
  157 root       672 S   /usr/sbin/mini_httpd -D -u root -c ./*.cgi|*.
  158 root      1036 S   /usr/sbin/mini_httpd -D -u root -c ./*.cgi|*.
  159 root       616 R  /usr/sbin/hostapd /var/tmp/hostapd.conf.wlan0
  360 root        328 R   ps
~ #
```

</td></tr>
<tr><td><b>ifconfig</b></td><td>

Used to display the current configuration of the AP/Bridge’s interfaces, and can be used to change the configuration of interfaces. *Any changes made using these commands are temporary; they are not saved into the AP/Bridge’s configuration and therefore are not persistent through a reboot.*

- **ifconfig <interface>**: Displays the current settings for a specific interface, such as eth0, wlan0, wlan1, brweb0 (the default SSID’s bridge). In the example below, the configuration for the default bridge is shown, including the IP address and netmask used to access the VivatoVision web interface.

```
~ # ifconfig brweb0
brweb0    Link encap:Ethernet  HWaddr 00:0B:33:08:05:00
          inet addr:192.168.0.233  Bcast:192.168.0.255  Mask:2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98928 errors:0 dropped:0 overruns:0 frame
          TX packets:253 errors:0 dropped:0 overruns:0 carrier
          collisions:0 txqueuelen:0
          RX bytes:7757394 (7.3 MiB)  TX bytes:178215 (174.0 k
```

- **ifconfig <interface> ip addr <IP address>** : Assign an IP address to an interface. For example, if you enter **brweb0** for the interface, the IP address that you specify is applied to the default bridge connected to the Ethernet 0 port. The VivatoVision web interface can then be accessed using this address (until a reboot is performed). After accessing the VivatoVision web interface, you can assign a persistent IP address by accessing the SSID Configuration settings for the default SSID and setting its IP address there.

</td></tr>
<tr><td><b>cat &lt;file name&gt;</b></td><td>Display the contents of a file. This command is typically used to examine the contents of the AP/Bridge’s configuration file.</td></tr>
</table>

Command(Continued)	Operation(Continued)
brctl show	Displays a list of the interfaces that have been added to existing bridges on the AP/ Bridge. The bridges are designated brweb0 and brweb0. ~ # brctl show bridge name bridge id STP enabled interfaces brweb0 8000.000b33080500 no wlan0 wlan1 eth0 wlan0wds0

Appendix A. Configuring Security Settings on Wireless Clients

Often, users will configure security on their wireless clients for access to many different networks. The list of "Available Networks" will change depending on the location of the client and which VA4200s are online and detectable in that location.[3] Once a VA4200 has been detected by the client and security is configured for it, it remains in the client's list of networks but shows as either reachable or unreachable depending on the situation. For each network (VA4200) you want to connect to, configure security settings on the client to match the security mode being used by that network.

We describe security setup on a client using Microsoft® Windows™ client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on personal and business computers. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey), but the configuration information you need to provide is the same.

Note	The recommended sequence for security configuration is (1) set up security on the AP/Bridge, and (2) configure security on each of the wireless clients. We expect that initially, you will connect to a AP/Bridge that has no security set (plain text mode) from an unsecure wireless client. With this initial connection, you can go to the AP/Bridge VivatoVision Web pages and configure a security mode (INTERFACE MANAGEMENT > SSID Configuration). When you re-configure the AP/Bridge with a security setting and click "Update", your wireless client will be disassociated and you will lose connectivity to the VA4200 VivatoVision Web pages. In some cases, you may need to make additional changes to the VA4200 security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.

The following sections describe how to set up each of the supported security modes on wireless clients of a network served by the Vivato Wi-Fi AP/Bridge.

- Network Infrastructure and Choosing Between Built-in or External Authentication Server
- Make Sure the Wireless Client Software is Up-to-Date
- Accessing the Microsoft Windows Wireless Client Security Settings
- Configuring a Client to Access an Unsecure Network (Plain Text mode)
- Configuring Static WEP Security on a Client
- Configuring IEEE 802.1x Security on a Client
- Configuring WPA with RADIUS Security on a Client
- Configuring WPA-PSK Security on a Client
- Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/Bridge

[3] The exception to this is if the AP/Bridge is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

- Obtaining a TLS-EAP Certificate for a Client

Network Infrastructure and Choosing Between Built-in or External Authentication Server

Network security configurations including *Public Key Infrastructures* (PKI), *Remote Authentication Dial-in User Server* (RADIUS) servers, and *Certificate Authority* (CA) can vary a great deal from one organization to the next in terms of how they provide *Authentication, Authorization,* and *Accounting* (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this document provides general guidelines about each type of client configuration supported by the Vivato Wi-Fi AP/ Bridge.

I Want to Use the Built-in Authentication Server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place and/or are unfamiliar with many of these concepts, we strongly recommend setting up the Vivato Wi-Fi AP/Bridges with security that uses the *Built-in Authentication Server* on the VA4200. This will mean setting up the VA4200 to use either IEEE 802.1x or WPA with RADIUS security mode. (The built-in authentication server uses EAP-PEAP authentication protocol.)

- If the Vivato Wi-Fi AP/Bridge is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in “IEEE 802.1x Client Using EAP/PEAP” on page 127.

- If the Vivato Wi-Fi AP/Bridge is configured to use WPA with RADIUS mode and the Built-in Authentication Server, configure wireless clients as described in “WPA with RADIUS Client Using EAP/PEAP” on page 133.

I Want to Use an External RADIUS Server with EAP-TLS Certificates or EAP-PEAP

We make the assumption that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are as follows:

- “IEEE 802.1x Client Using EAP/TLS Certificate” on page 130

- “WPA with RADIUS Client Using EAP-TLS Certificate” on page 136

- “Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/Bridge” on page 142

- “Obtaining a TLS-EAP Certificate for a Client” on page 145

Details on how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

Make Sure the Wireless Client Software is Up-to-Date

Before starting out, please keep in mind that service packs, patches, and new releases of drivers and other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is not having the right driver or updates to it on the client. For example; if you are setting up WPA on the client, make sure you have a driver installed that supports WPA, which is a relatively new technology. Even many client cards currently available do not ship from the factory with the latest drivers.

Accessing the Microsoft Windows Wireless Client Security Settings

Generally, on Windows XP™ there are two ways to get to the security properties for a wireless client:

1. From the wireless connection icon on the Windows task bar:

   › Right-click on the Wireless connection icon in your Windows task bar and select **View available wireless networks**.

   › Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

   Or

1. From the Windows Start menu at the left end of the task bar:

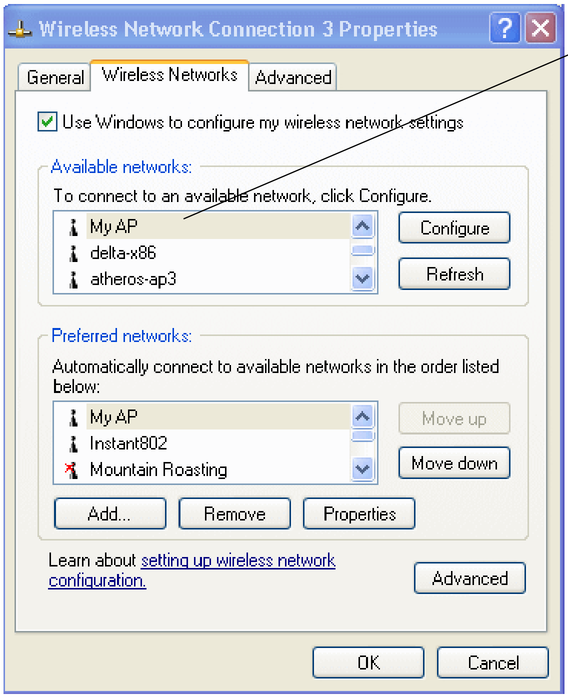
   › From the Windows Start menu on the task bar, choose **Start > My Network Places** to bring up the Network Connections window.

   › From the Network Tasks menu on the left, click **View Network Connections** to bring up the Network Connections window.

   › Select the Wireless Network Connection you want to configure, right-mouse click and choose **View available wireless networks**.

   › Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

   The Wireless Networks tab (which should be automatically displayed) lists Available networks and Preferred networks.



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

My AP
delta-x86
atheros-ap3

Automatically connect to available networks in the order listed below:

My AP
Instant802
Mountain Roasting

Learn about setting up wireless network configuration.

List of available networks will change depending on client location. Each network (or AP/Bridge) that that is detected by the client shows up in this list. ("Refresh" updates the list with current information.)

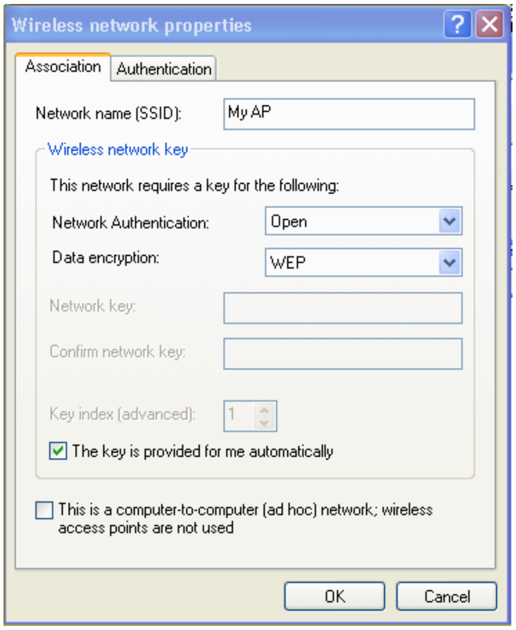
For each network you want to connect to, configure security settings on the client to match the security mode being used by that network.

Note: The exception to this is if the AP/Bridge is configured to prohibit broadcast of its network name, the name will not show on this list. In that case you would need to type in the exact network name to be able to connect to it.

2. From the list of "Available networks", select the SSID of the network to which you want to connect and

click **Configure**.

This brings up the Wireless Network Connection Properties dialog with the Association and Authentication tabs for the selected network.


Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

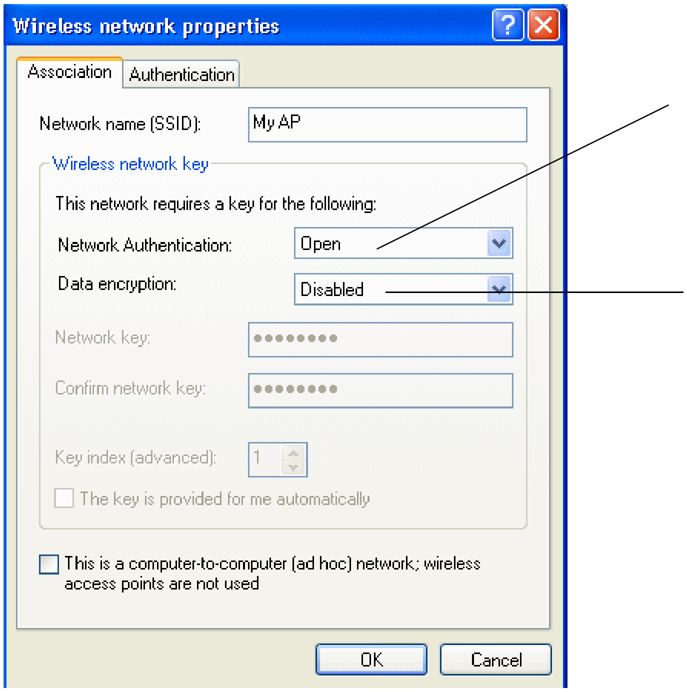
Use this dialog for configuring all the different types of client security described in the following sections. Make sure that the Wireless Network Properties dialog you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

Configuring a Client to Access an Unsecure Network (Plain Text mode)

If the AP/Bridge or wireless network to which you want to connect is configured as "Plain Text" security mode (no security), you need to configure the client accordingly. A client using no security to connect is configured with Network Authentication "Open" to that network and Data Encryption "Disabled" as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and AP/Bridge security configurations.

To configure the client to not use any security, bring up the client Network Properties dialog and configure the following settings.



Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Set Network Authentication to "Open"

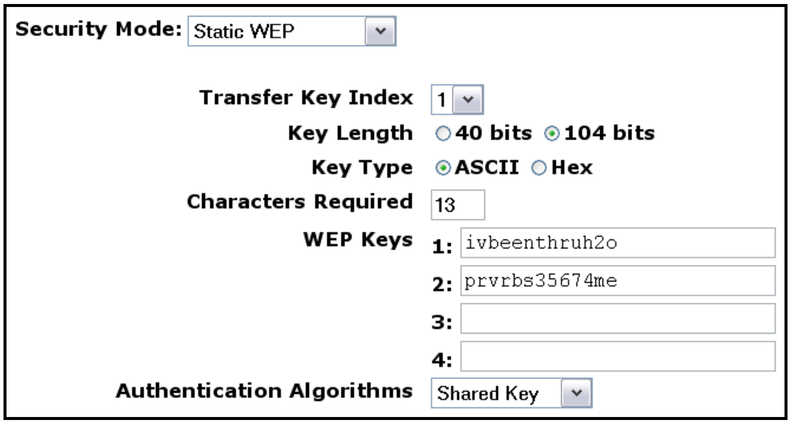
Set Data Encryption to "Disabled"

Association Tab	Network Authentication	Open
	Data Encryption	Disabled

Configuring Static WEP Security on a Client

Static *Wired Equivalent Privacy* (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a "stream" cipher called RC4. The AP/Bridge uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the AP/Bridge. Different clients can use different keys to transmit data to the AP/Bridge. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

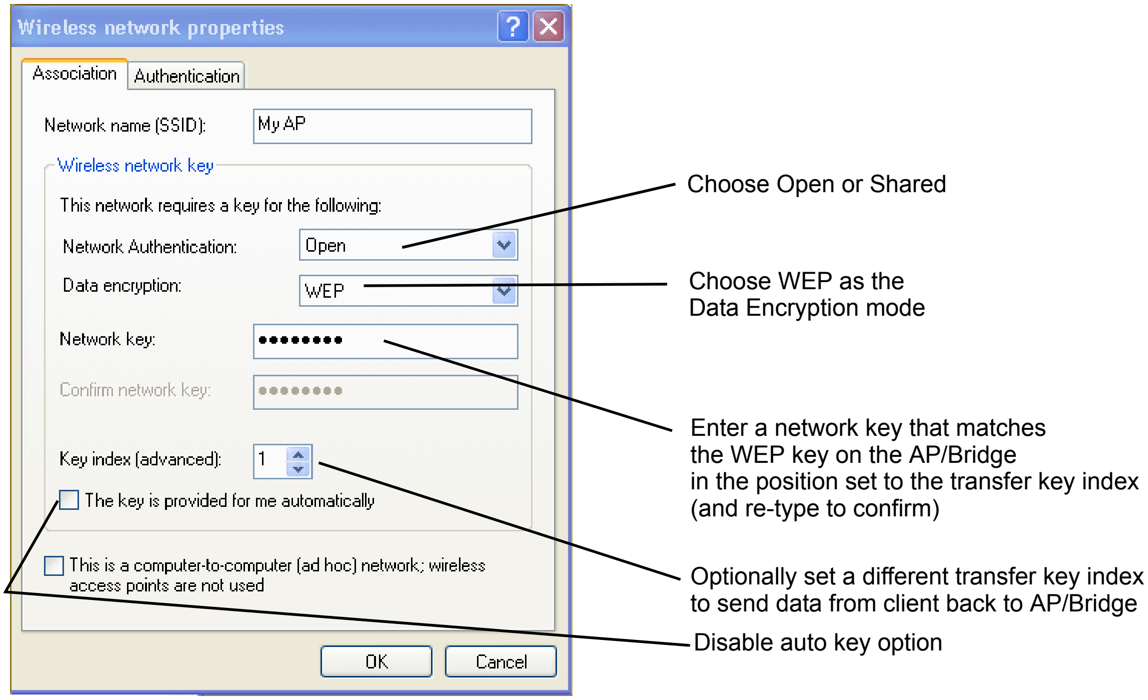
If you configured the Vivato Wi-Fi AP/Bridge to use Static WEP security mode . . .



