

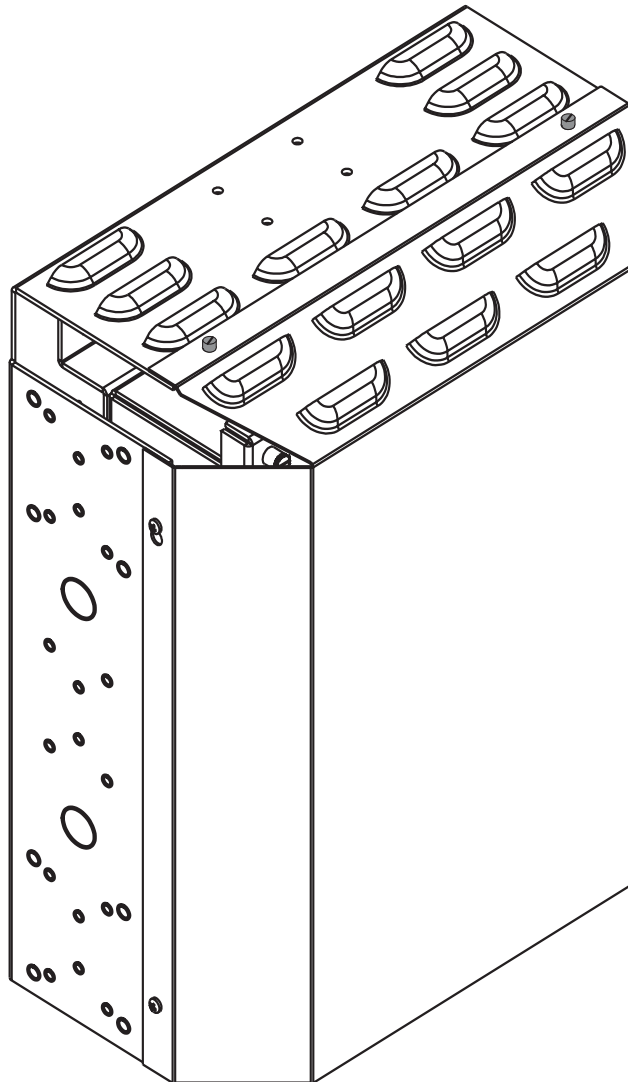


VA2410 802.11b/g Outdoor Microcell User Guide

Manual P/N: 770-01376-01

Release 3.0

August 29, 2005



Copyright © 2005, Vivato, Inc.

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

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

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 14.

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.....	15
User and Developer Audience	15
Online Help Features	15
Guidance on Configuring the Microcell with Recommended Settings	15
Typographical Conventions	16
Introduction.....	17
Overview of the Vivato 802.11b/g Outdoor Microcell.....	17
NEMA-4X Outdoor Enclosure	17
IEEE 802.11 ISM-Band Channel Operation.....	17
Basic Service Set Operation	18
Web Page Interface Configuration	18
Features and Benefits	18
Indicators and Connectors	20
VA2410 Abbreviated Specifications	20
Installation.....	22
Hardware Description	22
PreLaunch Checklist: Default Settings and Supported User/Client Platforms	24
Vivato 802.11b/g Outdoor Microcell	24
User's Computer.....	26
Wireless Client Computers	28
Quick Steps for Setup and Launch of Your Wireless Network	29
Step 1. Install the Microcell	29
Step 2. Set the PC's Network Interface to Talk to the Microcell	29
Step 3. Log in to the VivatoVision Web Pages	30
Step 4. Configure the Basic Settings	31
Step 5. Specify the IP Address and Security Settings for the Primary Wireless Network.....	32
Step 6. Configure the Default Gateway and DNS Nameserver IP Addresses	33
Next Steps	34
Configuring Basic Settings.....	35
Navigating to Basic Settings.....	35
Review Description of the Microcell	36
Specify a New User Password and the Wireless Network Name.....	37
Update Basic Settings	38
Global Network Settings	39
Navigating to Global Network Settings	39
Specifying the Default Gateway	39
Specifying the DNS Nameservers	40
Updating Settings	40
Setting Interface IP Addresses.....	41
Managing User Accounts	42
Navigating to User Management	43

Viewing User Accounts	43
Adding a User	43
Editing a User Account	44
Enabling and Disabling User Accounts	44
Removing a User Account	45
Enabling the Network Time Protocol Server	46
Navigating to Time Protocol Settings	46
Enabling or Disabling a Network Time Protocol (NTP) Server	47
Updating Settings	47
Configuring Radio Settings	48
Understanding Radio Settings	48
Navigating to Radio Settings	48
Configuring Radio Settings	49
Updating Settings	52
Viewing the Wireless Interface Settings	53
Navigating to Wireless Settings	53
Controlling Access by MAC Address Filtering	54
Navigating to MAC Filtering Settings	54
Using MAC Filtering	56
Updating Settings	56
Configuring Queues for Quality of Service (QoS)	57
Understanding QoS	57
Navigating to QoS Settings	60
Configuring QoS Queues	60
Updating Settings	62
Configuring the Wireless Distribution System (WDS)	63
Understanding the Wireless Distribution System	63
Navigating to WDS Settings	65
Configuring WDS Settings	67
Updating Settings	70
Setting the User Password	71
Navigating to Administrator Password Setting	71
Setting the User Password	71
Updating Settings	72
Maintenance and Monitoring	73
Interfaces	73
Event Log	74
Transmit/Receive Statistics	75
Associated Wireless Clients	76
Rebooting the Microcell	76
Resetting the Configuration	77
Upgrading the Firmware	78
Rogue Access Points	81
Creating and Managing Multiple Networks (SSIDs)	84
Using SSIDs with VLANs to Create Logically Separate Networks	84

Navigating to Current SSID Settings	85
Creating and Editing SSIDs	86
Updating Settings	87
Automatic VLAN Assignment	88
Configuring Security	89
Understanding Security Issues on Wireless Networks	89
Navigating to Security Settings	94
Configuring Security Settings	95
Updating Settings	108
Specifying the Management Interface(s)	109
Navigating to the Management Interfaces Settings	109
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
Mesh Network Operation	114
Mesh Operation and the Impact on Client Data Throughput	115
VLAN Operation Through Mesh Nodes	115
Rebooting After Changing Mesh Settings and After Firmware Upgrades	116
Configuring Mesh Operation	116
Navigating to Global Mesh Settings	116
Updating Settings	118
Navigating to Wireless Interface Mesh Settings	119
Updating Settings	120
Navigating to the Mesh Status Screen	121
System Recovery	122
Appendix A. Configuring Security Settings on Wireless Clients	124
Make Sure the Wireless Client Software is Up-to-Date	125
Accessing the Microsoft Windows Wireless Client Security Settings	126
Configuring a Client to Access an Unsecure Network (Plain Text mode)	128
Configuring Static WEP Security on a Client	129
Configuring IEEE 802.1x Security on a Client	131
Configuring WPA with RADIUS Security on a Client	137
Configuring WPA-PSK Security on a Client	144
Configuring an External RADIUS Server to Recognize the Vivato 802.11b/g Outdoor Microcell	146
Obtaining a TLS-EAP Certificate for a Client	149
.....	152
Appendix B: Assessing Traffic and Interference	153
ISM-Band Channel Spacing	153
Sources of Noise and Interference	154

Measuring Interfering Signal Levels 156

Glossary 158

Safety Information

You must heed any and all safety precautions and warnings in this document or indicated on the Vivato VA2410 802.11b/g Outdoor Microcell 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: VA2410 802.11b/g Outdoor Microcell
This product is certified for home or office use.

The Vivato VA2410 802.11b/g Outdoor Microcell has been evaluated under FCC Bulletin OET 65C and found to be compliant to the requirements set forth in CFR 47 15.247 (i) addressing RF Exposure from radio frequency devices. The Microcell 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 Microcell 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 802.11b/g Outdoor Microcell on a wireless network.

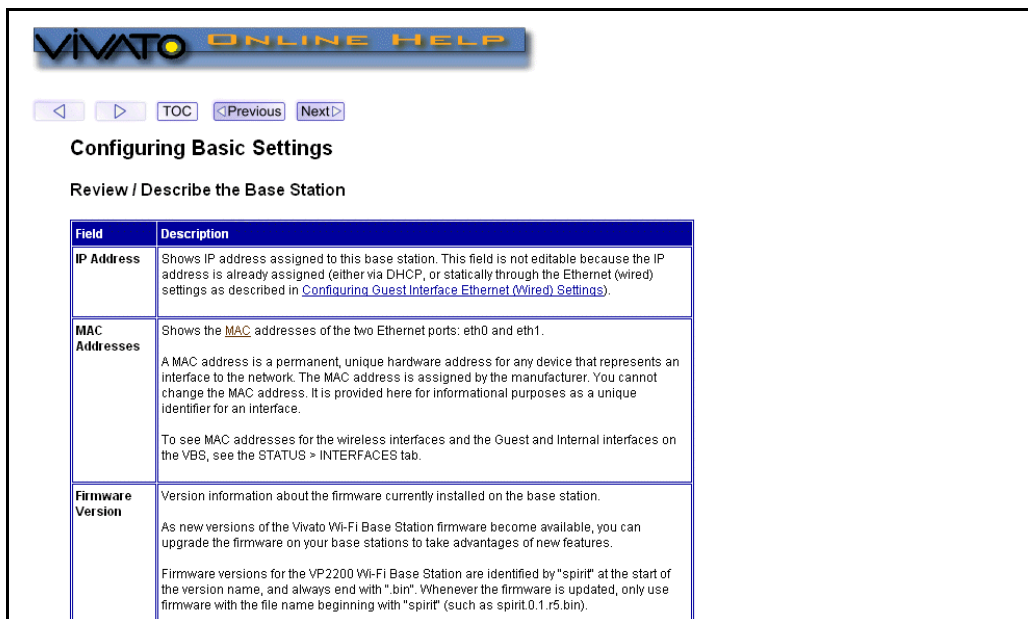
User and Developer Audience

This information is intended for the person responsible for installing, configuring, monitoring, and maintaining the Vivato 802.11b/g Outdoor Microcell.