Security Mode: Static WEP

Transfer Key Index	1
Key Length	○ **40 bits** ● **104 bits**
Key Type	● **ASCII** ○ **Hex**
Characters Required	13
WEP Keys	**1:** ivbeenthruh2o **2:** prvrbs35674me **3:** **4:**
Authentication Algorithms	Shared Key

. . . then configure WEP security on each client as follows.



Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ●●●●●●●●

Confirm network key: ●●●●●●●●

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Choose Open or Shared

Choose WEP as the Data Encryption mode

Enter a network key that matches the WEP key on the AP/Bridge in the position set to the transfer key index (and re-type to confirm)

Optionally set a different transfer key index to send data from client back to AP/Bridge

Disable auto key option

Association Tab	Network Authentication	"Open" or "Shared", depending on how you configured this option on the AP/Bridge. **Note:** When the Authentication Algorithm on the AP/Bridge is set to "Both", clients set to either Shared or Open can associate with the VA4200. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the VA4200. Clients configured to use WEP as an Open system can associate with the VA4200 even without a valid WEP key (but a valid key will be required to actually view and exchange data). For more information, see this Users Guide and the Online Help on the AP/Bridge.
	Data Encryption	WEP
	Network Key	Provide the WEP key you entered on the AP/Bridge Security settings in the Transfer Key Index position. For example, if the Transfer Key Index on the AP/Bridge is set to "1", then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the AP/Bridge.
	Key Index	Set key index to indicate which of the WEP keys specified on the AP/Bridge Security page will be used to transfer data from the client back to the AP/Bridge. For example, you can set this to 1, 2, 3, or 4 if you have all four WEP keys configured on the AP/Bridge.
	The key is provided for me automatically	Disable this option (click to uncheck the box).
Authentication Tab	Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (box should be unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting to the Wireless Network with a Static WEP Client

Static WEP clients should now be able to associate and authenticate with the AP/Bridge. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

Configuring IEEE 802.1x Security on a Client

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. *Extensible Authentication Protocol* (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

IEEE 802.1x Client Using EAP/PEAP

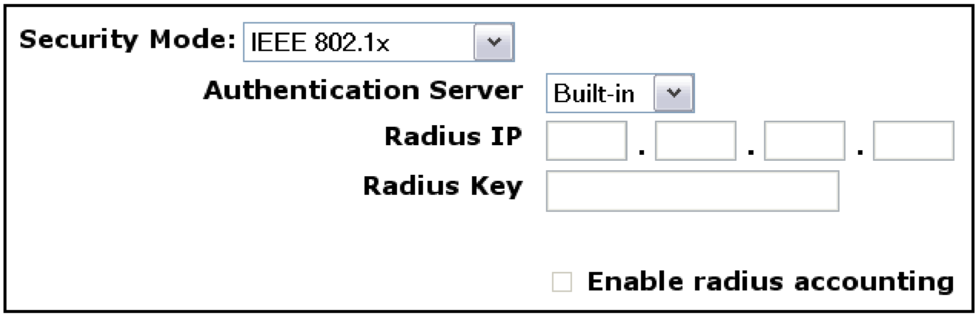
The Built-In Authentication Server on the Vivato Wi-Fi AP/Bridge uses Protected *Extensible Authentication Protocol* (EAP) referred to here as "EAP/PEAP".

- If you are using the Built-in Authentication server with "IEEE 802.1x" security mode on the Vivato Wi-Fi AP/Bridge, then you will need to set up wireless clients to use PEAP.

- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the Vivato Wi-Fi AP/Bridge to the list of RADIUS server clients, and (2) configure your IEEE 802.1x wireless clients to use PEAP.

Note	The following example assumes you are using the Built-in Authentication server that comes with the Vivato Wi-Fi AP/Bridge. If you are setting up EAP/PEAP on a client of a VA4200 that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

If you configured the Vivato Wi-Fi AP/Bridge to use IEEE 802.1x security mode . . .



Security Mode: IEEE 802.1x

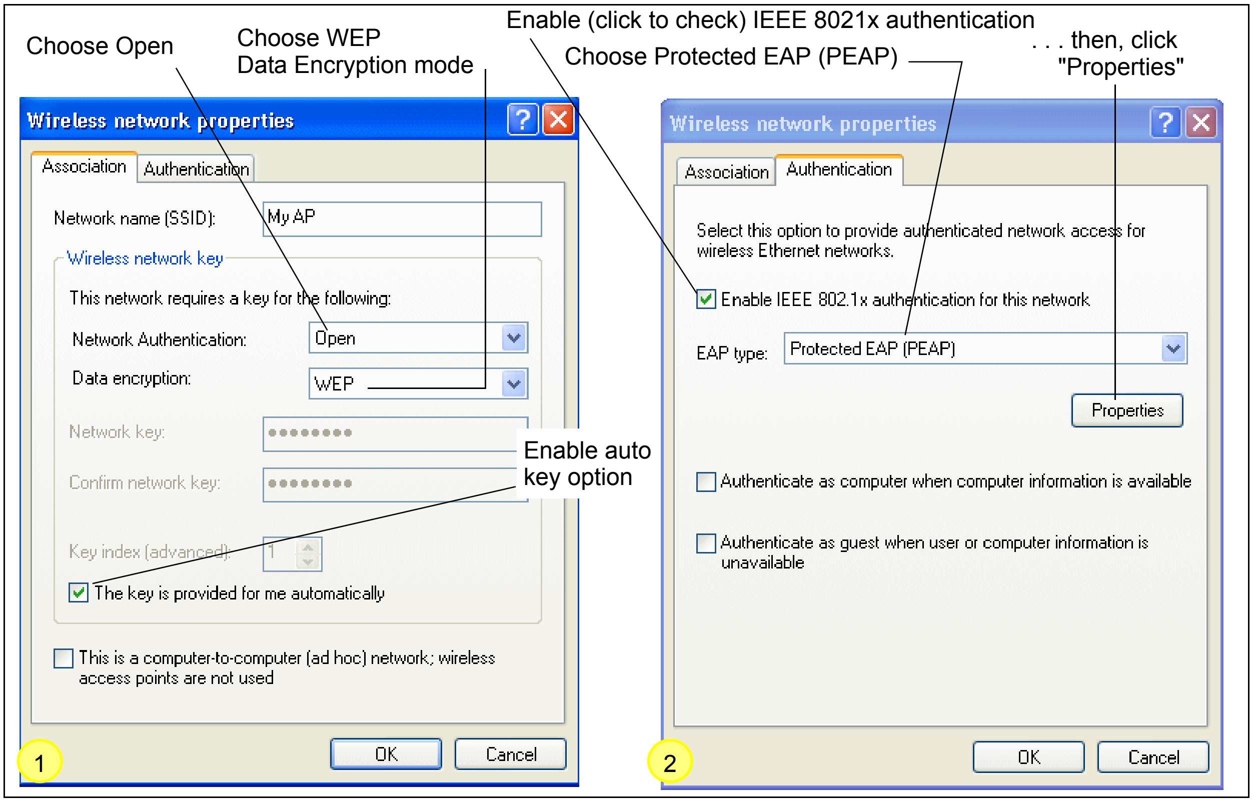
Authentication Server: Built-in

Radius IP: . . .

Radius Key:

□ Enable radius accounting

. . . then configure IEEE 802.1x security with PEAP authentication on each client as follows.



Choose Open

Choose WEP Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose Protected EAP (PEAP)

. . . then, click "Properties"

Enable auto key option

1

Wireless network properties

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ●●●●●●●●

Confirm network key: ●●●●●●●●

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

2

Wireless network properties

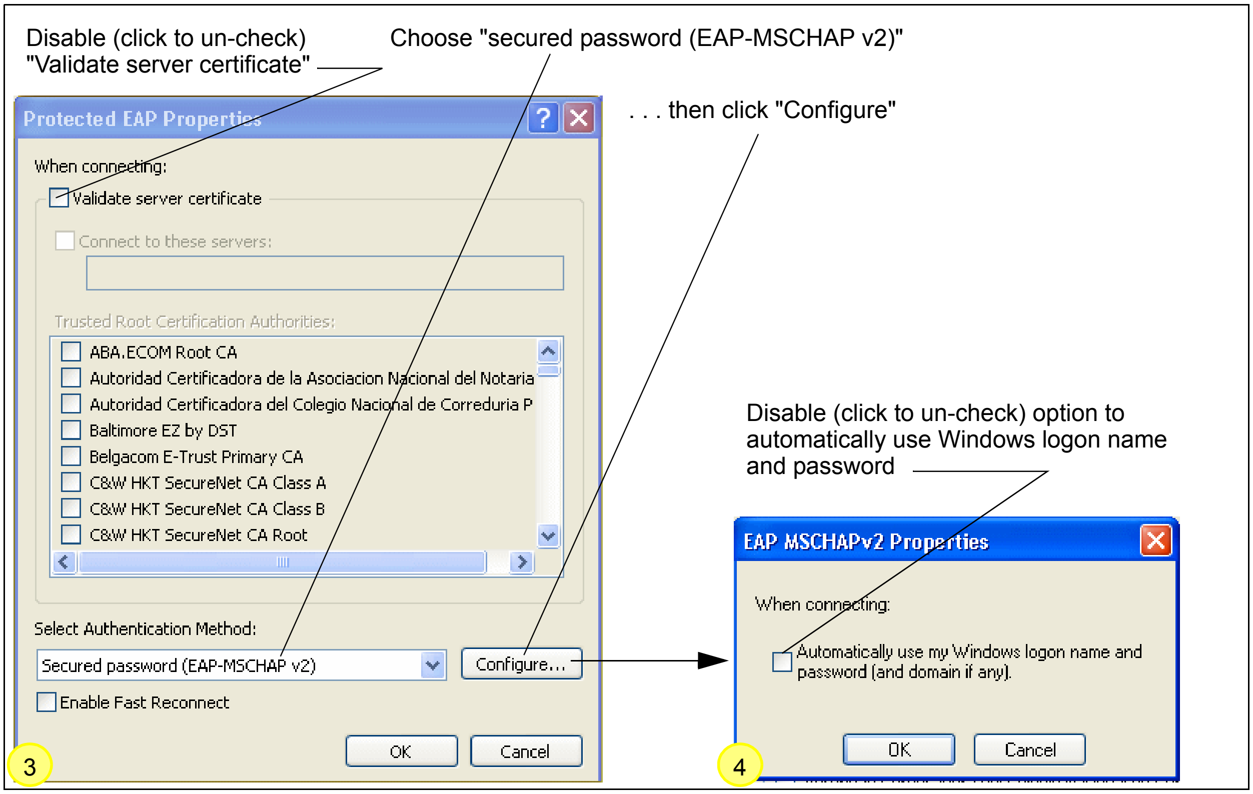
Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable



Disable (click to un-check) "Validate server certificate"

Choose "secured password (EAP-MSCHAP v2)"

. . . then click "Configure"

Disable (click to un-check) option to automatically use Windows logon name and password

3

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA

□ Autoridad Certificadora de la Asociacion Nacional del Notaria

□ Autoridad Certificadora del Colegio Nacional de Correduria P

□ Baltimore EZ by DST

□ Belgacom E-Trust Primary CA

□ C&W HKT SecureNet CA Class A

□ C&W HKT SecureNet CA Class B

□ C&W HKT SecureNet CA Root

Select Authentication Method: Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

4

EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

1. Configure the following settings on the **Association** tab on the Network Properties dialog.

Association Tab	Network Authentication	Open
	Data Encryption	WEP **Note:** An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
	This key is provided for me automatically	Enable (click to check) this option.

2. Configure this setting on the **Authentication** tab.

Authentication Tab	EAP Type	Choose "Protected EAP (PEAP)".

3. Click **Properties** to bring up the Protected EAP Properties dialog and configure the following settings.

Protected EAP Properties Dialog	Validate Server Certificate	Disable this option (click to un-checked the box). **Note:** This example assumes you are using the Built-in Authentication server on the VA4200. If you are setting up EAP/PEAP on a client of an VA4200 that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.
	Select Authentication Method	Choose "Secured password (EAP-MSCHAP v2)".

4. Click **Configure** to bring up the EAP MSCHAP v2 Properties dialog.

   On this dialog, disable (click to un-checked) the option to "Automatically use my Windows login name . . . " etc.

   Click **OK** on all dialogs (starting with the EAP MSCHAP v2 Properties dialog) to close and save your changes.

Logging on to the Wireless Network with an IEEE 802.1x PEAP Client

IEEE 802.1x PEAP clients should now be able to associate with the AP/Bridge. Client users will be prompted for a user name and password to authenticate with the network.

IEEE 802.1x Client Using EAP/TLS Certificate

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note

> If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure* (PKI) server, including a *Certificate Authority* (CA), configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.
>
> Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881 and How to Configure a Certificate Server at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

To use this type of security, you must do the following:

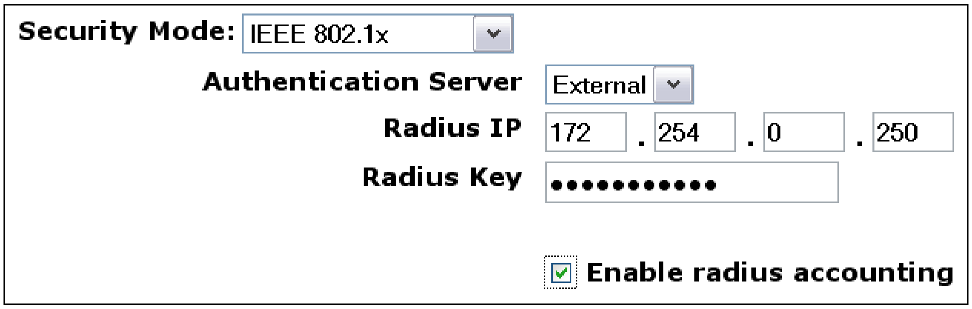
1. Add the Vivato Wi-Fi AP/Bridge to the list of RADIUS server clients. (See “Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/Bridge” on page 142.)

2. Configure the Vivato Wi-Fi AP/Bridge to use your RADIUS server (by providing the RADIUS server IP address as part of the "IEEE 802.1x" security mode settings).

3. Configure wireless clients to use IEEE 802.1x security and "Smart Card or other Certificate" as described in this section.

4. Obtain a certificate for this client as described in “Obtaining a TLS-EAP Certificate for a Client” on page 145.

If you configured the Vivato Wi-Fi AP/Bridge to use IEEE 802.1x security mode with an external RADIUS server . . .