Online Help Features

Online Help for the Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell 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.



VIVATO ONLINE HELP

Navigation: < Previous TOC Next >

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 Microcell 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 Microcell.

Typographical Conventions

This guide uses the following typographical conventions:

Microcell	Unless otherwise specified, refers to the Vivato 802.11b/g Outdoor Microcell.
<i>italics</i>	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
<i>typewriter font italics</i>	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 802.11b/g Outdoor Microcell

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

The Vivato 802.11b/g Outdoor Microcell 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 Microcell?

Inside the Microcell is a Wi-Fi radio system and a central microprocessor that coordinates all activities. The Microcell contains two wireless interfaces. Each interface supports 802.11b and 802.11g operation.

As new features and enhancements become available, you can upgrade the firmware to add new functions and performance improvements to the Microcells that make up your wireless network. (See “Upgrading the Firmware” on page 78.)

NEMA-4X Outdoor Enclosure

The VA2410 consists of a Vivato AP/Bridge enclosed in a weather tight housing, providing protection from moisture, dirt, and insects. A thermostatically controlled heater is used to maintain the proper internal temperature during times of cooler temperatures. Shielding panels are used to reduce solar heating of the electrical enclosure to prevent over heating and to provide attachment points for mounting the VA2410 and user-supplied antennas. See the *VA2210/2410 Installation Supplement* for details and installation information.

IEEE 802.11 ISM-Band Channel Operation

The VA2410 can communicate on any two channels in the IEEE channel set (although the default channel assignment of 1 and 11 should be used for best results). Both channels can operate at the maximum data rate of up to 54 Mbps. The Microcell can be configured to communicate with clients and with a Vivato Wi-Fi Base Station (using a Wireless Distribution System (WDS) connection).

Multi-Microcell Operation for Extended Coverage

The VA2410 contains one 10/100 Base-T Ethernet port and two wireless interfaces. Multiple VA2410's can be connected using a wired or a wireless connection to extend Wi-Fi coverage and provide maximum deployment flexibility.

Basic Service Set Operation

The VA2410 supports infrastructure basic service set (BSS) operation, providing all network communications between Wi-Fi clients and the wired network within the area of coverage.

Web Page Interface Configuration

An easy to use VivatoVision™ web interface is used to configure all settings in the VA2410 Microcell.

Features and Benefits

IEEE Standards Support

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

Wireless Features

- Allows simultaneous 802.11b and 802.11g operation using two separately configurable wireless interfaces.
- Transmit power adjustment (see “Configuring Radio Settings” on page 48).
- Wireless Distribution System (WDS) for connecting multiple Microcells 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 Microcell.
- 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

Simple Network Management Protocol (SNMP) Support

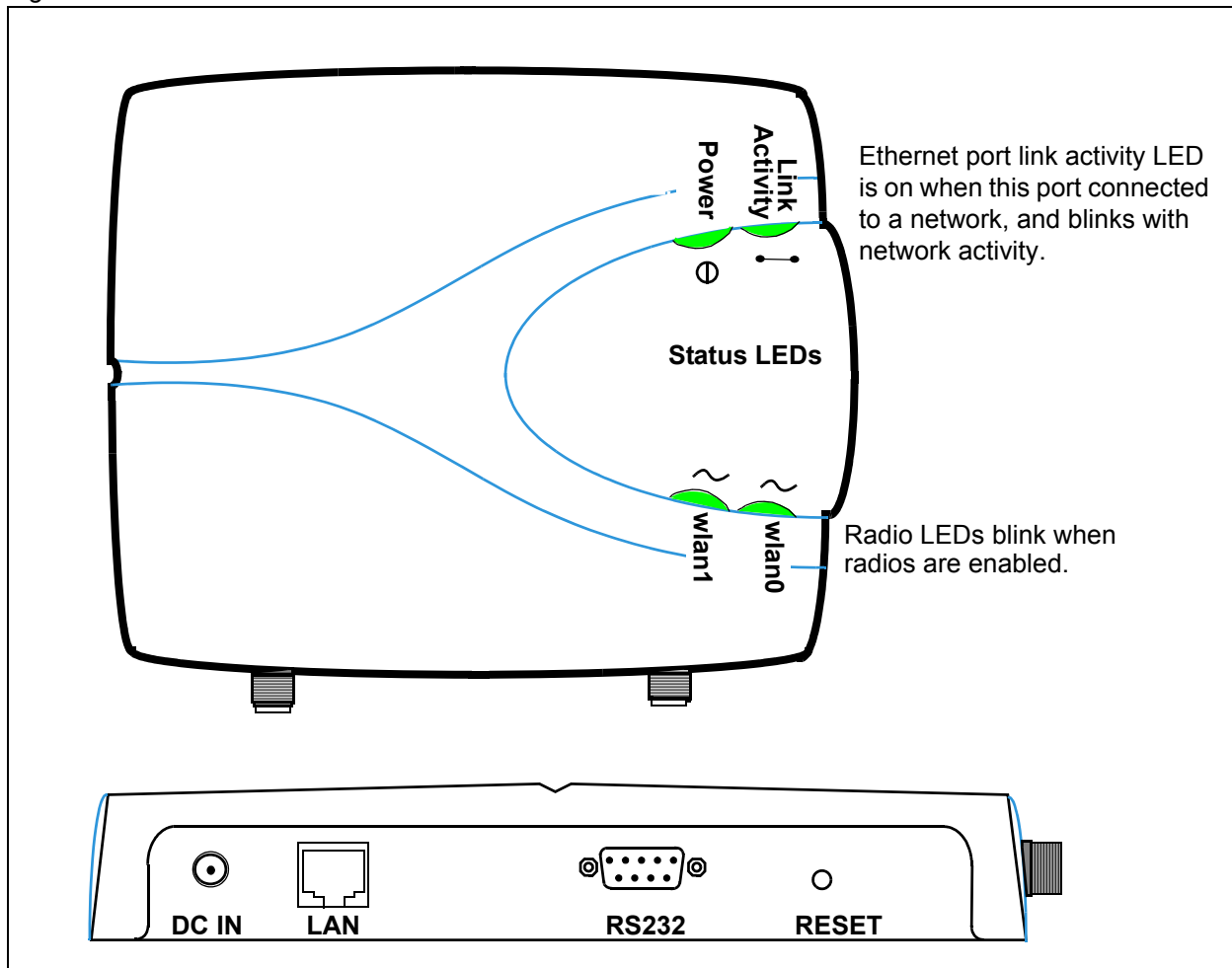
- Support for versions 1 and 2c.
- Management Information Base (MIBs) provided to monitor and manage Microcell operation.
- Traps can be set to alert the system administrator to specific conditions.

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

Figure 1 Internal Indicators and Connections



- **DC IN:** DC power from the pre-installed AC/DC power adapter.
- **LAN:** 10/100 Ethernet, RJ-45.
- **RS232:** Serial port for access to the Linux operating system (shell).
- **RESET:** Pressing and holding the **RESET** button in for at least four seconds re-configures the Microcell to use the factory default settings and deletes the previous configuration file.

VA2410 Abbreviated Specifications

The following are abbreviated specifications for the Vivato 802.11b/g Outdoor Microcell, and are subject to change without notice. Refer to the latest product data sheet for the most accurate and complete information:

- **Size:** 16.77" (43 cm) wide X 8.63" (22 cm) deep X 20.17" (51 cm) high
- **Weight:** ~32 lbs. (14.5 kg)

- **Installer Connections:**
 - Internal: One RJ-45 jack for a 10/100 Ethernet connection; one DB-9 (m) serial connector; AC power connections. Cables must be routed through chassis knockouts for 1" conduit. Refer to the *VA2210/2410 Installation Supplement* for details on powering the VA2410.
 - External: Two RP-TNC (f) jacks for antenna connections.
- **Power Requirements:**
 - Input Voltage: 100 – 120 VAC, 50/60 Hz
 - Current: 1.2 Amps
- **Operating temperature range:** -40 to 131F (-40 to 55C)
- **Transmit/Receive Frequency Range:** 2.412 to 2.462 GHz
- **Wi-Fi Operating Distance:** Dependant on antenna configuration.
- **Operates license-free under FCC Part 15 and complies as a Class B computing device.**
- **Complies with DOC regulations.**
- **Serial Port Communication Settings:**

The following settings must be used when communicating through the serial port:

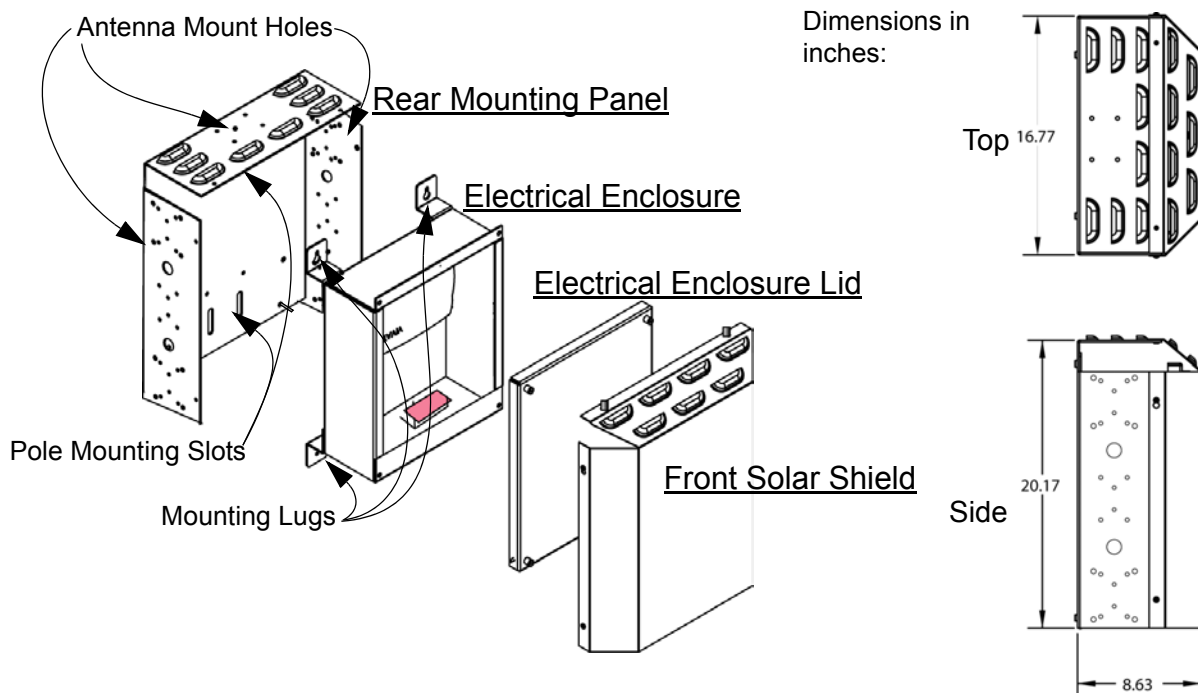
- Baud: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Installation

Hardware Description

NOTE: Refer to the printed *VA2210/2410 802.11 Outdoor Microcell Installation Supplement* included with the Microcell for instructions on how to mount and provide power and data connections to the VA2410.

The VA2410 consists of a Vivato Wi-Fi Microcell enclosed in a NEMA-4X rated case. The case provides protection from moisture, dirt, insects, and other foreign matter, and also provides temperature controls to operate in an extended temperature range.



Power Connections and Requirements

Refer to the product label next to the antenna ports on the underside of the electrical enclosure for the power requirements of this product.

Warning



Power to the VA2410 must be supplied through a 15 ampere circuit breaker in order to provide a power disconnect for servicing the VA2410 and to prevent fire or electrical shock if damage or electrical failure occurs.

The installer is solely responsible for understanding and following all applicable building and electrical codes regarding the installation of this device.

AC Surge Suppression

AC power surge suppression is not included with the VA2410, and must be provided by the installer in order to protect the product from damaging AC power surges. Damage to the VA2410 due to power surges is not covered by the product warranty.

It is the installer's responsibility to determine the proper level of surge protection required at the place where the VA2410 is to be installed. For example, high levels of induced voltage spikes caused by large electric motors or arc welding apparatus on the same power grid require the use of the highest levels of surge protection in order to prevent damage to the VA2410.

PreLaunch Checklist: Default Settings and Supported User/Client Platforms

Before you power-up a new Microcell, 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 802.11b/g Outdoor Microcell
 - › Default Settings for the Vivato 802.11b/g Outdoor Microcell
 - › What the Microcell Does Not Provide
- User's Computer
- Wireless Client Computers

Vivato 802.11b/g Outdoor Microcell

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

The Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell

Option	Default Settings	Related Information
System Name	VA2410	
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 37 in "Configuring Basic Settings" on page 35 "Setting the User Password" on page 71.
Network Name (SSID)	"Internal Vivato Network"	"Review Description of the Microcell" on page 36 in "Configuring Basic Settings" on page 35
Network Time Protocol (NTP)	None	"Enabling the Network Time Protocol Server" on page 46
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.	For information on setting the IP address, see Table 2 "SSID Configuration Settings" on page 86
Subnet Mask	255.255.0.0	
Radios	On	"Configuring Radio Settings" on page 48
IEEE 802.11 Mode	802.11b/g	"Configuring Radio Settings" on page 48
Radio Channel	- Radio 0: Channel 1 (b/g mode) - Radio 1: Channel 11 (b/g mode)	"Configuring Radio Settings" on page 48
Beacon Interval	500 milliseconds	"Configuring Radio Settings" on page 48
DTIM Period	2 beacons	"Configuring Radio Settings" on page 48
Fragmentation Threshold	2346 bytes	"Configuring Radio Settings" on page 48
Regulatory Domain	FCC	This is read-only. It cannot be modified.
RTS Threshold	2347 bytes	"Configuring Radio Settings" on page 48
MAX Stations	2007	"Configuring Radio Settings" on page 48

Option	Default Settings	Related Information
Transmit Power	100 percent	"Configuring Radio Settings" on page 48
Supported Rates (Mbps)	IEEE 802.11b/g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1	"Configuring Radio Settings" on page 48
Basic Rate (Mbps)	IEEE 802.11b/g: 11.0, 5.5, 2.0, 1.0	"Configuring Radio Settings" on page 48
Broadcast SSID	Allow	See "Does Prohibiting the Broadcast SSID Enhance Security?" on page 94 in "Configuring Security" on page 89
Security Mode	None (plain text)	See "Plain-text" on page 96 in "Configuring Security" on page 89
Authentication Type	None	
MAC Filtering	Allow any station unless in list	"Controlling Access by MAC Address Filtering" on page 54
WDS Settings	None	"Configuring the Wireless Distribution System (WDS)" on page 63

What the Microcell Does Not Provide

The Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell is accomplished by connecting to the Microcell 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 Microcell	The computer used to configure the Microcell must be connected to the Microcell (either directly or through a hub) by an Ethernet cable. Refer to "Indicators and Connectors" on page 20.

Required Software or Component	Description
Wireless Connection to the Network	After initial configuration and launch of the first Microcell 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 Microcell, 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 Microcell. (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 802.11b/g Outdoor Microcell. For more details on Wi-Fi client setup, see "Wireless Client Computers" on page 28.
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 802.11b/g Outdoor Microcell is provided through a Web-based user interface hosted on the Microcell. We recommend using one of the following supported Web browsers to access the Microcell 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 • Mozilla Firefox 1.06 • Safari (MAC OS X, version 10.3 or later) 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 Microcell.

Wireless Client Computers

The Vivato 802.11b/g Outdoor Microcell provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the Microcell 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 Microcell, 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 Microcell. (IEEE 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 VA2410 Microcell supports 802.11b/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 Microcell(s) is configured.
Wireless Client Software	Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the Vivato 802.11b/g Outdoor Microcell.
Client Security Settings	Security should be disabled on the client used to do initial configuration of the Microcell. If the Security mode on the Microcell is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the Microcell 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 Microcell, see "Configuring Security" on page 89.

Quick Steps for Setup and Launch of Your Wireless Network

Setting up and deploying one or more Vivato 802.11b/g Outdoor Microcells 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 802.11b/g Outdoor Microcell and the resulting wireless network.

The following topics are discussed:

- Step 1. Install the Microcell
- Step 2. Set the PC's Network Interface to Talk to the Microcell
- 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 Microcell

Installation instructions are provided in the *VA2210/2410 802.11 Outdoor Microcell Installation Supplement* provided in the shipping container. Use the instructions in that document to install the product. See also "Installation" on page 22.

Step 2. Set the PC's Network Interface to Talk to the Microcell

The IP address of your computer's network interface must be within the same IP address range as the default IP address of the Microcell in order for the two devices to communicate with each other. If your PC's operating system supports automatic IP addressing¹ (Microsoft® Windows® 2000 or XP), it can automatically get an IP address that will allow your computer to communicate with the Microcell.

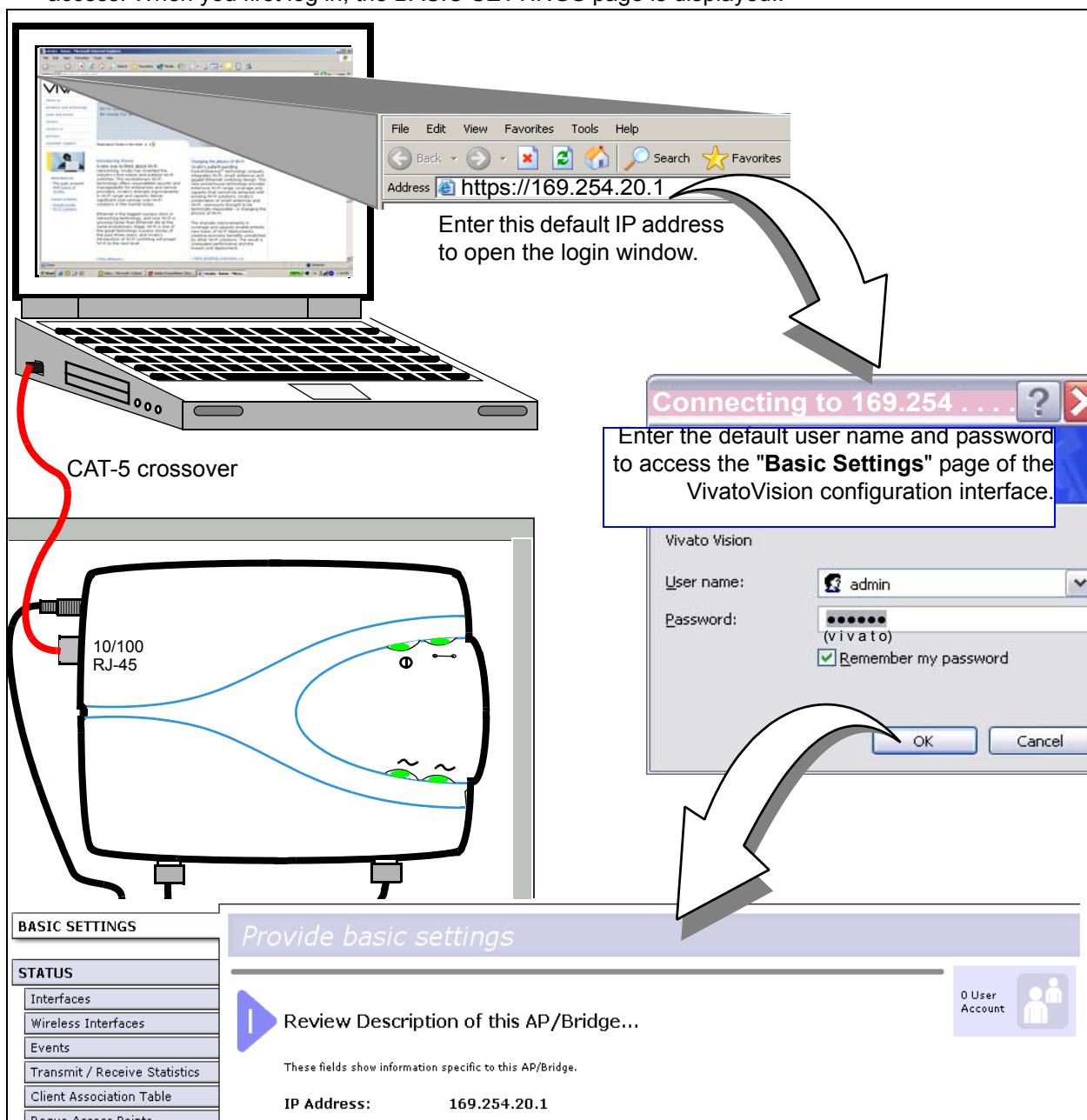
1. With your PC's Ethernet network interface card (NIC) configured for automatic IP addressing, and no other network interfaces on the PC connected to the network, turn the PC off for several seconds and then turn it back on.
2. Wait one minute after your computer has completed its reboot. Your computer's network interface(s) will automatically be assigned an IP address in the range that will allow it to access the Microcell.