Security Mode: IEEE 802.1x

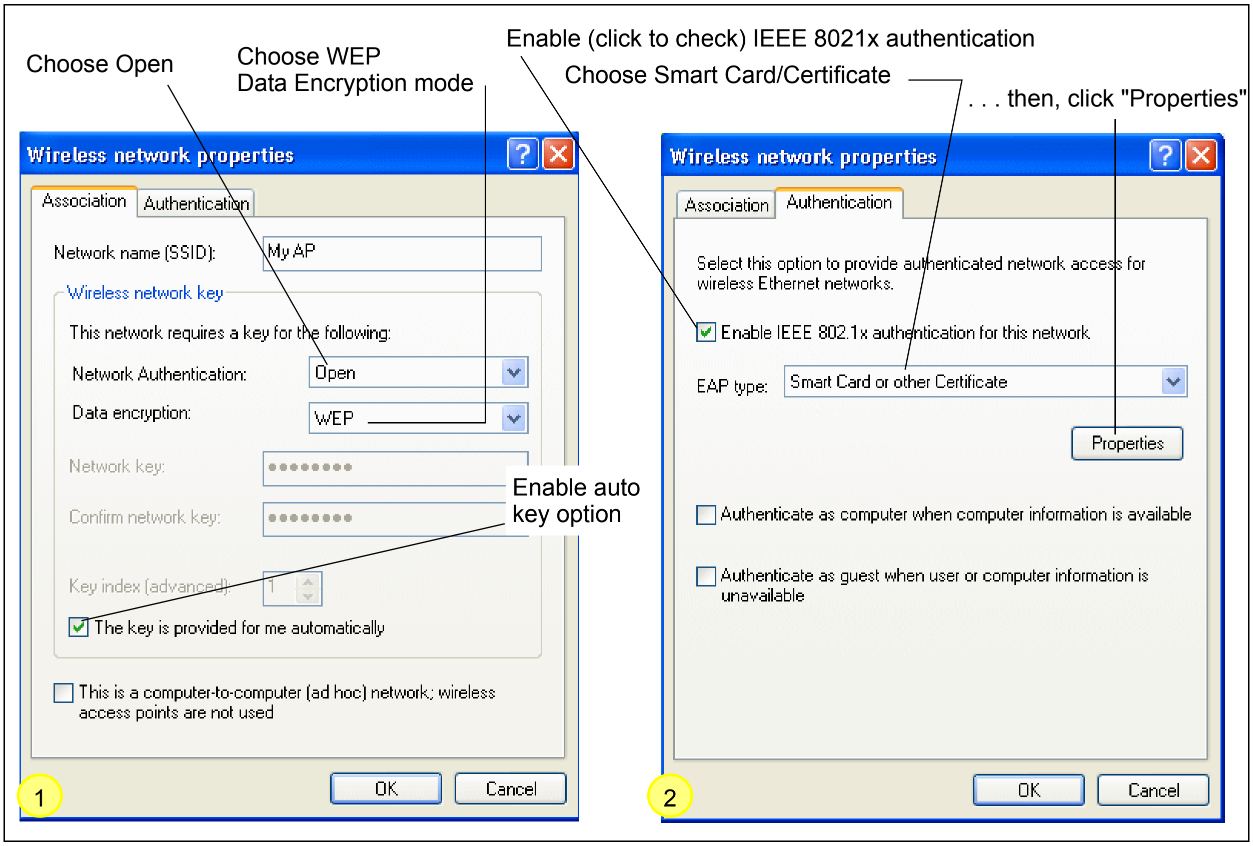
Authentication Server: External

Radius IP: 172 . 254 . 0 . 250

Radius Key: ●●●●●●●●●●●

☑ Enable radius accounting

. . . then configure IEEE 802.1x security with certificate authentication on each client as follows.



Choose Open

Choose WEP
Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose Smart Card/Certificate

. . . then, click "Properties"

Enable auto
key option

1

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

☑ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

2

Wireless network properties

Association | Authentication

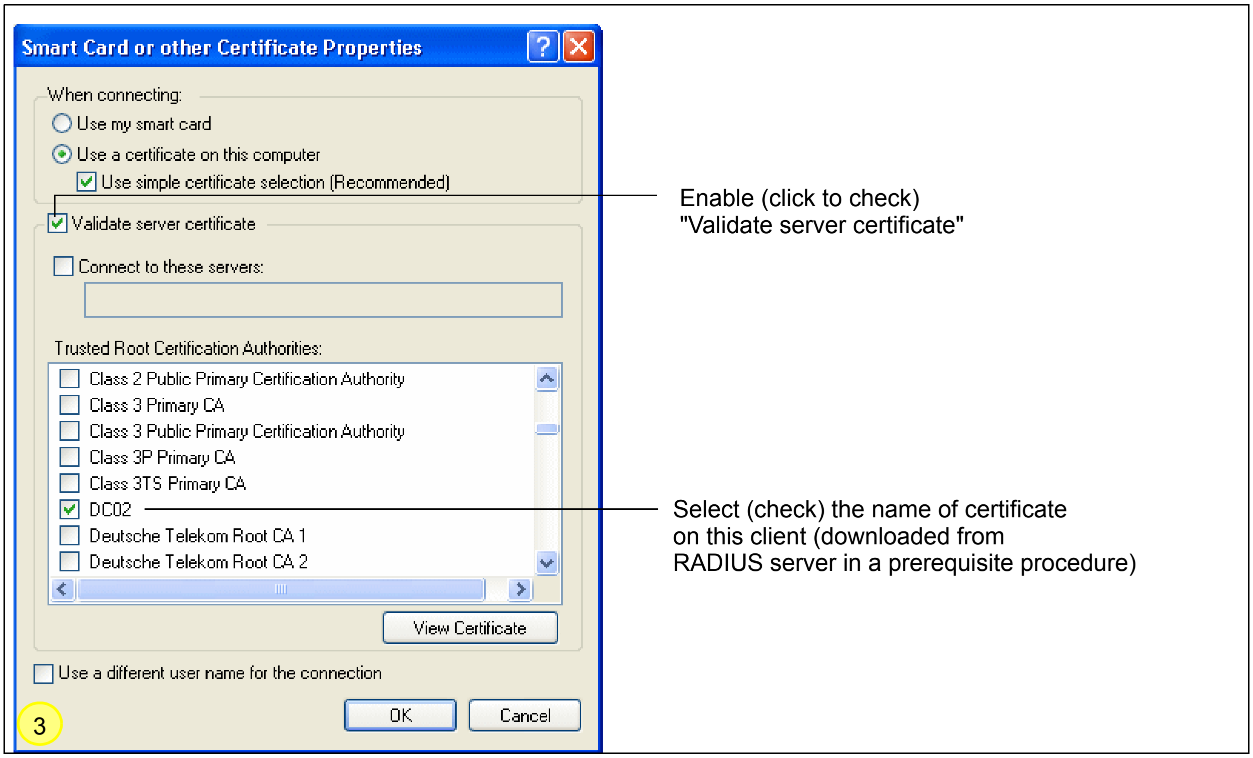
Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable



3

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

☐ Class 2 Public Primary Certification Authority
☐ Class 3 Primary CA
☐ Class 3 Public Primary Certification Authority
☐ Class 3P Primary CA
☐ Class 3TS Primary CA
☑ DC02
☐ Deutsche Telekom Root CA 1
☐ Deutsche Telekom Root CA 2

☐ Use a different user name for the connection

Enable (click to check)
"Validate server certificate"

Select (check) the name of certificate
on this client (downloaded from
RADIUS server in a prerequisite procedure)

1. Configure the following settings on the Association tab on the Network Properties dialog.

Association Tab	Network Authentication	Open
	Data Encryption	WEP **Note:** An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
	This key is provided for me automatically	Enable (click to check) this option.

2. Configure these settings on the Authentication tab.

Authentication Tab	Enable IEEE 802.1x authentication for this network	Enable (click to check) this option.
	EAP Type	Choose Smart Card or other Certificate.

3. Click **Properties** to bring up the Smart Card or other Certificate Properties dialog and enable the "Validate server certificate" option.

Smart Card or other Certificate Properties Dialog	Validate Server Certificate	Enable this option (click to check the box).
	Certificates	In the certificate list shown, select the certificate for this client.

   Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see "Obtaining a TLS-EAP Certificate for a Client" on page 145.

Connecting to the Wireless Network with an IEEE 802.1x Client Using a Certificate

IEEE 802.1x clients should now be able to connect to the AP/Bridge using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA with RADIUS Security on a Client

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), and *Counter mode/ CBC-MAC Protocol* IEEE. This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts on the AP/Bridge.

When you configure WPA with RADIUS security mode on the AP/Bridge, you have a choice of whether to use the Built-in Authentication Server or an external RADIUS server that you provide.

The Vivato Wi-Fi AP/Bridge Built-in Authentication Server supports Protected *Extensible Authentication Protocol* (EAP) known as "EAP/PEAP" and *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAP V2), which provides authentication for point-to-point protocol (PPP) connections between a Windows-based computer and network devices such as AP/Bridges.

So, if you configure the network (AP/Bridge) to use security mode and choose the Built-in Authentication server, you must configure client stations to use WPA with RADIUS and EAP/PEAP.

If you configure the network (AP/Bridge) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA with RADIUS and whichever security protocol your RADIUS server is configured to use.

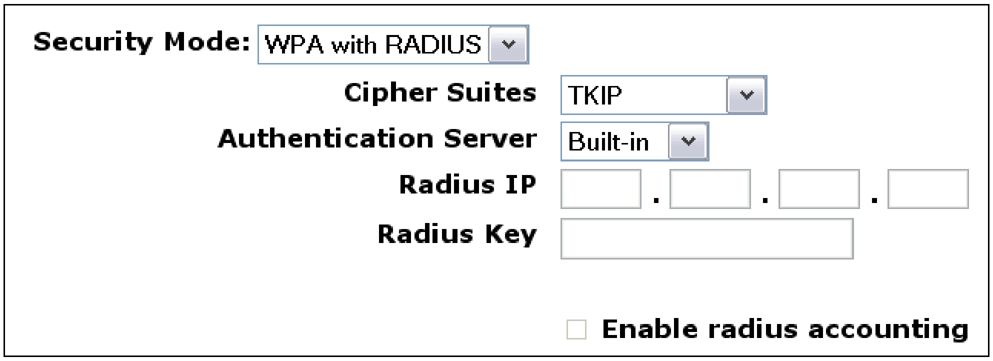
WPA with RADIUS Client Using EAP/PEAP

The Built-In Authentication Server on the Vivato Wi-Fi AP/Bridge uses Protected *Extensible Authentication Protocol* (EAP) known as "EAP/PEAP".

- If you are using the Built-in Authentication server with "WPA with RADIUS" security mode on the Vivato Wi-Fi AP/Bridge, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the Vivato Wi-Fi AP/Bridge to the list of RADIUS server clients, and (2) configure your "WPA with RADIUS" wireless clients to use PEAP.

Note	The following example assumes you are using the Built-in Authentication server that comes with the Vivato Wi-Fi AP/Bridge. If you are setting up EAP/PEAP on a client of an VA4200 that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

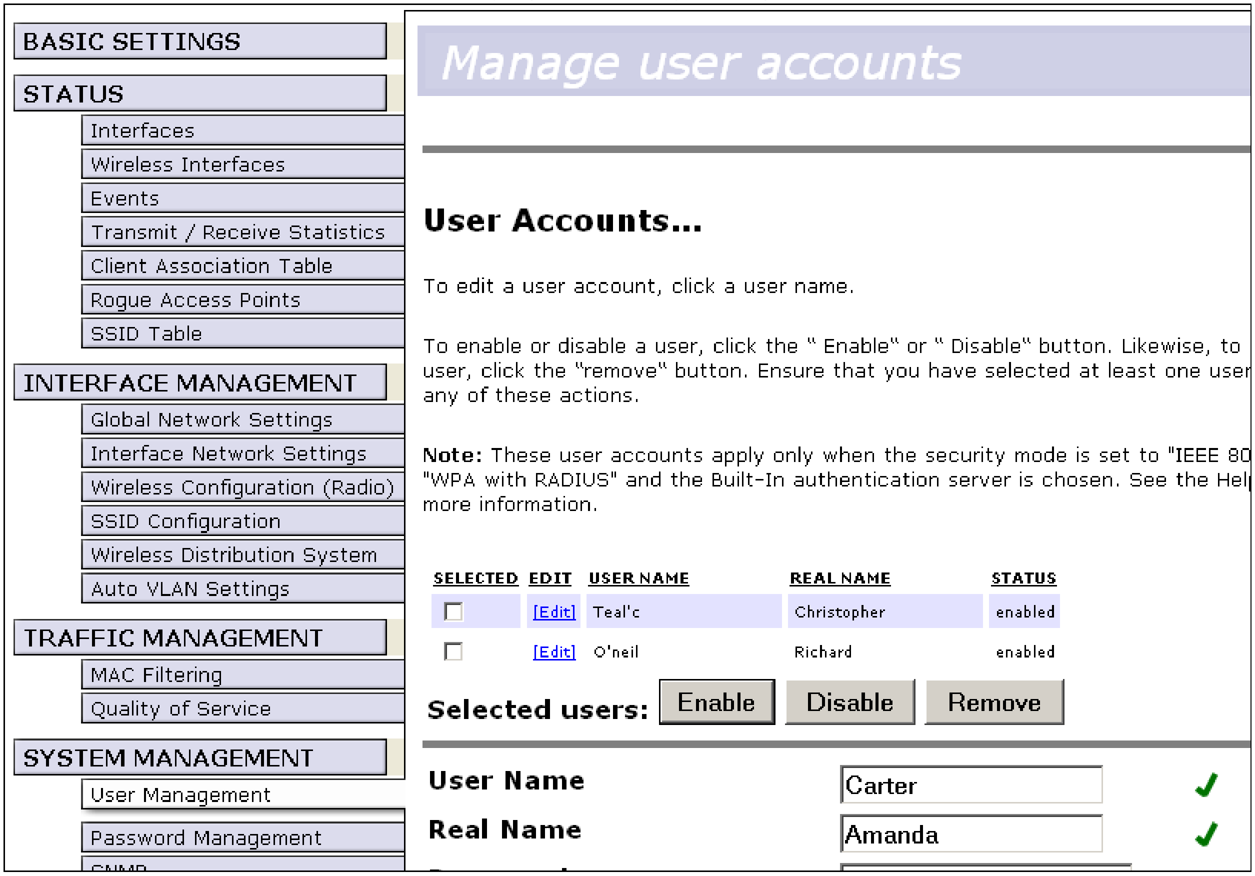
If you configured the Vivato Wi-Fi AP/Bridge to use WPA with RADIUS security mode and to use either the Built-in Authentication Server or an external RADIUS server that uses EAP/PEAP . . .



Security Mode:	WPA with RADIUS
Cipher Suites	TKIP
Authentication Server	Built-in
Radius IP	. . .
Radius Key	

□ **Enable radius accounting**

First set up user accounts on the AP/Bridge (**User Management**). . . .



User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the " Enable" or " Disable" button. Likewise, to user, click the "remove" button. Ensure that you have selected at least one user any of these actions.

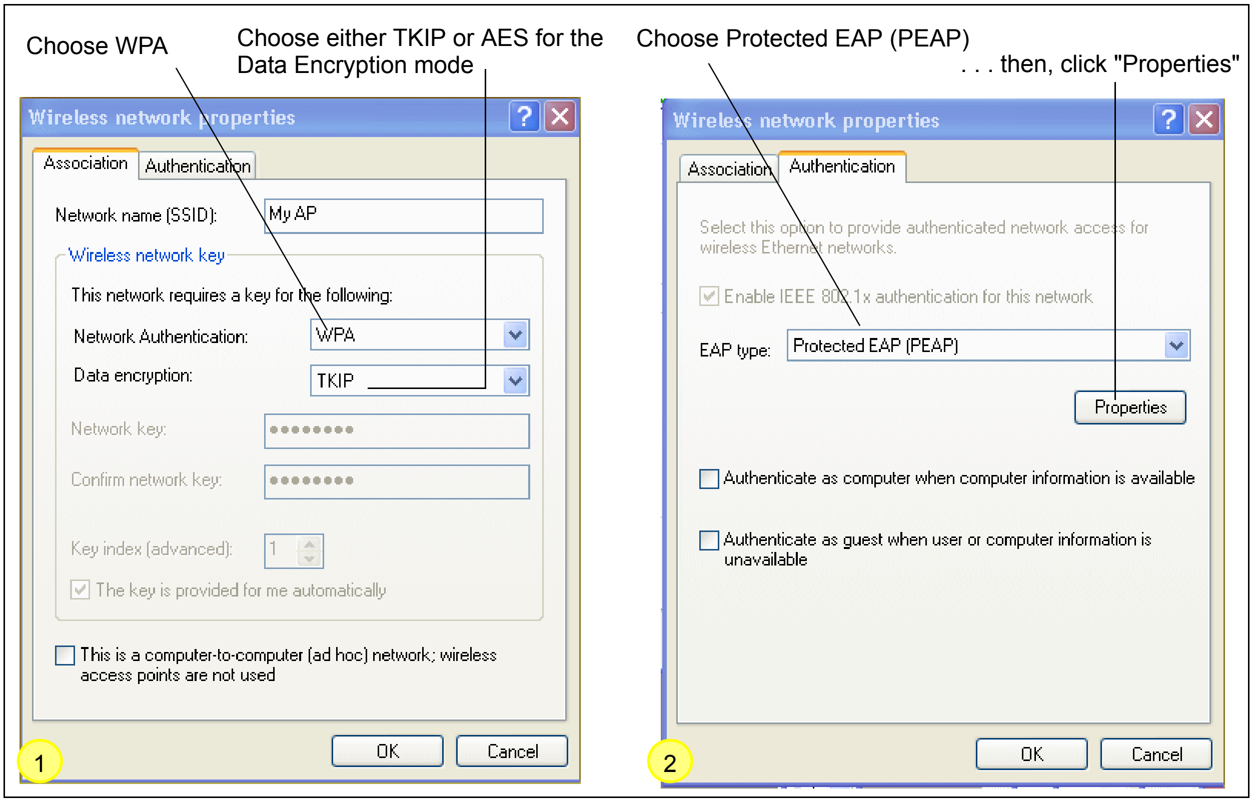
Note: These user accounts apply only when the security mode is set to "IEEE 80 "WPA with RADIUS" and the Built-In authentication server is chosen. See the Hel more information.

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
□	[Edit]	Teal'c	Christopher	enabled
□	[Edit]	O'neil	Richard	enabled

Selected users:

User Name	Carter ✓
Real Name	Amanda ✓

. . . then configure WPA security with PEAP authentication on each client as follows.



Choose WPA

Choose either TKIP or AES for the Data Encryption mode

Choose Protected EAP (PEAP)

. . . then, click "Properties"

1

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key: ●●●●●●●●

Confirm network key: ●●●●●●●●

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK | Cancel

2

Wireless network properties

Association | Authentication

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

☑ Enable IEEE 802.1x authentication for this network

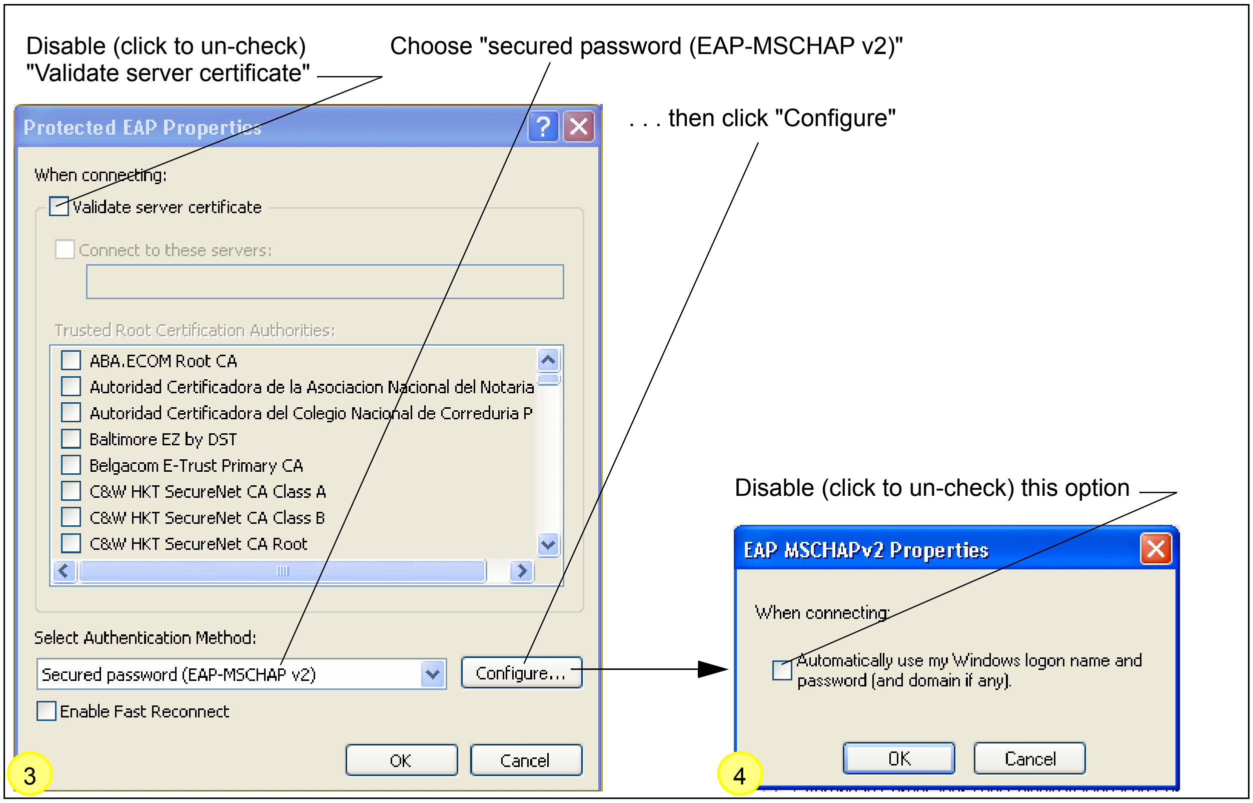
EAP type: Protected EAP (PEAP)

Properties

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

OK | Cancel



Disable (click to un-check) "Validate server certificate"

Choose "secured password (EAP-MSCHAP v2)"

. . . then click "Configure"

Disable (click to un-check) this option

3

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA

□ Autoridad Certificadora de la Asociacion Nacional del Notaria

□ Autoridad Certificadora del Colegio Nacional de Correduria P

□ Baltimore EZ by DST

□ Belgacom E-Trust Primary CA

□ C&W HKT SecureNet CA Class A

□ C&W HKT SecureNet CA Class B

□ C&W HKT SecureNet CA Root

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

□ Enable Fast Reconnect

OK | Cancel

4

EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

1. Configure the following settings on the Association and Authentication tabs on the Network Properties dialog.

Association Tab	Network Authentication	WPA
	Data Encryption	TKIP or AES depending on how this option is configured on the AP/Bridge. **Note:** When the Cipher Suite on the AP/Bridge is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the AP/Bridge. For more information, see Users Guide and Online Help on the AP/Bridge.

2. Configure this setting on the Authentication tab.

Authentication Tab	EAP Type	Choose "Protected EAP (PEAP)"

3. Click **Properties** to bring up the Protected EAP Properties dialog and configure the following settings.

Protected EAP Properties Dialog	Validate Server Certificate	Disable this option (click to un-checked the box). **Note:** This example assumes you are using the Built-in Authentication server on the VA4200. If you are setting up EAP/PEAP on a client of an VA4200 that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.
	Select Authentication Method	Choose "Secured password (EAP-MSCHAP v2)"

4. Click **Configure** to bring up the EAP MSCHAP v2 Properties dialog.

   On this dialog, disable (click to un-checked) the option to "Automatically use my Windows login name . . . " etc. so that upon login you will be prompted for user name and password.

   Click **OK** on all dialogs (starting with the EAP MSCHAP v2 Properties dialog) to close and save your changes.

Logging on to the Wireless Network with a WPA PEAP Client

"WPA with RADIUS" PEAP clients should now be able to associate with the AP/Bridge. Client users will be prompted for a user name and password to authenticate with the network.

WPA with RADIUS Client Using EAP-TLS Certificate

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note

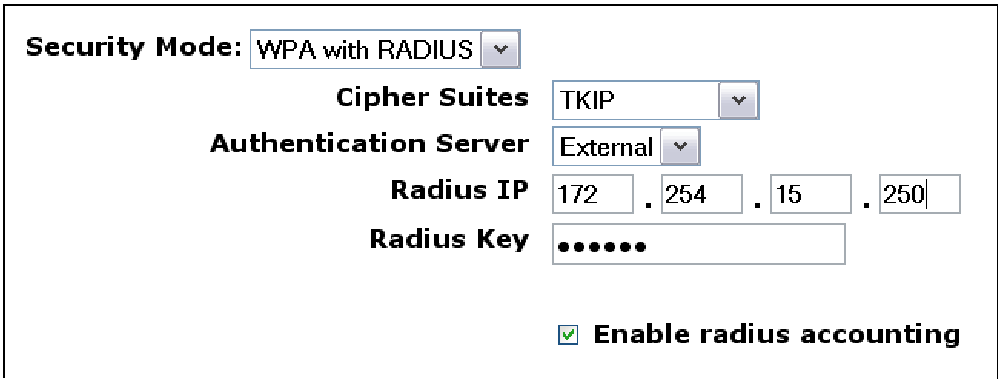
If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure* (PKI) server, including a *Certificate Authority* (CA), configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881 and How to Configure a Certificate Server at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

To use this type of security, you must do the following:

1. Add the Vivato Wi-Fi AP/Bridge to the list of RADIUS server clients. (See “Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/Bridge” on page 142.)
2. Configure the Vivato Wi-Fi AP/Bridge to use your RADIUS server (by providing the RADIUS server IP address as part of the "WPA with RADIUS" security mode settings).
3. Configure wireless clients to use WPA security and "Smart Card or other Certificate" as described in this section.
4. Obtain a certificate for this client as described in “Obtaining a TLS-EAP Certificate for a Client” on page 145.

If you configured the Vivato Wi-Fi AP/Bridge to use WPA with RADIUS security mode with an external RADIUS server . . .



Security Mode: WPA with RADIUS

Cipher Suites: TKIP

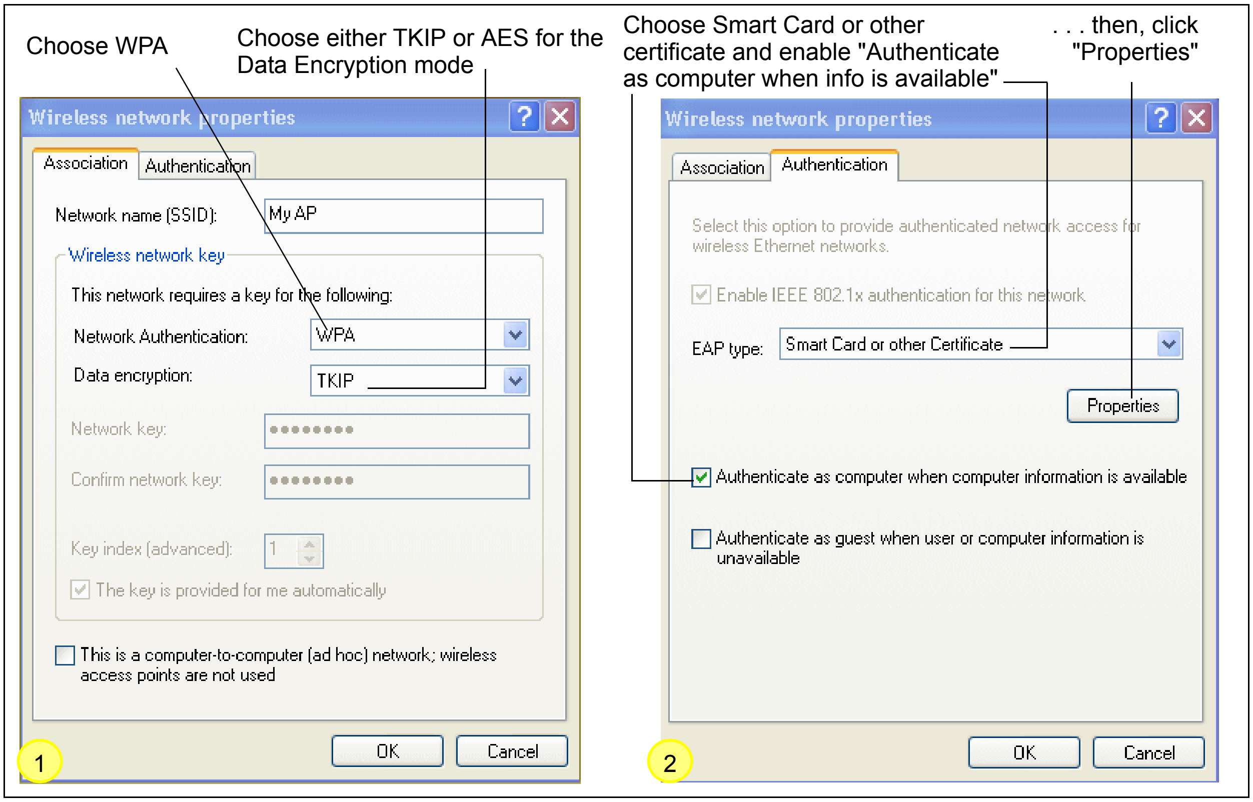
Authentication Server: External

Radius IP: 172 . 254 . 15 . 250

Radius Key: ••••••

☑ Enable radius accounting

. . . then configure WPA security with certificate authentication on each client as follows.