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. Connect the Microcell to the PC's NIC through a CAT-5 RJ-45 cable. If connecting directly to the Microcell, use a CAT-5 crossover cable. If connecting through a network device (hub, switch, router) use a standard CAT-5 cable.
2. Power on the Microcell and wait at least 30 seconds for it to fully initialize.
3. Open a web browser on the PC and enter the default IP address of the Microcell for the address/location (<https://169.254.20.1>) as shown below. A login screen is then displayed. Be sure to enter "https", not just "http".
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 Microcell to avoid unauthorized access. When you first log in, the BASIC SETTINGS page is displayed..



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.

BASIC SETTINGS

Provide basic settings

1 Review Description of this AP/Bridge...

These fields show information specific to this AP/Bridge.

IP Address: 169.254.20.1
MAC Address (eth0): 00:0B:33:1B:C9:00
Firmware Version: va2400.3.0.a2
Location:

2 Provide Network Settings ...

These settings apply to this AP/Bridge.

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

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

3 Settings ...

Click "update" to save the new settings.

STATUS

- Interfaces
- Wireless Interfaces
- Events
- Transmit / Receive Statistics
- Client Association Table
- Rogue Access Points
- SSID Table
- Mesh Status

INTERFACE MANAGEMENT

- Global Network Settings
- Interface Network Settings
- Wireless Configuration (Radio)
- SSID Configuration
- Wireless Distribution System
- Auto VLAN Settings
- Management Interfaces
- Mesh Interfaces

TRAFFIC MANAGEMENT

- MAC Filtering
- Quality of Service

SYSTEM MANAGEMENT

- User Management
- Password Management
- SNMP
- Time Protocol

Review Description of this Microcell:

- › **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 Microcell firmware.
- › **Location:** Enter a name that identifies where this Microcell 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 will see in their list of available networks.

Settings:

- › Select the "Update" button to start using these settings and enter the changes into the Microcell'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 35.

Default Configuration

If you follow the steps above and accept all the defaults, the Microcell will have the default configuration described in “Default Settings” on page 25.

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

The IP address of the Microcell can be configured statically or dynamically to work on your wired network. Static addressing is recommended in order to always have a known IP address that can be used to access the VivatoVision configuration interface. 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 Microcell and on the clients.

1. Select the **INTERFACE MANAGEMENT>Interface Network Settings** tab.
2. For the **Interface** setting, select the “Primary Wireless Network Name” that you entered on the Basic Settings screen.

BASIC SETTINGS

STATUS

- Interfaces
- Wireless Interfaces
- Events
- Transmit / Receive Statistics
- Client Association Table
- Rogue Access Points
- SSID Table
- Mesh Status

INTERFACE MANAGEMENT

- Global Network Settings
- 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

Update

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 Microcell will request an IP address from your DHCP server when it is connected to your network.
4. Select **Update** to save your settings. If you selected to use DHCP, the IP address of the Microcell 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.

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

View list of configured SSIDs

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

SSID Configuration

SSID Name: Internal Vivato Network

Radio Interfaces: ☒ Radio 0 ☒ Radio 1

Backhaul Interface: Available Interfaces: Bound Interfaces: eth0

VLAN:

TX Retry Threshold:

TX Retry Timeout:

Beacon: ☐ Yes ☐ No

Broadcast SSID: ☒ Enabled ☐ Disabled

DTIM Period:

Security Mode: Open

Radius MAC Filtering: ☐

NAS IP Address: . . .

NAS Identifier:

Primary Radius:

Radius IP: . . .

Radius Key:

Radius Key Confirmation:

☐ Enable radius accounting

Secondary Radius:

Radius IP: . . .

Radius Key:

Radius Key Confirmation:

☐ Enable radius accounting

[Update](#)

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 89 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 Microcell 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.

BASIC SETTINGS	<i>Modify Global Network Settings</i>	
STATUS		
Interfaces		
Wireless Interfaces		
Events		
Transmit / Receive Statistics		
Client Association Table		
Rogue Access Points		
SSID Table		
Mesh Status		
INTERFACE MANAGEMENT		
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. See "Global Network Settings" on page 39.

Select **Update** to save these settings.

Next Steps

1. Connect the Microcell directly to your wired network.
2. Connect to the Microcell 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 if you selected "Open" for the security mode.
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 28 for information on requirements for these clients.

4. After the wireless network is up and you have tested the Microcell 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.

Configuring Basic Settings

The basic configuration tasks are described in the following sections:

- Navigating to Basic Settings
- Review Description of the Microcell
- Specify a New User Password and the Wireless Network Name
- Update Basic Settings
- At initial startup, no security is in place on the Microcell. An important next step is to configure security, as described in “Configuring Security” on page 90.

Navigating to Basic Settings

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

BASIC SETTINGS

Provide basic settings

1 Review Description of this AP/Bridge...

These fields show information specific to this AP/Bridge.

IP Address: 169.254.20.1
 MAC Address (eth0): 00:0B:33:1B:C9:00
 Firmware Version: va2400.3.0.a2
 Location:

2 Provide Network Settings ...

These settings apply to this AP/Bridge.

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

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

3 Settings ...

Click "update" to save the new settings.

0 User Account

STATUS

- Interfaces
- Wireless Interfaces
- Events
- Transmit / Receive Statistics
- Client Association Table
- Rogue Access Points
- SSID Table
- Mesh Status

INTERFACE MANAGEMENT

- Global Network Settings
- Interface Network Settings
- Wireless Configuration (Radio)
- SSID Configuration
- Wireless Distribution System
- Auto VLAN Settings
- Management Interfaces
- Mesh Interfaces

TRAFFIC MANAGEMENT

- MAC Filtering
- Quality of Service

SYSTEM MANAGEMENT

- User Management
- Password Management
- SNMP
- Time Protocol

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 Description of the Microcell


Review Description of this AP/Bridge...

These fields show information specific to this AP/Bridge.

IP Address: 169.254.20.1

MAC Address (eth0): 00:0B:33:1B:C9:00

Firmware Version: va2400.3.0.a3

Location

Field	Description
IP Address	Shows IP address assigned to this Microcell. The address is not editable here, but can be changed on the Interface Network Settings screen. See “Setting Interface IP Addresses” on page 41.
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 VA2410, see the STATUS > Interfaces tab.
Firmware Version	Version information about the firmware currently installed on the Microcell. As new versions of the Vivato 802.11b/g Outdoor Microcell firmware become available, you can upgrade the firmware on your Microcells to take advantages of new features. Firmware versions for the VA2410 Microcell are identified by "va2400" 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 "VA2400" (such as VA2400.3.0.bin). For instructions on how to upgrade the firmware, see “Upgrading the Firmware” on page 78.
Location	Specify a location description for this Microcell 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

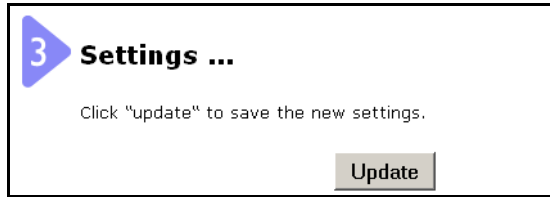
Administrator Password (again for safety)

Primary Wireless Network Name (SSID)

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 for safety)	Re-enter the new administrator password to confirm that you typed it as intended.
Primary Wireless Network Name (SSID)	Enter a name for the wireless network. This name will typically be used for all Microcells on this network. The <i>Service Set Identifier</i> (SSID) is an alphanumeric character string of up to 32 characters. Note: If you are connected as a wireless client to the same VA2410 that you are administering, resetting the SSID will cause you to lose connectivity to the VA2410. You will need to reconnect to the new SSID after you save this new setting.

Note	The Vivato 802.11b/g Outdoor Microcell is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple Microcells, 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



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

At initial startup, no security is in place on the Microcell. An important next step is to configure security, as described in “Configuring Security” on page 89.

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 Microcell, navigate to the **INTERFACE MANAGEMENT > Global Network Settings** tab, and update the fields as described below.

BASIC SETTINGS	Modify Global Network Settings	
STATUS		
Interfaces	Default Gateway Dynamic ☐ Manual ☒ . . . DNS Nameservers Dynamic ☐ Manual ☒ Search Domain vivato.net Update	
Wireless Interfaces		
Events		
Transmit / Receive Statistics		
Client Association Table		
Rogue Access Points		
SSID Table		
Mesh Status		
INTERFACE MANAGEMENT		
Global Network Settings		

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 Microcell 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 Microcell 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 VA2410 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 interface. By default, a wireless network called "Internal Vivato Network" is configured on the VA2410 with an IP address of 169.254.20.1.