Choose WPA

Choose either TKIP or AES for the Data Encryption mode

Choose Smart Card or other certificate and enable "Authenticate as computer when info is available"

. . . then, click "Properties"

1

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key: ●●●●●●●●

Confirm network key: ●●●●●●●●

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK | Cancel

2

Wireless network properties

Association | Authentication

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

☑ Enable IEEE 802.1x authentication for this network

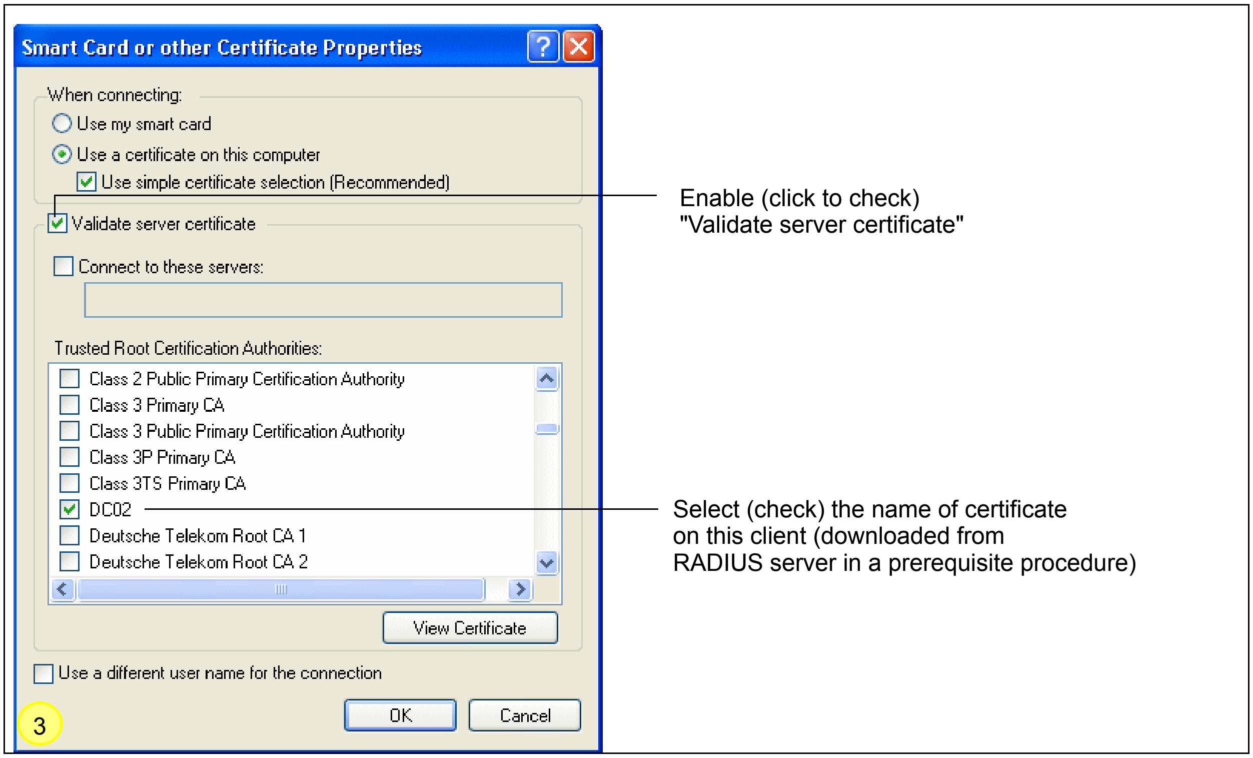
EAP type: Smart Card or other Certificate

Properties

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

OK | Cancel



3

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ Class 2 Public Primary Certification Authority
□ Class 3 Primary CA
□ Class 3 Public Primary Certification Authority
□ Class 3P Primary CA
□ Class 3TS Primary CA
☑ DC02
□ Deutsche Telekom Root CA 1
□ Deutsche Telekom Root CA 2

View Certificate

□ Use a different user name for the connection

OK | Cancel

Enable (click to check) "Validate server certificate"

Select (check) the name of certificate on this client (downloaded from RADIUS server in a prerequisite procedure)

1. Configure the following settings on the Association tab on the Network Properties dialog.

Association Tab	Network Authentication	WPA

	Data Encryption	TKIP or AES depending on how this option is configured on the AP/Bridge. **Note:** When the Cipher Suite on the AP/Bridge is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the AP/Bridge. For more information, see Users Guide and Online Help on the AP/Bridge.

2. Configure these settings on the Authentication tab.

Authentication Tab	Enable IEEE 802.1x authentication for this network	Enable (click to check) this option.
	EAP Type	Choose Smart Card or other Certificate.

3. Click **Properties** to bring up the Smart Card or other Certificate Properties dialog and enable the "Validate server certificate" option.

Smart Card or other Certificate Properties Dialog	Validate Server Certificate	Enable this option (click to check the box).
	Certificates	In the certificate list shown, select the certificate for this client.

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining a TLS-EAP Certificate for a Client” on page 145.

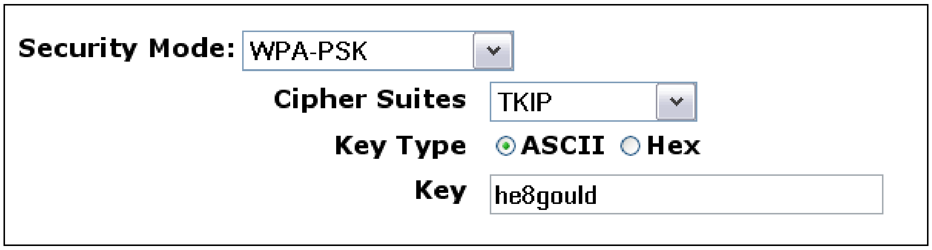
Logging on to the Wireless Network with a WPA Client Using a Certificate

WPA clients should now be able to connect to the AP/Bridge using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA-PSK Security on a Client

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Algorithm* (AES), and *Counter mode/CBC-MAC Protocol* (CCMP) mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

If you configured the Vivato Wi-Fi AP/Bridge to use WPA-PSK security mode . . .



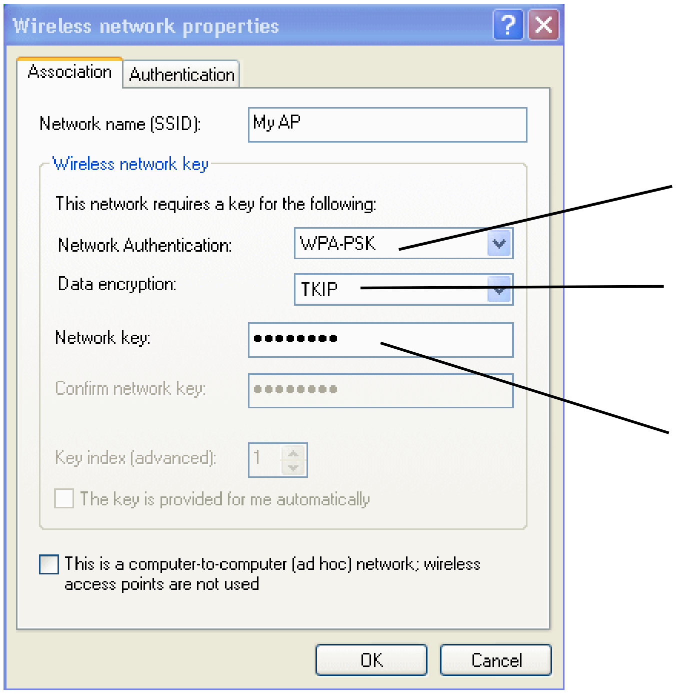
Security Mode: WPA-PSK

Cipher Suites TKIP

Key Type ● **ASCII** ○ **Hex**

Key he8gould

. . . then configure WPA-PSK security on each client as follows.



Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Choose WPA-PSK

Choose either TKIP or AES for the Data Encryption mode

Enter a network key that matches the one specified on the AP/Bridge (and confirm by re-typing)

Association Tab	Network Authentication	WPA-PSK
	Data Encryption	TKIP or AES depending on how this option is configured on the AP/Bridge. **Note:** When the Cipher Suite on the AP/Bridge is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the AP/Bridge. For more information, see Users Guide and Online Help on the AP/ Bridge.

	Network Key	Provide the key you entered on the AP/Bridge Security settings for the cipher suite you are using. For example, if the key on the AP/Bridge is set to use a TKIP key of "012345678", then a TKIP client specify this same string as the network key.
	The key is provided for me automatically	This box should be disabled automatically based on other settings.
Authentication Tab	Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting to the Wireless Network with a WPA-PSK Client

WPA-PSK clients should now be able to associate and authenticate with the AP/Bridge. As a client, you will not be prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

Configuring an External RADIUS Server to Recognize the Vivato Wi-Fi AP/ Bridge

An external *Remote Authentication Dial-in User Server* (RADIUS) server running on the network can support EAP-TLS smart card/certificate distribution to clients in a *Public Key Infrastructure* (PKI) as well as EAP-PEAP user account setup and authentication. By *external* RADIUS server, we mean an authentication server external to the AP/Bridge itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the *Built-in Authentication Server* on the Vivato Wi-Fi AP/Bridge.

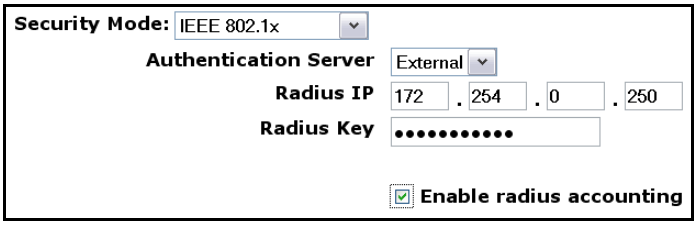
This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular Vivato Wi-Fi AP/Bridge configured for either "WPA with RADIUS" or "IEEE 802.1x" security modes. The intention of this section is to provide some idea of what this process will look like; procedures will vary depending on the RADIUS server you use and how you configure it. For this example, we use the Internet Authentication Service that comes with Microsoft Windows 2003 server.

Note

This document does not describe how to set up Administrative users on the RADIUS server. In this example, we assume you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Please consult the documentation for your RADIUS server for information on setting up user accounts.

The purpose of this procedure is to identify your Vivato Wi-Fi AP/Bridge as a "client" to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the VA4200. This procedure is required *per AP/Bridge*. If you have more than one AP/Bridge with which you plan to use an external RADIUS server, you need to follow these steps for each of those VA4200s.

Keep in mind that the information you need to provide to the RADIUS server about the AP/Bridge corresponds to settings on the AP/Bridge (SSID Configuration) and vice versa. You should have already provided the RADIUS server IP Address to the VA4200; in the steps that follow you will provide the AP/Bridge IP address to the RADIUS server. The RADIUS Key provided on the VA4200 is the "shared secret" you will provide to the RADIUS server.



Security Mode: IEEE 802.1x

Authentication Server: External

Radius IP: 172 . 254 . 0 . 250

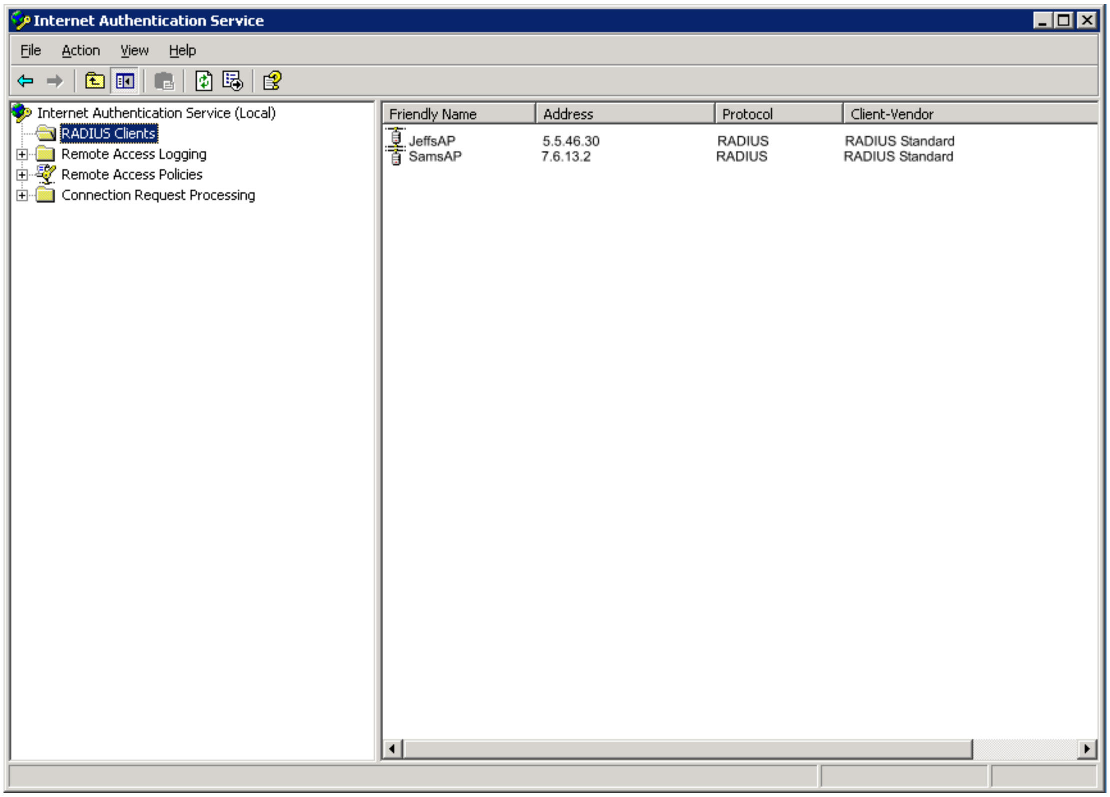
Radius Key: ●●●●●●●●●●●

☑ Enable radius accounting

Note

The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the Vivato Wi-Fi AP/Bridge, the RADIUS server *User Datagram Protocol* (UDP) ports used by the AP/Bridge are not configurable. (The Vivato Wi-Fi AP/Bridge is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

1. Log on to the system hosting your RADIUS server and bring up the Internet Authentication Service.


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

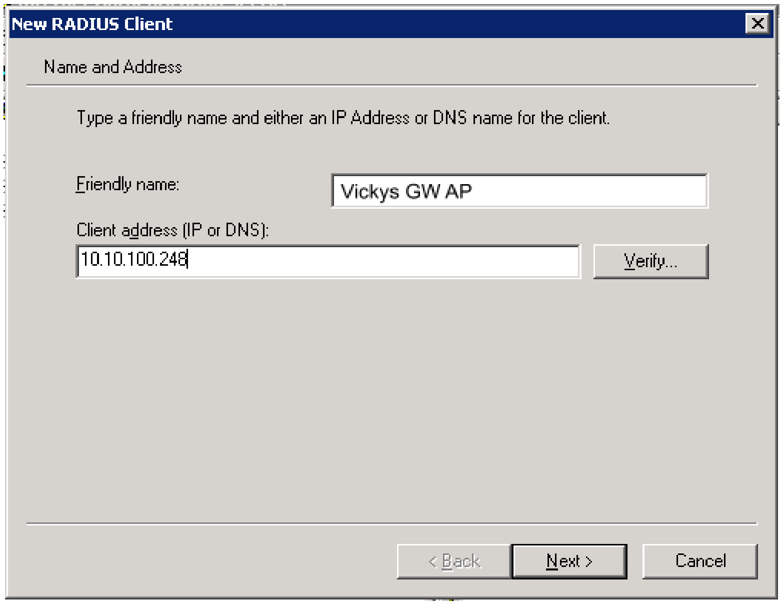
Friendly Name	Address	Protocol	Client-Vendor
JeffsAP	5.5.46.30	RADIUS	RADIUS Standard
SamsAP	7.6.13.2	RADIUS	RADIUS Standard

2. In the left panel, right click on "RADIUS Clients" node and choose New > Radius Client from the popup menu.

3. On the first screen of the New RADIUS Client wizard provide information about the Vivato Wi-Fi AP/ Bridge to which you want your clients to connect:

   › A logical (friendly) name for the AP/Bridge. (You might want to use DNS name or location.)

   › IP address for the AP/Bridge.



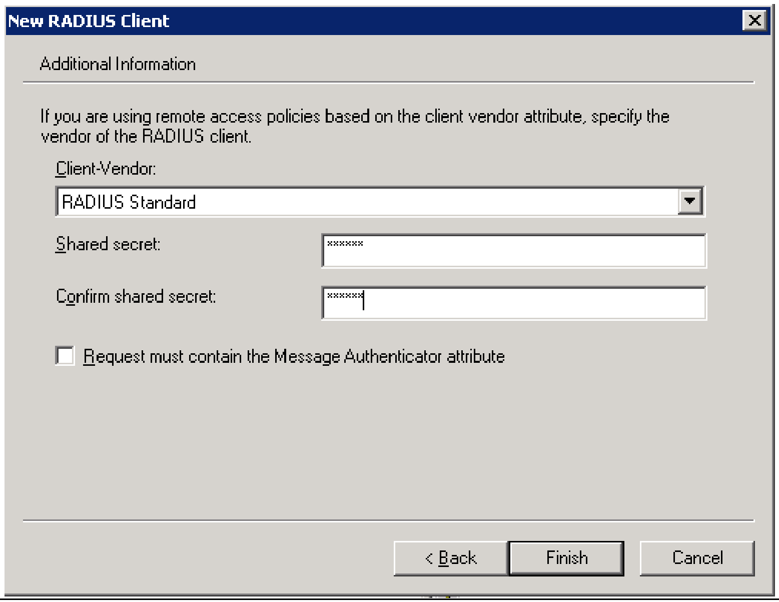
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: Vickys GW AP

Client address (IP or DNS): 10.10.100.248

Click **Next**.

4. For the "Shared secret" enter the RADIUS Key you provided to the AP/Bridge (on the INTERFACE MANAGEMENT > SSID Configuration page). Re-type the key to confirm.



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

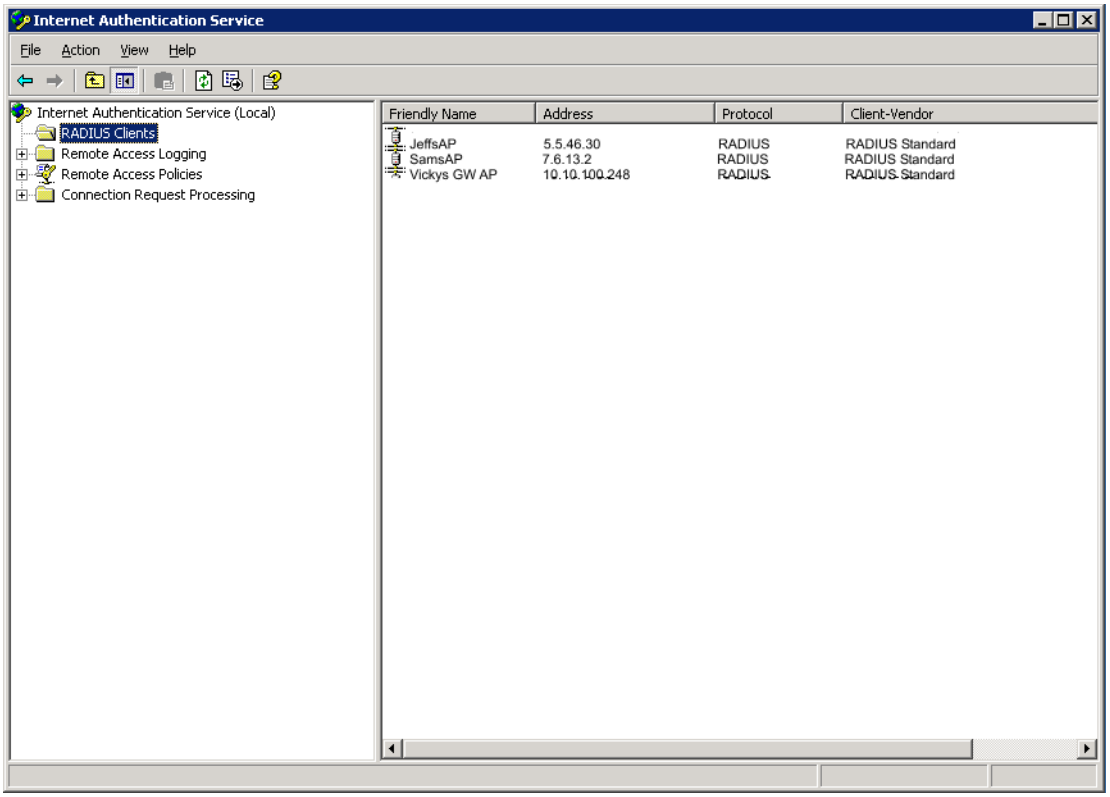
Client-Vendor: RADIUS Standard

Shared secret: ******

Confirm shared secret: ******

☐ Request must contain the Message Authenticator attribute

5. Click **Finish**.



Internet Authentication Service

Friendly Name	Address	Protocol	Client-Vendor
JeffsAP	5.5.46.30	RADIUS	RADIUS Standard
SamsAP	7.6.13.2	RADIUS	RADIUS Standard
Vickys GW AP	10.10.100.248	RADIUS	RADIUS Standard

The AP/Bridge is now displayed as a client of the Authentication Server.

Obtaining a TLS-EAP Certificate for a Client

> **Note**
>
> If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure* (PKI) server, including a *Certificate Authority* (CA), configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.
>
> Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881 and How to Configure a Certificate Server at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

Wireless clients configured to use either "WPA with RADIUS" or" IEEE 802.1x" security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server.

This is an initial one-time step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

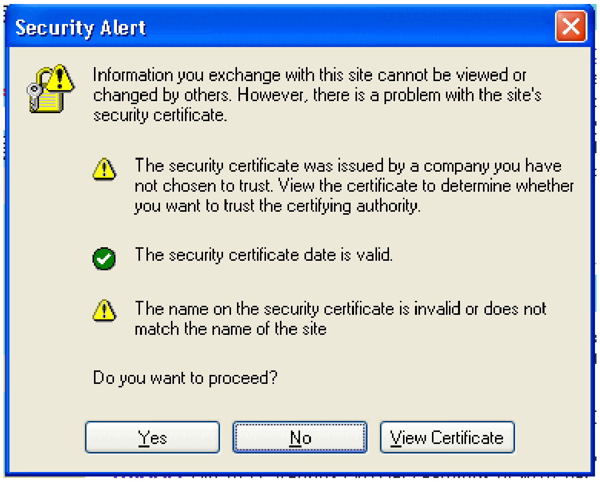
To obtain a certificate for a client, follow these steps.

1. Go to the following URL in a Web browser:

   `https://IPAddressOfServer/certsrv/`

   Where *`IPAddressOfServer`* is the IP address of your external RADIUS server, or of the *Certificate Authority* (CA), depending on the configuration of your infrastructure.

2. Click "Yes" to proceed to the secure Web page for the server.



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

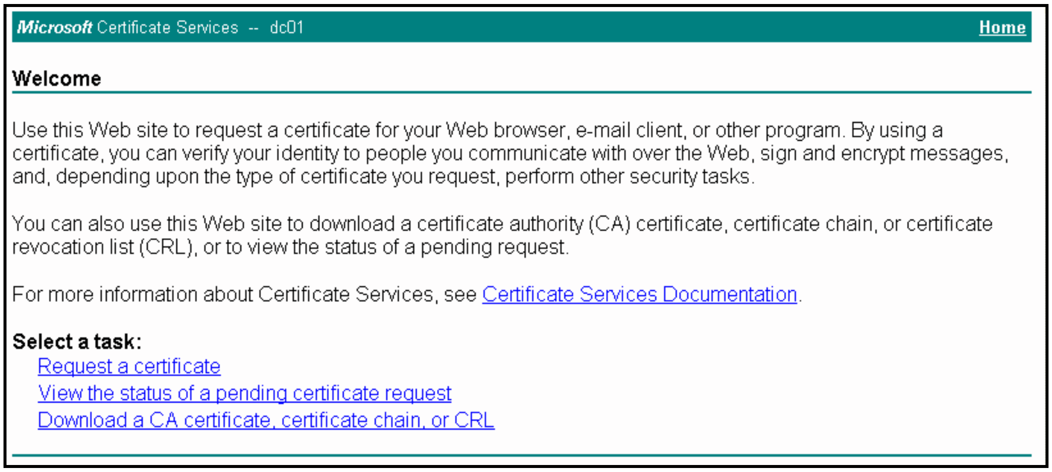
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ 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?

The Welcome screen for the Certificate Server is displayed in the browser.



Microsoft Certificate Services -- dc01 Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

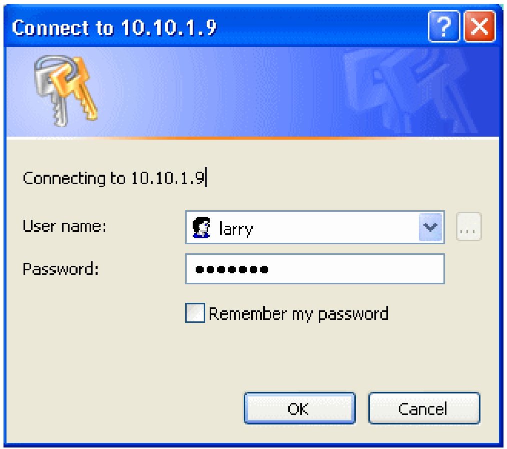
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Click "Request a certificate" to get the login prompt for the RADIUS server.

4. Provide a valid user name and password to access the RADIUS server.



Connect to 10.10.1.9

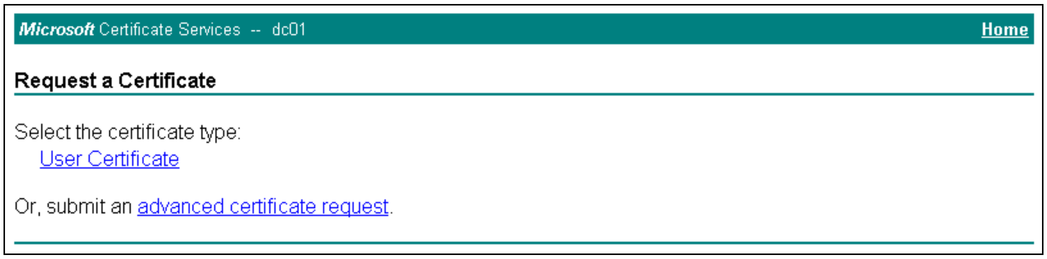
Connecting to 10.10.1.9

User name: larry

Password: ●●●●●●●

Note	The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.

5. Click "User Certificate" on the next page displayed.



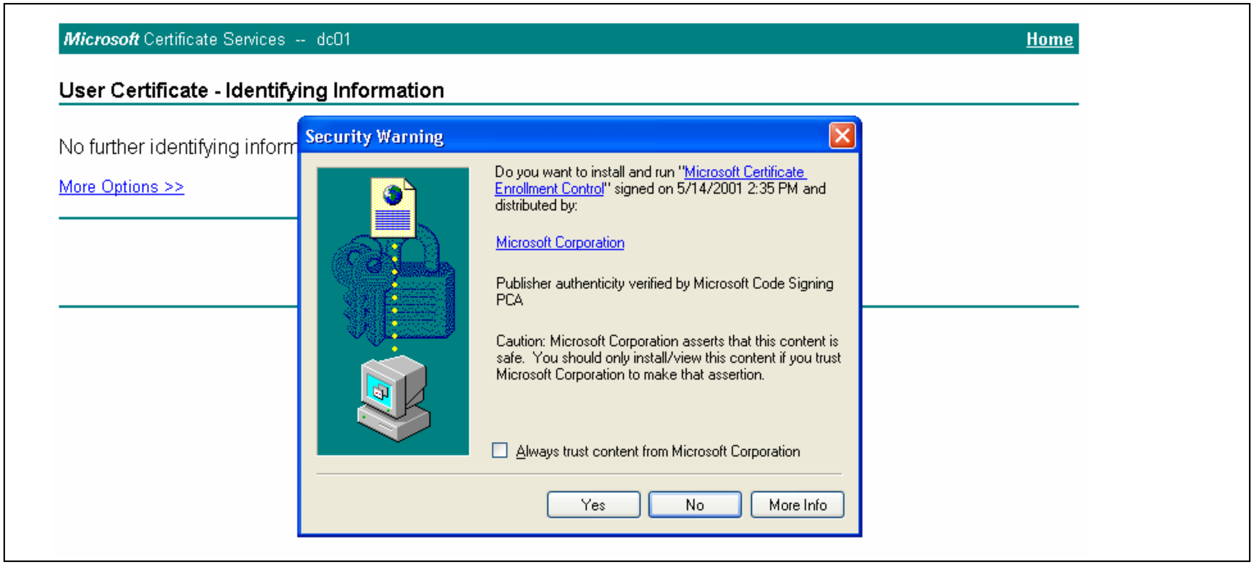
Microsoft Certificate Services -- dc01 Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

6. Click "Yes" on the dialog displayed to install the certificate.



Microsoft Certificate Services -- dc01 Home

User Certificate - Identifying Information

No further identifying inform

More Options >>

Security Warning

Do you want to install and run "Microsoft Certificate Enrollment Control" signed on 5/14/2001 2:35 PM and distributed by:

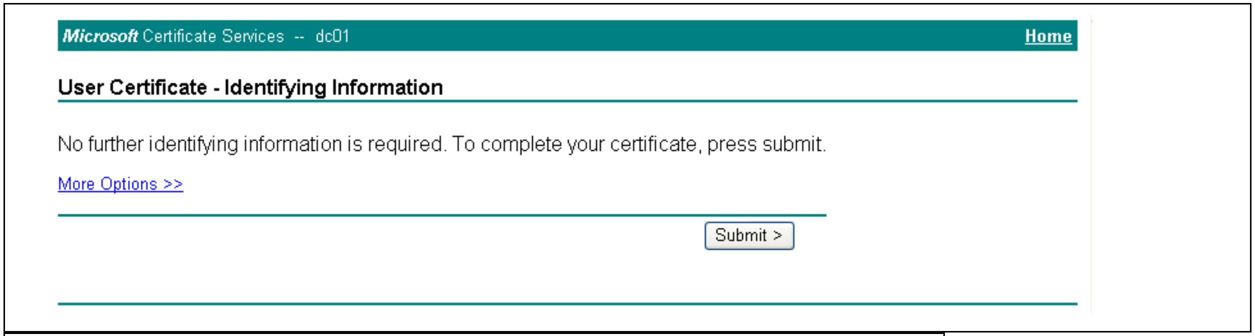
Microsoft Corporation

Publisher authenticity verified by Microsoft Code Signing PCA

Caution: Microsoft Corporation asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation to make that assertion.

□ Always trust content from Microsoft Corporation

7. Click "Submit" to complete and click "Yes" to confirm the submittal on the popup dialog.

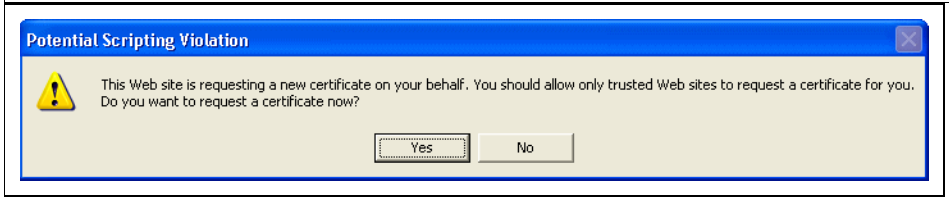


Microsoft Certificate Services -- dc01 Home

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.

More Options >>

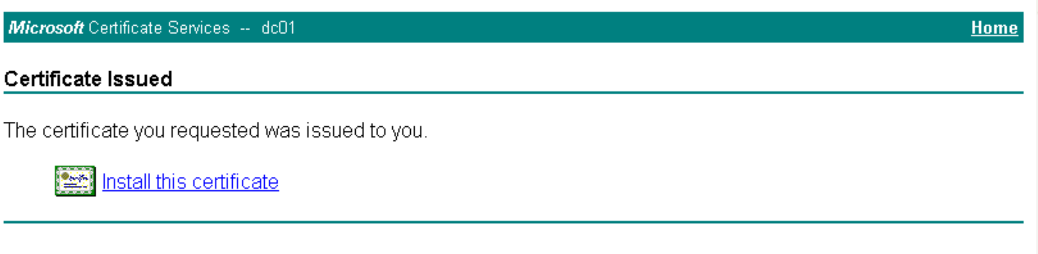


Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

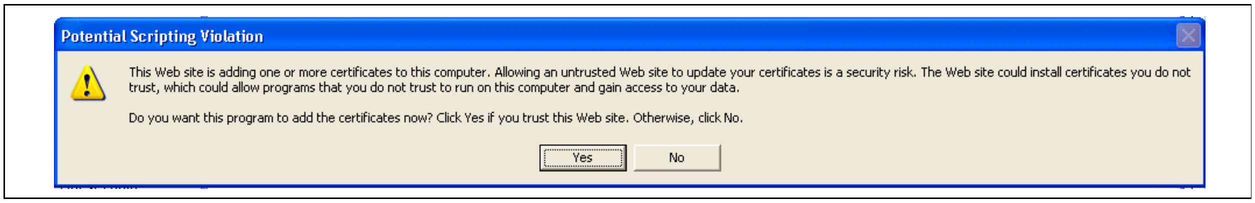
8. Click "Install this certificate" to install the newly issued certificate on your client station. (Also, click

"Yes" on the popup windows to confirm the install and to add the certificate to the Root Store.)