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

BASIC SETTINGS	<i>Modify interface network settings</i>	
STATUS		
Interfaces		
Wireless Interfaces		
Events		
Transmit / Receive Statistics		
Client Association Table		
Rogue Access Points		
SSID Table		
Mesh Status		
INTERFACE MANAGEMENT		
Global Network Settings		
Interface Network Settings		
Interface: Internal Vivato Network		
☒ Static IP ☐ DHCP		
Static IP Address: 192 . 168 . 0 . 194		
Subnet Mask: 255 . 255 . 255 . 0		
Update		

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 802.11b/g Outdoor Microcell 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 100 in Configuring Security)
- WPA with RADIUS mode (see “WPA with RADIUS” on page 102 in Configuring Security)

You have the option of using either the internal RADIUS server embedded in the Vivato 802.11b/g Outdoor Microcell or an external RADIUS server that you provide. If you use the embedded RADIUS server, use this VivatoVision Web page on the Microcell 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 Microcells to access local and possibly external networks via your wireless network.

Note	Users specified here are clients of the Microcell 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]	amanda	(null)	disabled
☐	[Edit]	oneil	(null)	disabled

Selected users: [Enable](#) [Disable](#) [Remove](#)

Add a user...

To add a user, fill in the fields below and click "add account".

User Name ✓

Real Name ✓

Password ✓

Password (again for safety) ✓

[Cancel](#) [Add Account](#)

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 44.)

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 Microcell 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 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. 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

Selected users:

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 Microcell.

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 Microcells 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 Microcells 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 802.11b/g Outdoor Microcell 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.

The screenshot displays the web interface for configuring the Time Protocol. On the left is a navigation menu with categories: BASIC SETTINGS, STATUS, INTERFACE MANAGEMENT, TRAFFIC MANAGEMENT, and SYSTEM MANAGEMENT. The 'Time Protocol' option is selected under SYSTEM MANAGEMENT. The main content area has a title 'Modify how the AP/Bridge discovers the time'. It features a toggle for 'Network Time Protocol (NTP)' with 'Enabled' and 'Disabled' radio buttons; 'Disabled' is selected. Below this is a text field for 'NTP Server' and an 'Update' button.

BASIC SETTINGS	Modify how the AP/Bridge discovers the time Network Time Protocol (NTP) ☐ Enabled ☒ Disabled NTP Server Update
STATUS	
Interfaces	
Wireless Interfaces	
Events	
Transmit / Receive Statistics	
Client Association Table	
Rogue Access Points	
SSID Table	
Mesh Status	
INTERFACE MANAGEMENT	
Global Network Settings	
Interface Network Settings	
Wireless Configuration (Radio)	
SSID Configuration	
Wireless Distribution System	
Auto VLAN Settings	
Management Interfaces	
Mesh Interfaces	
TRAFFIC MANAGEMENT	
MAC Filtering	
Quality of Service	
SYSTEM MANAGEMENT	
User Management	
Password Management	
SNMP	
Time Protocol	

Enabling or Disabling a Network Time Protocol (NTP) Server

To configure your Microcell 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 Microcell.)

Field	Description
Network Time Protocol	NTP provides a way for the Microcell to obtain and maintain its time from a server on the network. Using an NTP server gives your VA2410 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 (such as time-nw.nist.gov) or by 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 802.11b/g Outdoor Microcell:

- 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 Microcell. 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 48 and 'Configuring Radio Settings' on page 49.

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

BASIC SETTINGS		Modify wireless settings																						
STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status		Radio Interfaces: ☒ Radio 0 ☒ Radio 1 Select All																						
INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces		Radio Mode: IEEE 802.11b Select Radio Mode IEEE 802.11b IEEE 802.11b/g																						
TRAFFIC MANAGEMENT MAC Filtering Quality of Service		Radio Interface: ☒ Enable ☐ Disable																						
SYSTEM MANAGEMENT User Management Password Management SNMP Time Protocol System Logging Mesh Upgrade Firmware Reset Configuration		☒ 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 Preamble type																						
		☒ Use Current Settings																						
		Max Stations:																						
		☒ Use Current Settings																						
		Power Level:																						
		☒ Use Current Settings																						
		Beacon Interval:																						
		☒ Use Current Settings																						
		Regulatory Domain: FCC																						
		☒ Use Current Settings																						
		Rate Sets:																						
		<table border="1"> <thead> <tr> <th>Rate</th> <th>Supported</th> <th>Basic</th> </tr> </thead> <tbody> <tr> <td>11 Mbps</td> <td>☒</td> <td>☐</td> </tr> <tr> <td>5.5 Mbps</td> <td>☒</td> <td>☐</td> </tr> <tr> <td>2 Mbps</td> <td>☒</td> <td>☒</td> </tr> <tr> <td>1 Mbps</td> <td>☒</td> <td>☒</td> </tr> <tr> <td>Set</td> <td></td> <td></td> </tr> <tr> <td>All Mbps: All</td> <td>☐</td> <td>☐</td> </tr> </tbody> </table>		Rate	Supported	Basic	11 Mbps	☒	☐	5.5 Mbps	☒	☐	2 Mbps	☒	☒	1 Mbps	☒	☒	Set			All Mbps: All	☐	☐
Rate	Supported	Basic																						
11 Mbps	☒	☐																						
5.5 Mbps	☒	☐																						
2 Mbps	☒	☒																						
1 Mbps	☒	☒																						
Set																								
All Mbps: All	☐	☐																						
		Update																						

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 802.11b/g Outdoor Microcell contains two radios. Select the checkbox next to the radio(s) to be configured, or select "All" to configure all radios at once.
Radio Mode	The <i>Mode</i> defines the <i>Physical Layer</i> (PHY) standard being used by the radio. To only allow 802.11g clients to associate with the Microcell 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 52.

Field (Continued)	Description (Continued)
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 Microcell uses channel 6 on all radios. When "Auto" is selected, the Microcell analyzes signals in the area and sets the channel to the one anticipated to provide the best coverage.
Fragmentation Threshold	Specify an even number between 256 and 2,346 to set the frame size threshold in bytes. The <i>fragmentation threshold</i> 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 <i>improve</i> 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.

Field (Continued)	Description (Continued)
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 Microcell, 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 Microcell.
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 Microcell at any one time. You can enter a value between 0 and 2007.
Power Level	Provide a percentage value to set the transmit power for this Microcell. The default is to have the Microcell transmit using 100 percent of its power. This power level is the maximum level that complies with FCC regulations.  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 Microcell a maximum broadcast range, and reduces the number of VA2410s 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 Microcell's signal on other 802.11 devices in that specific area.
Beacon Interval	Beacon frames are transmitted by a Microcell 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 2 per second). The <i>Beacon Interval</i> value is set in milliseconds. Enter a value from 20 to 2000.
Regulatory Domain	This value is read-only and cannot be changed.

Field (Continued)	Description (Continued)
Rate Sets	Check the transmission rate sets you want the Microcell to support and the basic rate sets you want the Microcell to use when setting up communications. Rates are expressed in megabits per second. • Supported Rate Sets indicate rates that the Microcell 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 Microcell will automatically choose the most efficient rate based on factors like error rates and signal strength. • Basic Rate Sets indicate rates that the Microcell advertises to the network for the purposes of setting up communication with other VA2410s 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 Microcell and their current configuration.

Selecting "Configure" for any of the wireless interfaces displays the Radio screen. See "Configuring Radio Settings" on page 48 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 Microcell, select the **STATUS > Wireless Interfaces** tab.