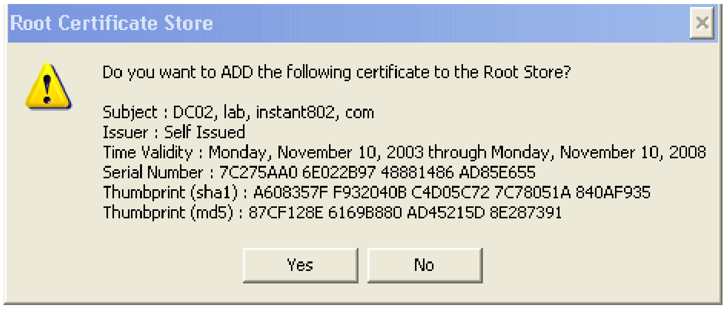
Certificate Issued

The certificate you requested was issued to you.



This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

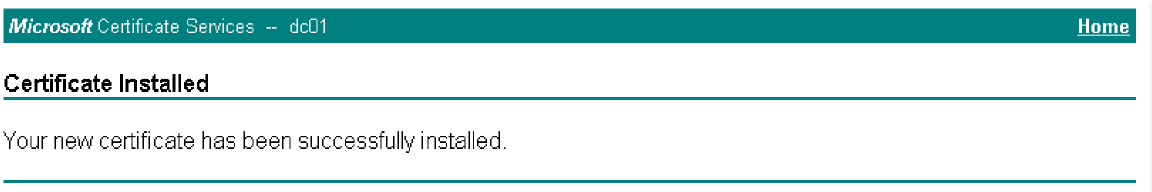
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.



Do you want to ADD the following certificate to the Root Store?

Subject : DC02, lab, instant802, com
Issuer : Self Issued
Time Validity : Monday, November 10, 2003 through Monday, November 10, 2008
Serial Number : 7C275AA0 6E022B97 48881486 AD85E655
Thumbprint (sha1) : A608357F F932040B C4D05C72 7C78051A 840AF935
Thumbprint (md5) : 87CF128E 6169B880 AD45215D 8E287391

A success message is displayed indicating the certificate is now installed on the client.



Certificate Installed

Your new certificate has been successfully installed.

Appendix B: Assessing Traffic and Interference

The Vivato AP/Bridge operates in the industrial, scientific, and medical (ISM) frequency band, which is used by a growing number of consumer and commercial devices. ANY device that creates a signal of sufficient power level within this frequency band will reduce data rate on one or more 802.11a/b/g channels.

To select the best channel to use in the intended deployment area, the channel assignments and sources of possible interference need to be understood.

ISM-Band Channel Spacing

The ISM band channels have a bandwidth of 22 MHz, but are only spaced 5 MHz apart. This means that transmissions on any channel can interfere with operation on a channel that is within four channel spacings (20 MHz) above or below that channel. As shown below, this leaves channels 1, 6, and 11 as the only channels that can be used at the same time with a minimum interference with each other.

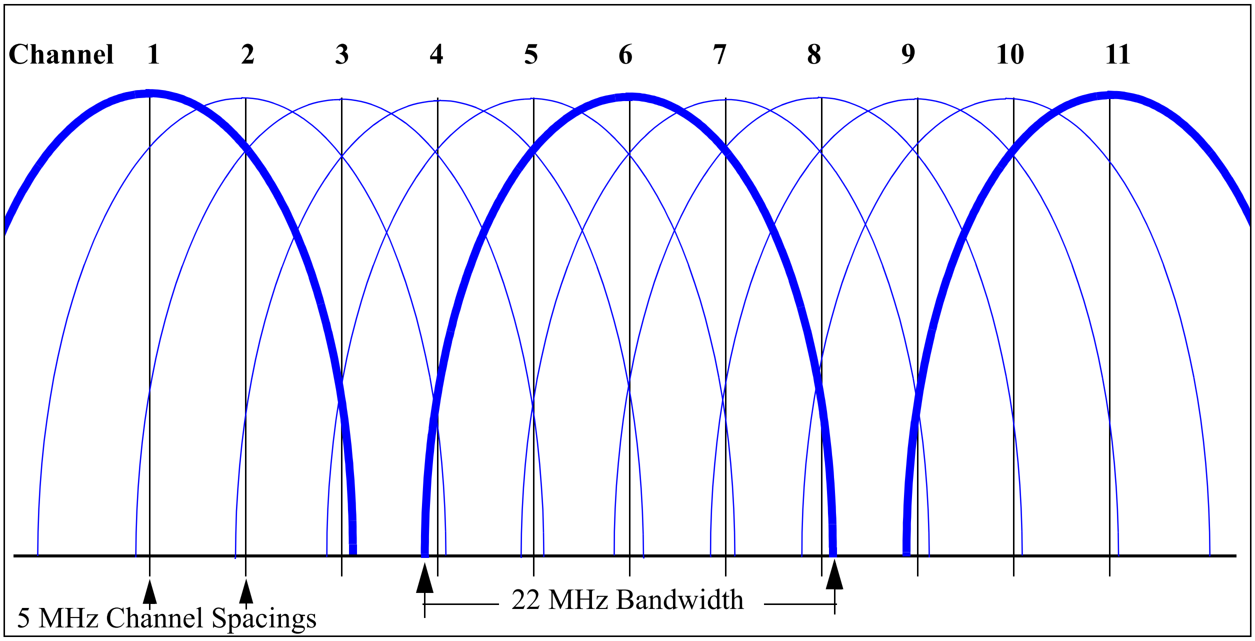


Figure 10—ISM Band Channel Spacings for Channels 1 to 11

Unfortunately, many devices are deployed using channels other than 1, 6, or 11. This means that they can interfere (and often do interfere) with 802.11 devices using these non-overlapping channels. For example, a wireless video link operating on channel 4 will interfere with 802.11 operation (and probably with the operation of any other wireless data communication systems) on channels 1 through 8! In return, other devices operating on those channels could also interfere with the video link.

Therefore, it is very important that channels for Wi-Fi operation are chosen carefully to prevent interference from other systems and to prevent creating interference for other systems.

Note: The following table lists channels that may be used in many countries. However, it is the responsibility of the person configuring the Vivato AP/Bridge or W-Fi Bridge/Router to configure the product in accordance with the laws governing the deployment location.

Table 3 802.11 ISM Band DSSS Channel Assignments

Channel Number	Center Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12 (N/A)	2.467
13 (N/A)	2.472
14 (N/A)	2.483
N/A = Not available in the Vivato AP/Bridge.	

Sources of Noise and Interference

Interfering signals can be broken down into four basic types: in-channel 802.11a/b/g signals, non-overlapping out-of-channel 802.11a/b/g signals, overlapping out-of-channel 802.11a/b/g signals, signals produced by non-802.11a/b/g devices.

Every 802.11a/b/g device measures the signal level on its assigned channel and compares it to one or more threshold levels before transmitting. If the received signal is high enough, the device does not transmit. This function is called clear channel assessment (CCA).

A channel sharing feature, carrier sense multiple access with collision avoidance (CSMA/CA), is intended to prevent signal collisions and data loss. If another 802.11a/b/g system is using the same channel, the AP/Bridge (and therefore the clients that it serves) must wait for a clear channel before sending data. Conversely, while the AP/Bridge or one of its clients is transmitting, the devices on the other 802.11a/b/g system should withhold transmission. This reduces the total packet rate through the AP/Bridge.

Due to the AP/Bridge's high antenna gain, the interfering signal may come from an access point (AP) or a client that is a large distance from the from the AP/Bridge. This makes it impossible to guarantee any level of service unless the channel assignments of all of the APs within the coverage area can be coordinated.

The carrier sense function also applies to non-802.11a/b/g signals. If ANY received signal is of sufficient level, the carrier sense function will still block Wi-Fi transmission on that channel.

In-Channel 802.11b Signals

As previously stated, other 802.11b devices on the same channel must use CSMA/CA to share the channel. The greater the number of packets sent by 802.11 devices sharing a channel, the lower the overall throughput at each device.

Most 802.11a/b/g devices use a single channel at one time and use the direct sequence spread spectrum (DSSS) method of sending data. However, some home RF devices use frequency hopping, using either overlapping or non-overlapping channels Frequency hopping interferes with Wi-Fi operation using DSSS.

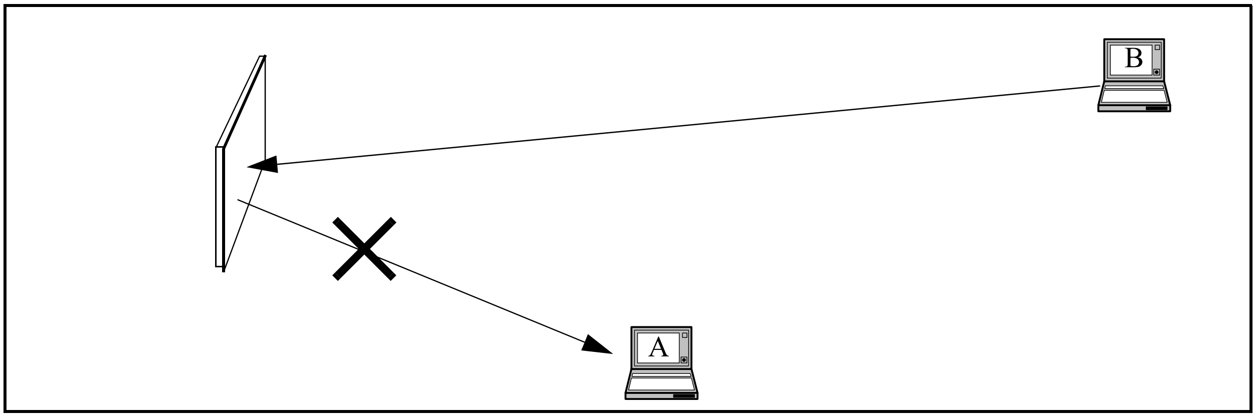
Frequency hopping jumps from channel to channel during operation. When non-overlapping 802.11b frequency hopping is used, channels 1, 6, and 11 will be occupied by these signals. The traffic to/from the AP/Bridge and its clients that are assigned to these channels has to take place between the periods where a channel is used during the hopping operation. When overlapping hopping is used, the channels being used will overlap with at least two of the three non-overlapping channels (1, 6, and 11); effectively limiting the AP/Bridge's operation to the one remaining non-overlapped channel and therefore limiting data throughput.

When one of these situations exists, you can do one or more of the following:

- Pick another RF channel to use that does not interfere with the other system(s).
- Change the other device's RF channel number. This may require working with the administrator or owner of the interfering system. However, agreeing to use separate channels benefits BOTH systems.
- Disable the other device.
- Relocate your AP/Bridge or tilt it down.

Multi-MAC Controller

Because the AP/Bridge has multiple wireless interfaces that can be assigned to the same channel(s), signals received from a client at one pointing direction may not be detected by the receiver for another pointing direction. In the example below, clients A and B are both associated with the AP/Bridge on the same channel, and client B is currently transmitting to the AP/Bridge. If the wireless interface associating with client A didn't detect the signal from client B and began transmitting to client A, it could cause errors in the signal received from client B.



The Vivato AP/Bridge has a multi-MAC controller function that coordinates traffic on multiple interfaces that are sharing the same channel. Anytime a client's signal is being received by the AP/Bridge, all other transmissions on that channel, including beacons, are held off until the client stops transmitting. This effectively coordinates the CSMA function for all AP/Bridge interfaces.

MMC is enabled on the AP/Bridge by default.

Out-of-Channel 802.11a/b/g Signals

Only three 802.11a/b/g channels do not overlap each other: 1, 6, and 11. All other channels overlap one of these channels to some degree. For example, if your AP/Bridge is set to use channel 1 on one or more wireless interfaces, a system transmitting on channel 3 would overlap its signals. The AP/Bridge's receiver sees the overlapping signal as noise. If the overlapping signal level is high enough, the resulting signal-to-noise ratio will be too low to demodulate the desired signal. In this case, the best thing to do is to change the channel of the other system to a non-overlapping channel; 6 or 11. The only alternative in this case is to set all of the AP/Bridge's wireless interfaces to channel 11 to prevent operation on channel 3 from interfering with the AP/Bridge's operation.

Signals on a non-overlapping channel minimizes interference with operation on other non-overlapping channels. However, if other 802.11a/b/g devices are already using all three non-overlapping channels in the desired coverage area, you have no alternative but to share those channels with the existing systems or work with the owners of those systems to restrict each system to specific non-overlapping channels.

Important ❗	Do not try to use an overlapping channel to try to "squeeze in" between the non-overlapping channels. The result will be interference on two of the non-overlapping channels and poor or no operation on the overlapping channel that you selected.

Non-802.11b Signals

Because the ISM band is used by non-licensed devices, many types of interfering signals can be present in the same RF spectrum used by 802.11a/b/g devices. Some of these devices occupy a single channel, while others may occupy several channels. Because these signals are not recognized as 802.11a/b/g signals, these signals are seen by 802.11a/b/g receivers as noise. As with out-of-band 802.11a/b/g signals, these signals can raise the level of noise high enough to reduce the SNR to unusable levels, disabling 802.11a/b/g operation on these channels.

Depending on the source of these signals, you may or may not be able to reduce their levels. If the level of an interfering signal cannot be reduced, you must select a channel where the interference is low enough to allow 802.11a/b/g operation over the desired coverage area.

Transient Interference

Microwave ovens use a magnetron to create microwave energy. During operation, the magnetron is only radiating during ½ of the 50 - 60 Hz AC power cycle. This means that the oven is sending out interference for 8 to 10 milliseconds (ms), then is off for 8 to 10ms, repeating this cycle whenever the oven is operating. Using the 802.11 CSMA function, clients and access points will either see a busy channel or an open (clear) channel, depending on whether the magnetron is currently transmitting. If it is transmitting, 802.11 transmissions are held off. If the magnetron is not transmitting, 802.11 transmissions will begin. Because the period of time in between microwave transmissions is long enough to send packets at higher data rates, the effect is similar to sharing the channel with other 802.11 devices. However, if the 802.11 signal level is very low, requiring the use of lower data rates, the period between transmissions may not allow complete 802.11 packet transmissions to occur before another microwave transmission begins; blocking the reception of any packets being transmitted.

Frequency hopping is also used by some non-802.11b communications systems as a security feature. If the hopping rate is too fast, the signal will interfere with 802.11b operation on one or more channels by “jumping” on the Wi-Fi signal during transmission.

Continuous Transmission Interference

2.4 GHz Cordless telephones, video surveillance and distribution systems, and point-to-point data communication links are common devices that may be operating nearby and interfere with Wi-Fi operation.

Determining if a Signal is Strong Enough to Affect Wi-Fi Operation

As previously stated, 802.11 operation requires the use of carrier sense multiple access (CSMA) protocol to prevent signal collisions and share the channel. The AP/Bridge uses an energy level detector and a carrier level detector to determine whether a channel is clear or busy. The detector threshold for both detectors can be changed simultaneously using the command line interface sensitivity <1-5> command.