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management	<i>View wireless settings</i> <table border="0"> <tr> <td data-bbox="459 850 544 1071" rowspan="10">Radio 0 Enabled (Configure)</td> <td data-bbox="560 850 974 871">Radio Mode:</td> <td data-bbox="990 850 1417 871">IEEE 802.11b/g</td> </tr> <tr> <td data-bbox="560 877 974 898">CTS Protection:</td> <td data-bbox="990 877 1417 898">Auto</td> </tr> <tr> <td data-bbox="560 905 974 926">Channel:</td> <td data-bbox="990 905 1417 926">1</td> </tr> <tr> <td data-bbox="560 932 974 953">Beacon Interval:</td> <td data-bbox="990 932 1417 953">500</td> </tr> <tr> <td data-bbox="560 959 974 980">Fragmentation Threshold:</td> <td data-bbox="990 959 1417 980">2346</td> </tr> <tr> <td data-bbox="560 987 974 1008">RTS/CTS Threshold:</td> <td data-bbox="990 987 1417 1008">2347</td> </tr> <tr> <td data-bbox="560 1014 974 1035">ICCF:</td> <td data-bbox="990 1014 1417 1035">Disable</td> </tr> <tr> <td data-bbox="560 1041 974 1062">Short Preamble:</td> <td data-bbox="990 1041 1417 1062">Enable</td> </tr> <tr> <td data-bbox="560 1068 974 1089">Power Level:</td> <td data-bbox="990 1068 1417 1089">100</td> </tr> <tr> <td data-bbox="560 1096 974 1117">Regulatory Domain:</td> <td data-bbox="990 1096 1417 1117">FCC</td> </tr> <tr> <td data-bbox="560 1123 974 1144">Supported Rate Set (Mbps):</td> <td data-bbox="990 1123 1417 1186">54.0, 48.0, 36.0, 24.0, 18.0, 12.0, 11.0, 9.0, 6.0, 5.5, 2.0, 1.0</td> </tr> <tr> <td data-bbox="560 1192 974 1213">Basic Rate Set (Mbps):</td> <td data-bbox="990 1192 1417 1213">11.0, 5.5, 2.0, 1.0</td> </tr> <tr> <td data-bbox="459 1402 544 1476" rowspan="10">Radio 1 Enabled (Configure)</td> <td data-bbox="560 1260 974 1281">Radio Mode:</td> <td data-bbox="990 1260 1417 1281">IEEE 802.11b/g</td> </tr> <tr> <td data-bbox="560 1287 974 1308">CTS Protection:</td> <td data-bbox="990 1287 1417 1308">Auto</td> </tr> <tr> <td data-bbox="560 1314 974 1335">Channel:</td> <td data-bbox="990 1314 1417 1335">11</td> </tr> <tr> <td data-bbox="560 1341 974 1362">Beacon Interval:</td> <td data-bbox="990 1341 1417 1362">500</td> </tr> <tr> <td data-bbox="560 1369 974 1390">Fragmentation Threshold:</td> <td data-bbox="990 1369 1417 1390">2346</td> </tr> <tr> <td data-bbox="560 1396 974 1417">RTS/CTS Threshold:</td> <td data-bbox="990 1396 1417 1417">2347</td> </tr> <tr> <td data-bbox="560 1423 974 1444">ICCF:</td> <td data-bbox="990 1423 1417 1444">Disable</td> </tr> <tr> <td data-bbox="560 1451 974 1472">Short Preamble:</td> <td data-bbox="990 1451 1417 1472">Enable</td> </tr> <tr> <td data-bbox="560 1478 974 1499">Power Level:</td> <td data-bbox="990 1478 1417 1499">100</td> </tr> <tr> <td data-bbox="560 1505 974 1526">Regulatory Domain:</td> <td data-bbox="990 1505 1417 1526">FCC</td> </tr> <tr> <td data-bbox="560 1533 974 1554">Supported Rate Set (Mbps):</td> <td data-bbox="990 1533 1417 1596">54.0, 48.0, 36.0, 24.0, 18.0, 12.0, 11.0, 9.0, 6.0, 5.5, 2.0, 1.0</td> </tr> <tr> <td data-bbox="560 1602 974 1623">Basic Rate Set (Mbps):</td> <td data-bbox="990 1602 1417 1623">11.0, 5.5, 2.0, 1.0</td> </tr> </table>	Radio 0 Enabled (Configure)	Radio Mode:	IEEE 802.11b/g	CTS Protection:	Auto	Channel:	1	Beacon Interval:	500	Fragmentation Threshold:	2346	RTS/CTS Threshold:	2347	ICCF:	Disable	Short Preamble:	Enable	Power Level:	100	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	Radio 1 Enabled (Configure)	Radio Mode:	IEEE 802.11b/g	CTS Protection:	Auto	Channel:	11	Beacon Interval:	500	Fragmentation Threshold:	2346	RTS/CTS Threshold:	2347	ICCF:	Disable	Short Preamble:	Enable	Power Level:	100	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
Radio 0 Enabled (Configure)	Radio Mode:		IEEE 802.11b/g																																																
	CTS Protection:		Auto																																																
	Channel:		1																																																
	Beacon Interval:		500																																																
	Fragmentation Threshold:		2346																																																
	RTS/CTS Threshold:		2347																																																
	ICCF:		Disable																																																
	Short Preamble:		Enable																																																
	Power Level:		100																																																
	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																																																		
Radio 1 Enabled (Configure)	Radio Mode:	IEEE 802.11b/g																																																	
	CTS Protection:	Auto																																																	
	Channel:	11																																																	
	Beacon Interval:	500																																																	
	Fragmentation Threshold:	2346																																																	
	RTS/CTS Threshold:	2347																																																	
	ICCF:	Disable																																																	
	Short Preamble:	Enable																																																	
	Power Level:	100																																																	
	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 00: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.

MAC filtering can also be used in conjunction with RADIUS authentication when IEEE 802.1x or WPA with RADIUS security is used. In this case, MAC filtering is applied before a client's RADIUS authentication requests is passed to the RADIUS server. If the requesting client is allowed to associate based on its MAC address, its RADIUS request is passed through. If the client is denied association based on its MAC address, its RADIUS request is not passed on to the RADIUS server. See "Configuring Security" on page 89 for information about RADIUS-based security configuration.

The following sections describe how to use MAC address filtering on the Vivato 802.11b/g Outdoor Microcell:

- 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.

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

Mesh Status

INTERFACE MANAGEMENT

Global Network Settings

Interface Network Settings

Wireless Configuration (Radio)

SSID Configuration

Wireless Distribution System

Auto VLAN Settings

Management Interfaces

Mesh Interfaces

TRAFFIC MANAGEMENT

MAC Filtering

Configure MAC Filtering of client stations

Filter

☒ Allow only stations in list

☐ Allow any station unless in list

Stations List

00:0B:33:06:05:7A

Remove

:::::

Add

Update

Using MAC Filtering

This page allows you to control access to Vivato 802.11b/g Outdoor Microcell 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 VA2410 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 802.11b/g Outdoor Microcell.

The following sections describe how to configure Quality of Service queues on the Vivato 802.11b/g Outdoor Microcell:

- Understanding QoS
 - › 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.

QoS Queues and Parameters to Coordinate Traffic Flow

Configuring QoS options on the Vivato 802.11b/g Outdoor Microcell 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 Microcell always prioritizes packets identified with the SpectraLink Radio Protocol type in the IPv4 header for SpectraLink® Voice Priority (SVP) operation.

The Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell 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 Microcell examines the ToS field in the headers of all packets that pass through the VA2410. Based on the value in a packet's ToS field, the VA2410 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 (reserved)

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

Note	Wireless traffic travels: • Downstream from the Microcell to the client station • Upstream from client station to Microcell • Upstream from Microcell to network • Downstream from network to Microcell QoS settings on the Vivato 802.11b/g Outdoor Microcell affect only the first of these; <i>downstream</i> traffic flowing from the Microcell to client station. The other phases of the traffic flow are not under control of the QoS settings on the VA2410.
-------------	---

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.

The Vivato 802.11b/g Outdoor Microcell supports the *Distribution Coordination Function* (DCF). 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* (DIFS) before transmitting.

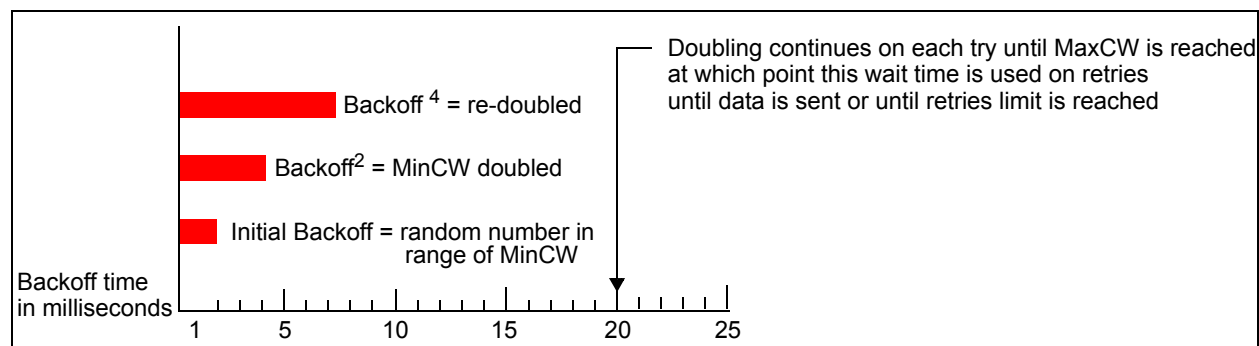
This parameter is configurable.

(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 Microcells 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 Microcell 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 Microcell 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 VA2410s 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.



The random backoff used by the Microcell 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 Microcell 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.

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.

BASIC SETTINGS	<i>Modify QoS queue parameters</i>				
STATUS					
Interfaces					
Wireless Interfaces					
Events					
Transmit / Receive Statistics					
Client Association Table					
Rogue Access Points					
SSID Table					
Mesh Status					
INTERFACE MANAGEMENT					
Global Network Settings					
Interface Network Settings					
Wireless Configuration (Radio)					
SSID Configuration					
Wireless Distribution System					
Auto VLAN Settings					
Management Interfaces					
Mesh Interfaces					
TRAFFIC MANAGEMENT					
MAC Filtering					
Quality of Service					

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

Update

Configuring QoS Queues

Configuring Quality of Service (QoS) on the Vivato 802.11b/g Outdoor Microcell 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 Microcell 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 VA2410-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 (reserved) For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 57.
Inter-Frame Space	The Interframe Space specifies a wait time (in milliseconds) for <i>data frames</i>. For more information, see “DCF Control of Data Frames and Interframe Spaces” on page 58.

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 <i>Minimum Contention Window</i> 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 59.
Max. Contention Window	The value specified here in the <i>Maximum Contention Window</i> 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 59.
Max. Burst Length	This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A <i>packet burst</i> is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

Updating Settings

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

Configuring the Wireless Distribution System (WDS)

The Vivato 802.11b/g Outdoor Microcell lets you connect multiple Microcells and base stations together using a Wireless Distribution System (WDS). WDS allows Microcells and base stations 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 802.11b/g Outdoor Microcell:

- 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

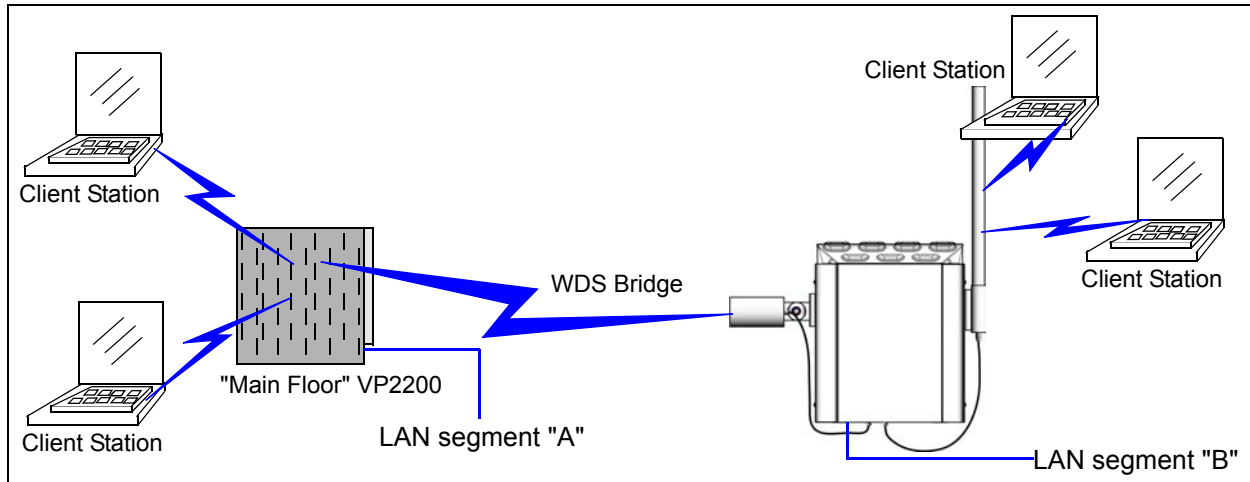
A *Wireless Distribution System* (WDS) connects Microcells, known as Basic Service Sets (BSS), to form what is known as an *Extended Service Set* (ESS).