Table 4 Energy Detect and Carrier Detect Thresholds for Each Sensitivity Setting

Sensitivity Setting	Energy Detect Threshold	Carrier Detect Threshold
1 (default for maximum range)	-85 dBm	-99 dBm
2	-85 dBm	-90 dBm
3	-75 dBm	-85 dBm
4	-62 dBm	-72 dBm
5 (use for minimum range)	-56 dBm	-66 dBm

Energy Level Detection

The energy level detector measures ANY signals at the assigned channel. If the measured level is high enough, the threshold is reached and the channel is determined to be busy. The highest energy detect sensitivity setting (1) is the default setting of approximately -85 dBm. This means that ANY signal detected on a channel that is greater than this level will prevent the AP/Bridge from transmitting on that channel. If the signal from clients is well above this level, the sensitivity can be reduced to prevent background signals from blocking Wi-Fi operation on that channel.

Carrier Level Detection

The carrier detect function looks for valid 802.11 packets on signals above a preset threshold. If valid packets are detected above the threshold, the channel is determined to be busy. At the highest sensitivity setting (1), the default carrier detect level is approximately -99 dBm. This means that a valid 802.11 packet detected on a channel that is greater than this level will prevent the AP/Bridge from transmitting on that channel. If the signals from the intended clients are well above this level, the sensitivity can be reduced to prevent weak signals from distant access points or other clients from blocking Wi-Fi operation on that channel.

Measuring Interfering Signal Levels

Two methods can be used to measure the level of noise and isolate its source: spectral analysis and the the Neighboring AP/Bridges feature.

Spectral analysis provides a visual presentation of the signal levels within the selected frequency range. This provides an easily read graphic display of the RF environment. However, this method requires a spectrum analyzer and a high gain directional antenna to perform the measurements. This method is explained in the Vivato Outdoor Wi-Fi System Deployment document on the Vivato Customer Support Knowledge Base.

Neighboring AP/Bridges is a feature in the Vivato AP/Bridge that displays the received signal level and channel number on each of the 6 pointing directions. Neighboring AP/Bridges can provide very useful results by letting you know which channels are being used, their signal strengths at the Wi- Fi AP/ Bridge, and the direction of the origin of these signals.

Using the Neighboring AP/Bridges Feature to Analyze Interfering Signals

The AP/Bridge's Neighboring AP/Bridges feature is used when the AP/Bridge is mounted at its proposed location to determine the best channel to use when automatic channel assignment is not used. By looking at the signal strength and channel number of local signals, you can make an initial determination about which channel will have the least known interference and set the channel accordingly.

Glossary

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11a

IEEE 802.11a operates in the 5 GHz ISM band of frequencies.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in kμsec) of a burst of data.

IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WME) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter AP/Bridge protocol (IAPP) for AP/Bridges (wireless hubs) in an extended service set (ESS). The standard defines how AP/Bridges communicate the associations and re-associating of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a developing IEEE standard for security in a wireless local area network (WLAN). It defines enhancements to the MAC Layer to counter the some of the weaknesses of WEP. 802.11i will incorporate 802.1x and stronger encryption techniques, such as Advanced Encryption Standard (AES).

IEEE 802.11i is still a draft IEEE standard (most recent version is D5.0, August 2003). A currently available subset of 802.11i is the Wi-Fi *Protected Access* (WPA) standard.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies. (See http://www.ieee802.org/1/pages/802.1Q.html.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

AP/Bridge

A AP/Bridge is the communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one AP/Bridge is connected to wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad hoc Mode

Ad hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the "heartbeat" of a WLAN, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.

- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.

- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.

- The *Service Set Identifier* (SSID).

- The Basic Rate Set is a bitmap that lists the rates that the WLAN supports.

- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).

- The optional *Traffic Indication Map* (TIM) identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the AP/Bridge sends data traffic in the form of IEEE 802.1x Frames to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Multicast.

Broadcast Address

See IP Address.

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single AP/ Bridge. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the AP/Bridge.

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server. It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

Client

A wireless *client* is any device that is equipped with an IEEE 802.11a, 802.11b, or 802.11g wireless interface that uses radio signals to connect to an 802.11 access point or base station in order to access hosts on a local network or a gateway that provides access to the Internet. Common examples of clients are laptop computers, personnel digital assistants (PDAs), and remote video cameras. Clients are also referred to as "*stations*".

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/ contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF). See also RTS and CTS.

The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an IEEE 802.11 client station in response to an *request to send* (RTS) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS.)

dB

"dB" is the abbreviation for decibel, which is a logarithmic unit of relative signal level. dB units are commonly used for describing gains or losses in radio frequency (RF) signal levels, rather than using linear values, because of their ease of use when calculating signal level changes. Using dB units, signal gains and losses are simply added or subtracted, rather than being multiplied or divided as they would for linear calculations. A common use of dB units is the signal-to-noise ratio (SNR) measurement that compares the level of the received signal relative to the noise level.

dBm

"dBm" is the abbreviation for decibel units relative to 1 milliwatt of power. A wireless card may transmit at 100 mW of RF power, which equates to 20 dBm. 0 dBm = 1 mW. Signals of <1 mW result in negative values; –3 dBm equates to 0.5 mW. dBm units are typically used to report the signal level of an associated client.

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server "offers" a "lease" (for a pre-configured period of time—see Lease Time) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, `www` is the host name of a Web server and `www.Vivato.net` is the fully-qualified name of that server. DNS translates the domain name `www.Vivato.net` to some IP address, for example `66.93.138.219`.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example `.de` for Germany, `.fr` for France, `.jp` for Japan, `.tw` for Taiwan, `.uk` for the United Kingdom, `.us` for the U.S.A., and so on. There are also `.com` for commercial bodies, `.edu` for educational institutions, `.net` for network operators, and `.org` for other organizations as well as `.gov` for the U. S. government and `.mil` for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the AP/Bridge awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See IP Address.

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple AP/Bridges, forming a single subnetwork that can support more clients than a basic service set (BSS). Each AP/Bridge supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as "*X*base*Y*", where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or "Yellow Cable"). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by IEEE 802.11g stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE 802.11g standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the AP/Bridge and enable *request to send* (RTS) and *clear to send* (CTS) protection before sending data.

See also CSMA/CA protocol.

Frame

A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head>` ... `</head>` section, which contains the metadata to define the document, and a `<body>` ... `</body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser via HTTP. Also see XML.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (`GET`, `HEAD`, `POST`, etc.), a request followed by a response.

IAPP

The *Inter AP/Bridge Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the AP/Bridges in a "distribution system". This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between AP/Bridges.

IBSS

An *independent basic service set* (IBSS) is an Ad hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11b, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.)

For more information about IEEE task groups and standards, see http://standards.ieee.org/.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an AP/Bridge. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The AP/Bridge is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single AP/Bridge (BSS) or a number of AP/Bridges (ESS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called IPv6 or IPng, is under development. IPv6 is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form `192.168.2.254`. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

- The Network Address consists of a host number that is all zeroes (for example, `192.168.2.0`).

- The Broadcast Address consists of a host number that is all ones (for example, `192.168.2.255`).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

`10.0.0.0` to `10.255.255.255`
`172.16.0.0` to `172.31.255.255`
`192.168.0.0` to `192.168.255.255`

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.

- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver. Latency can occur when data is transmitted from the AP/Bridge to a client and vice versa. It can also occur when data is transmitted from AP/Bridge to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example `FE:DC:BA:09:87:65`.

MDI and MDI-X

Medium Dependent Interface (MDI) and *MDI crossover* (MDIX) are twisted pair cabling technologies for Ethernet ports in hardware devices. Built-in twisted pair cabling and auto-sensing enable connection between like devices with the use of a standard Ethernet cable. (For example, if a wireless AP/Bridge supports MDI/MDIX, one can successfully connect a PC and that AP/Bridge with an Ethernet cable rather than having to use a crossover cable).

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an AP/Bridge or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the AP/Bridge sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Broadcast.

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See IP Address.

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.

- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.

- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.

- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.

- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).

- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.

- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects.

Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

PoE

Power Over Ethernet (PoE) provides the ability to power the AP/Bridge through an Ethernet connection using an IEEE 802.3af-compliant switch or other device, eliminating the need to have a power supply where the AP/Bridge is located.

Port Forwarding

Port Forwarding creates a ‘tunnel’ through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user’s point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (VPN) within the *Point-to-Point Protocol* (PPP). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task group. A subset of 802.11e features is described in the WME specification.

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an 802.1x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the AP/Bridge, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS Threshold and CTS.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the AP/Bridge, and is especially useful for performance tuning on a AP/Bridge with a many clients.

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See IP Address.

Station

See Client.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between AP/Bridges. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

STP

Shielded Twisted Pair (STP) is a type of copper conductor cable where each of the two copper wires that are twisted together are coated with a shield that functions as a ground for the wires. This shield protects the cable from electromagnetic interference that otherwise could get into or out of the cable.

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as `255.255.255.0`) or as a number appended to the IP address (for example, `192.168.2.0/24`).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is `192.168.2.128` and the netmask is `255.255.255.0`, the resulting Network address is `192.168.2.0`.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

IP address	192.168.2.128	11000000 10101000 00000010 10000000
Netmask	255.255.255.0	11111111 11111111 11111111 00000000
Resulting network address	192.168.2.0	11000000 10101000 00000010 00000000

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, UDP, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called "Michael"), and a re-keying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit Type *of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way "best-effort" settings depending upon the requirements of the data. The ToS field is used by the Vivato Wi-Fi AP/Bridge to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the VA4200 to client stations.

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the AP/Bridge sends data traffic in the form of IEEE 802.1x Frames directly to a single client station MAC address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Multicast and Broadcast.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.glasplanes.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.glasplanes.com/index.html` specifies a Web page that should be fetched using the HTTP protocol.

VLAN

A *virtual* LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The Vivato Wi-Fi AP/Bridge supports the configuration of a wireless VLAN. This technology is leveraged on the AP/Bridge for the "virtual" guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an AP/Bridge is connected to a wired LAN. WDS allows AP/Bridges to be connected wirelessly. The AP/Bridges can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and AP/Bridges on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations (clients) communicate directly with one another in an Ad hoc Mode network, also known as an independent basic service set (IBSS).

- Stations communicate through an AP/Bridge in an Infrastructure Mode network. A single AP/Bridge creates an infrastructure basic service set (BSS) whereas multiple AP/Bridges are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WME

Wireless Multimedia Enhancements (WME) is a subset of the 802.11e draft specification. It uses four priority queues between an AP/Bridge and its clients. WME provides an interim, standards-based QoS solution. WME is not supported on the AP/Bridge at this time.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.

A

access point
- monitoring 74

administrator
- platform 22

administrator password 72
- on Network > Basic Settings 40

antenna connectors 18

antenna polarization 33

AP/Bridge
- administrator password 72
- global network settings 42
- MAC filtering 57
- QoS 59
- radio 51
- security 91
- time protocol 49
- user management 45
- WDS bridging 66
- wireless settings 56

associated wireless clients 77

authentication
- in different security modes 92

authentication server
- for IEEE 802.1x security mode 102
- for WPA with RADIUS security mode 104

Auto VLAN Settings 89

B

backup links
- WDS 67

beacon interval
- configuring 52

bridges
- WDS 66

C

certificate
- obtaining TLS-EAP certificate for client 145
- security for IEEE 802.1x client 130
- security for WPA with RADIUS client 136

channel
- configuring 52

Channel Spacing 149

client
- platform 23
- security 120
- See also *stations* 52

connectors 18
Customer Support 13
customer support 13

D

DCF
- as related to QoS 61

default configuration, restore 19
default gateway 42
default settings
- defined 21
- resetting to 79

DHCP
- understanding in relation to self-managed VWBSs 25

DNS servers, specifying 43
documentation feedback 13
DTIM period
- configuring 52

E

EAP-PEAP
- configuring on IEEE 802.1x client 127
- configuring on WPA with RADIUS client 133

encryption in different security modes 92
event log 75
events
- monitoring 75

extended service set
- with WDS bridging 66

F

factory defaults
- described 21
- returning to 79

features
- overview 17

feedback, documentation 13
firmware
- upgrade 80

firmware upgrade 80
fragmentation threshold
- configuring 52

front panel indicators 18

G

gateway, default 42
global network settings 42

I

IEEE 802.11a
- configuring 52

IEEE 802.11a Turbo
- configuring 52

IEEE 802.11b
- configuring 52

IEEE 802.11g
- configuring 52

IEEE 802.1x radio mode
- configuring 52

IEEE 802.1x security mode
- client configuration 127
- configuring 102
- when to use 93

IEEE rate set
- configuring 52

Interference 149
interference, signal 33
interframe spaces
- as related to QoS 61

IP address, setting 44
IP addresses
- understanding policies for self-managed VWBSs 25

K

key management
- security 92

L

LED indicators 18
logging (syslog) 90, 112
logon
- administration Web pages 27

loops
- WDS 67

M

MAC filtering
- configuring 58

management interface, specifying 90
management password 72
manual feedback 13

N

neighboring access points 82
networking
- features overview 17

Noise, interfering 150
NTP server
- configuring AP/Bridge to use 50

O

obstructions, indoor 35, 36

P

packet bursting
- as related to QoS 62

password
- configuring administrator 72
- network setting for administrator 40
- on Network > Basic Settings 40

password recovery 114
PEAP
- configuring on IEEE 802.1x client 127
- configuring on WPA with RADIUS client 133

plain text security mode
- client configuration 124
- configuring 98
- when to use 92

platform
- administrator requirements 22
- client requirements 23

power connection 18

Q

quality of service 59
queueus
- configuring for QoS 63

R

radio
- configuring 52

Radio Settings 51

RADIUS server
- configuring to acknowledge AP/Bridges 142
- See also *authentication server*

recovery, password 114

remote logging 112

reset access point to factory defaults 79

restore factory configuration (Reset) 19

rogue access points 82

RTS threshold
- configuring 52

S

security
- authentication server 142
- certificates on client 145
- comparison of modes 92
- configuring on the access point 97
- configuring on wireless clients 120
- features overview 17
- IEEE 802.1x 102
- plain text 98
- pros and cons of different modes 91
- static WEP 98
- WEP 98
- WPA with RADIUS 104
- WPA-PSK 108

serial port 19

SNMP Network Management 110

spanning tree protocol (STP) 67

Spectrallink Voice Priority (SVP) 60

starting the network 41

static WEP security mode
- configuring 98
- on WDS bridge 68
- when to use 93

stations
- configuring maximum allowed 52
- See also *client*

Support Contacts 13

support contacts 13

support, customer 13

supported platforms
- administrator 22
- client 23

System Recovery 114

T

time
- configuring an AP/Bridge to use NTP server 50

TLS-EAP
- configuring on IEEE 802.1x client 130
- configuring on WPA with RADIUS client 136
- obtaining certificate for client 145

ToS
- as related to QoS 60

transmit power
- configuring 52

transmit/receive
- monitoring 76

transmit/receive information 76

U

upgrading the firmware 80

user accounts
- for built-in authentication server 45

user authentication
- configuring on IEEE 802.1x client 127
- configuring on WPA with RADIUS client 133

V

Voice over IP
- improved service with QoS 59

W

Warranty and End User License 3

WDS
- configuring 69
- example 70
- explanation 66
- rules 69

weight
- indoor switch 32

WEP security mode
- client configuration 125
- configuring 98
- when to use 93

wired
- settings 42

wireless
- overview of VWBS features 16

settings 56

WPA with RADIUS security mode

client configuration 133

configuring 104

when to use 94

WPA-PSK security mode

client configuration 140

configuring 108

when to use 96

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

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

Vivato, Inc. declares that VA4200 (FCC ID: QLNVA4200AP) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.