Note	A BSS generally equates to a Microcell (deployed as a single-VA2410 wireless "network"), except in cases where multi-BSSID features make a single Microcell look like two or more Microcells to the network. In such cases, the Microcell has multiple unique BSSIDs.
-------------	---

Using WDS to Bridge Distant Wired LANs

In an ESS, each Microcell or base station 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 base station that is connected to LAN segment "A" by Ethernet and is serving multiple client stations on the main floor of a building, and a Microcell that is connected to LAN segment "B" and is serving stations in conference area behind the main floor. You can bridge the base station and the Microcell using a WDS link between

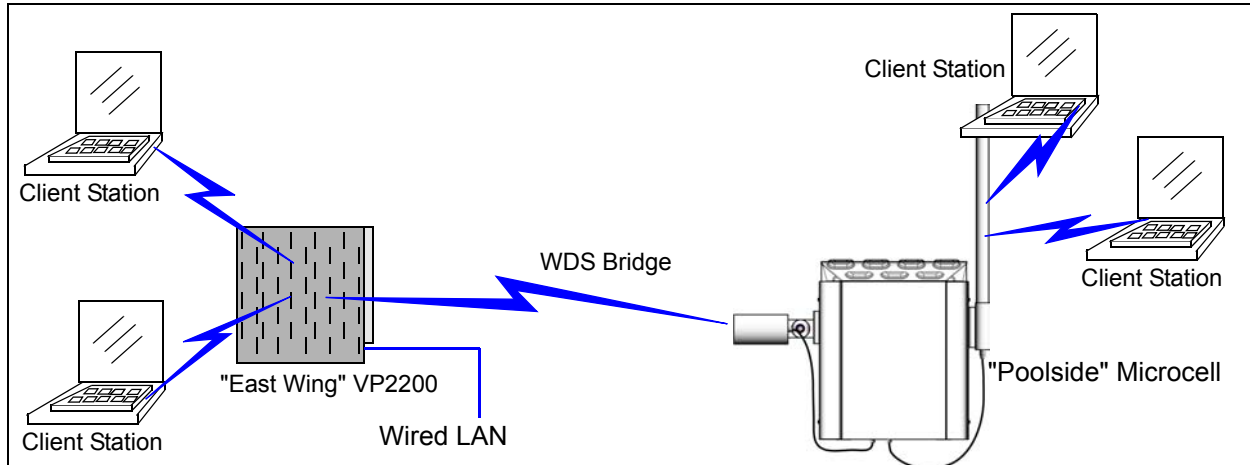
them to create a single network in both areas.



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 base station 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 a Microcell closer to second group of stations ("Poolside" in our example) and bridge the two products 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 VA2410. 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 VA2410 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 67.

Security Considerations Related to WDS Bridges

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both devices in a 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 Microcells 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 only recommend using WDS to bridge non-sensitive traffic for this release. Do not use WDS to bridge Microcells 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 89. This topic also covers use of plain text security mode for VA2410-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 Microcell to others, navigate to the **INTERFACE MANAGEMENT > Wireless Distribution System** tab, and update the fields as described below.

BASIC SETTINGS	<i>Configure WDS bridges to other AP/Bridges</i>	
STATUS	Radio 0 Local Address 00:0B:33:1B:C9:20	
Interfaces		
Wireless Interfaces		
Events		
Transmit / Receive Statistics		
Client Association Table		
Rogue Access Points		
SSID Table		
Mesh Status		
INTERFACE MANAGEMENT		
Global Network Settings		
Interface Network Settings		
Wireless Configuration (Radio)		
SSID Configuration		
Wireless Distribution System		
Auto VLAN Settings		
Management Interfaces		
Mesh Interfaces		
TRAFFIC MANAGEMENT		
MAC Filtering		
Quality of Service		
SYSTEM MANAGEMENT		
User Management		
Password Management		
SNMP		
Time Protocol		
System Logging		
Mesh		
Upgrade Firmware		
Reset Configuration		
Reboot System		
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 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		
Update		

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 Microcells 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 <i>both</i> Microcells participating in the WDS link. • You can have only one WDS link between any pair of Microcells or to a base station. That is, a remote MAC (peer) address may appear only once on the WDS page for a particular Microcell. • 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 48 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. <i>Spanning Tree Protocol</i> (STP), which manages path redundancy and prevents unwanted loops, is not provided on the VA2410. Keep these rules in mind when working with WDS on this release of the Vivato 802.11b/g Outdoor Microcell: • Only one path should exist between two Microcells or a Microcell and a base station; 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 VA2410s 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 Microcell or interface. For each WDS link on the VA2410, 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 Microcell or base station 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 <i>Wired Equivalent Privacy</i> (WEP) encryption enabled for the WDS link. • Enabled • Disabled <i>Wired Equivalent Privacy</i> (WEP) is a data encryption protocol for 802.11 wireless networks. Both Microcells 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 Microcell.

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 Microcells **"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://IPAddressOfMicrocell`

where *IPAddressOfMicrocell* is the address of MyVBS1.

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

The MAC address for MyVBS1 (the Microcell 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 security of the link and save the settings (click Update). Remember that if you choose to use WEP security on the WDS link you must use the identical settings on MyVBS2.

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 Microcells 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. The WDS interface must be added to an SSID that carries the network traffic between the wireless interfaces and the Ethernet interface on the device in order to bridge the WDS data. To do this, click on the **STATUS > SSID Table** tab and then click on **Configure** for the SSID carrying the WDS traffic. The WDS interface will be shown in a list of **Available Interfaces** that can be bound to this SSID. Select to bind this WDS interface to the selected SSID and select Update.

BASIC SETTINGS

STATUS

- Interfaces
- Wireless Interfaces
- Events
- Transmit / Receive Statistics
- Client Association Table
- Rogue Access Points
- SSID Table

BASIC SETTINGS

STATUS

- Interfaces
- Wireless Interfaces
- Events
- Transmit / Receive Statistics
- Client Association Table
- Rogue Access Points
- SSID Table
- Mesh Status

INTERFACE MANAGEMENT

- Global Network Settings
- Interface Network Settings
- Wireless Configuration (Radio)

View list of configured SSIDs

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

SSID Configuration

SSID Name:

Radio Interfaces: ☒ Radio 0 ☒ Radio 1

Backhaul Interface:

Available Interfaces	Bound Interfaces
wlan0wds0	eth0
	wlan0wds0

VLAN:

6. 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.)
 - › Bind the WDS interface to the SSID used to pass traffic on this Microcell (as shown in step 5).
 - › Be sure to save the settings by clicking **Update**.
7. If MyVBS1 and MyVBS2 are close enough to provide a good signal between each other, you can access the STATUS > Client Association Table and look at the quality of the link between the two devices.

Updating Settings

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

Configuring The User Password

The administrator password controls access to the VivatoVision Web pages for the Vivato 802.11b/g Outdoor Microcell. The password can be set on this screen and also on the **Network > Basic Settings** page. The new password is updated when you enter it in either place and apply the change.

The following sections describe how to configure the Administrator password on the Vivato 802.11b/g Outdoor Microcell:

- 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.

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management	<i>Change the Administrator password</i> Existing Password New Password (Enter New Password) (Re-enter to Confirm) Update
---	--

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 Microcell.

BASIC SETTINGS	<i>View settings for network interfaces</i>	
STATUS		
Interfaces	Wired Settings	
Wireless Interfaces	Ethernet 0	
Events	MAC Address	00:0B:33:1B:C9:00
Transmit / Receive Statistics		
Client Association Table	Wireless Settings (Configure)	
Rogue Access Points	Radio 0	
SSID Table	MAC Address	00:0B:33:1B:C9:20 - 00:0B:33:1B:C9:2F
Mesh Status	Mode	IEEE 802.11g
	Channel	1 (2412 MHz)
	Beacon Interval	500ms
INTERFACE MANAGEMENT		
Global Network Settings	Radio 1	
Interface Network Settings	MAC Address	00:0B:33:1B:C9:30 - 00:0B:33:1B:C9:3F
Wireless Configuration (Radio)	Mode	IEEE 802.11g
SSID Configuration	Channel	11 (2462 MHz)
Wireless Distribution System	Beacon Interval	500ms
Auto VLAN Settings		
Management Interfaces		

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 (802.11b or 802.11g) and the channel number, and the beacon Interval. See “Configuring Radio Settings” on page 48 for more information.)

Event Log

To view a list of the Microcell'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.

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

Mesh Status

INTERFACE MANAGEMENT

Global Network Settings

Interface Network Settings

Wireless Configuration (Radio)

SSID Configuration

Wireless Distribution System

Auto VLAN Settings

View events generated by this AP/Bridge

System Events Log

TIME	SEVERITY	SERVICE	DESCRIPTION
Aug 3 19:50:00	info	login[1098]	root login on `ttyS0'
Aug 3 19:49:15	info	init	Starting pid 1098, console /dev/ttyS0: '/bin/login'
Aug 3 19:49:15	info	init	Process '-/bin/login -d default' (pid 1070) exited. Scheduling it for restart.
Aug 3 19:48:15	info	init	Starting pid 1070, console /dev/ttyS0: '/bin/login'
Aug 3 19:48:15	info	init	Process '-/bin/login -d default' (pid 1069) exited. Scheduling it for restart.
Aug 3 19:47:15	info	init	Starting pid 1069, console /dev/ttyS0: '/bin/login'
Aug 3 19:47:15	info	init	Process '-/bin/login -d default' (pid 1068) exited. Scheduling it for restart.
Aug 3 19:46:14	info	init	Starting pid 1068, console /dev/ttyS0: '/bin/login'
Aug 3 19:46:14	info	init	Process '-/bin/login -d default' (pid 1040) exited. Scheduling it for restart.
Aug 3 19:45:14	info	init	Starting pid 1040, console /dev/ttyS0: '/bin/login'
Aug 3 19:45:14	info	init	Process '-/bin/login -d default' (pid 1039) exited. Scheduling it for restart.
Aug 3 19:44:14	info	init	Starting pid 1039, console /dev/ttyS0: '/bin/login'
Aug 3 19:44:14	info	init	Process '-/bin/login -d default' (pid 1038) exited. Scheduling it for restart.
Aug 3 19:43:14	info	init	Starting pid 1038, console /dev/ttyS0: '/bin/login'
Aug 3 19:43:14	info	init	Process '-/bin/login -d default' (pid 1010) exited. Scheduling it for restart.
Aug 3 19:42:14	info	init	Starting pid 1010, console /dev/ttyS0: '/bin/login'

Kernel Log

SEVERITY	DESCRIPTION
----------	-------------

The **Events** page lists the most recent events generated by this Microcell.

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 802.11b/g Outdoor Microcell acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as <i>Greenwich Mean Time</i>). 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 46.

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.

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

View transmit and receive statistics for this AP/Bridge

SSIDSG-1VLANIP192.168.0.194

	TRANSMIT			RECEIVE			
INTERFACE	MAC	PACKETS	BYTES	ERRORS	PACKETS	BYTES	ERRORS
wlan0	00:0B:33:1B:C9:20	909	112896	0	23	3055	0
wlan1	00:0B:33:1B:C9:30	0	0	0	0	0	0
eth0	00:0B:33:1B:C9:00	13401	0	0	48828	5525758	0

This page provides some basic information about the SSID and a real-time display of the transmit and receive statistics for this Microcell as described in the following table. All transmit and receive statistics shown are totals since the Microcell was last started. If the Microcell 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	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 802.11b/g Outdoor Microcell 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 Microcell.
Bytes	Indicates total number of bytes sent (in the Transmit table) or received (in the Received table) by this Microcell.
Errors	Indicates total errors related to sending and receiving data through this interface.

Associated Wireless Clients

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

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

View list of currently associated client stations

RADIO	NETWORK	VLAN	IP ADDRESS	STATION/*PEER	STATUS	FROM STATION	TO STATION	AUTHENTICATED	ASSOCIATED	PACKETS	BYTES	PACKETS	BYTES	TX RATE	SNR	SIGNAL
wlan0	-	-	0.0.0.0	*00:0b:33:08:05:20	-	-		1	57	0	0	11.0	14	-84 dBm		
wlan0	SG-1		192.168.0.68	00:0a:8a:47:b9:19	Yes	Yes		322	11869	130	8206	1.0	48	-50 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/*Peer	The MAC address of the client. An asterisk (*) indicates that this is a WDS link to another Microcell or base station, and the MAC address shown is the address of the wireless interface used on the other device for the WDS link.
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 (Packets/Bytes)	The number of packets and bytes from the client.
TO STATION (Packets/Bytes)	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 Microcell

For maintenance purposes or as a troubleshooting measure, you can reboot the Vivato 802.11b/g Outdoor Microcell as follows.

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

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management SNMP Time Protocol System Logging Mesh Upgrade Firmware Reset Configuration Reboot System	Reboot the AP/Bridge Reboot AP/Bridge Reboot
---	---

8. Click the **Reboot** button.

The VA2410 reboots. See also “Resetting the Configuration”.

Resetting the Configuration

Resetting the Configuration

If you are experiencing extreme problems with the Vivato 802.11b/g Outdoor Microcell 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 Microcell, 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 802.11b/g Outdoor Microcell” on page 25.

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

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management SNMP Time Protocol System Logging Mesh Upgrade Firmware Reset Configuration Reboot System	<i>Reset the AP/Bridge back to factory settings</i> Restore Factory Default Configuration Reset
--	--

2. Click the **Reset** button.

Factory defaults are restored.

Upgrading the Firmware

As new versions of the Vivato 802.11b/g Outdoor Microcell 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 VA2410 Outdoor Microcell.

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 VA2400<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.

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management SNMP Time Protocol System Logging Mesh Upgrade Firmware	Upgrade firmware <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: right; width: 30%;">Model</td> <td>VA24xx</td> </tr> <tr> <td style="text-align: right;">Firmware Version</td> <td>va2400.3.0.a2</td> </tr> <tr> <td style="text-align: right;">New Firmware Image</td> <td> Browse... </td> </tr> <tr> <td colspan="2" style="text-align: right; padding-top: 20px;"> Update </td> </tr> </table>	Model	VA24xx	Firmware Version	va2400.3.0.a2	New Firmware Image	Browse...	Update	
Model	VA24xx								
Firmware Version	va2400.3.0.a2								
New Firmware Image	Browse...								
Update									

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 Microcell will be unavailable. Do not power down the Microcell while the upgrade is in process. When the upgrade is complete, the Microcell 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 Microcells, Wi-Fi base stations, and access points within range of the Microcell 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

BASIC SETTINGS

STATUS

Interfases

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

Mesh Status

INTERFACE MANAGEMENT

Global Network Settings

Interface Network Settings

Wireless Configuration (Radio)

SSID Configuration

Wireless Distribution System

Auto VLAN Settings

Management Interfaces

Mesh Interfaces

TRAFFIC MANAGEMENT

MAC Filtering

Quality of Service

SYSTEM MANAGEMENT

User Management

Password Management

SNMP

View rogue access points

Access Point Detection ☒ Enabled ☐ Disabled

MAC ADDR.	RADIO	BEACON INT.	TYPE	SSID	PRIVACY	WPA	BAND	CHANNEL	RATE	SIGNAL	# OF BEACONS	LAST BEACON	RATES
00:0b:33:06:0c:95	wlan1	100	AP	bapnet-p8	On	On	2.4	11	20	-79 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:01:0e:6c	wlan1	100	AP	bapnet-lj	On	On	2.4	11	20	-86 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:01:26:b5	wlan1	100	AP	sqal-djs-8021x	On	Off	2.4	11	20	-86 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:01:0e:72	wlan1	100	AP	bapnet-lj	On	On	2.4	11	20	-86 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:01:26:b3	wlan1	100	AP	sqal-djs-8021x	On	Off	2.4	11	20	-82 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:01:26:aa	wlan1	100	AP	sqal-djs-8021x	On	Off	2.4	11	20	-87 dBm	1	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:06:02:13	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-71 dBm	2	Thu Aug 4 00:04:16 2005	1, 2, 5, 11
00:0b:33:12:04:e0	wlan1	100	AP	-	Off	Off	2.4	11	10	-90 dBm	184	Thu Aug 4 00:04:41 2005	1, 2, 5, 5, 6, 9, 11, 12, 18, :
00:0b:33:01:15:6b	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-70 dBm	29	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:69	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-72 dBm	29	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:6a	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-66 dBm	30	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:0c	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-76 dBm	291	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:0b	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-76 dBm	289	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:02:24:34:33:97	wlan1	100	AP	Dangr	On	Off	2.4	11	20	-74 dBm	283	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:15	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-73 dBm	292	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:6c	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-77 dBm	30	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:13	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-77 dBm	296	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:75	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-77 dBm	30	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:14	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-76 dBm	288	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:0a	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-72 dBm	297	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:73	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-65 dBm	32	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:12	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-77 dBm	298	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:15:72	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-67 dBm	35	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:60	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-71 dBm	281	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:06:02:12	wlan1	4000	AP	Vivato	Off	Off	2.4	11	20	-65 dBm	584	Thu Aug 4 00:04:37 2005	1, 2, 5, 11
00:0b:33:01:15:74	wlan1	1000	AP	<00>	On	Off	2.4	11	20	-72 dBm	3221	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:01:bb:09	wlan1	100	AP	Vivato	Off	Off	2.4	11	20	-77 dBm	15131	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:50	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-65 dBm	28040	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:20	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-66 dBm	20768	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:40	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-71 dBm	18398	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:30	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-72 dBm	12047	Thu Aug 4 00:04:41 2005	1, 2, 5, 11
00:0b:33:08:1a:70	wlan1	100	AP	littlebo	On	Off	2.4	11	10	-70 dBm	31619	Thu Aug 4 00:04:41 2005	1, 2, 5, 11

Refresh

Information provided on neighboring Microcells is described in the following table.

Field	Description
MAC Address	Shows the MAC address of a neighboring Microcell, access point, or base station. A MAC address is a hardware address that uniquely identifies each node of a network.
RADIO	This is the radio that received this signal..

Field (Continued)	Description (Continued)
Beacon Interval	Shows the Beacon interval being used by this device. Beacon frames are transmitted by a Microcell 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 48.)
Type	Indicates the type of device: • AP indicates the neighboring device is a Microcell 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 access point. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as <i>peer-to-peer</i> mode or an <i>Independent Basic Service Set</i> (IBSS).
SSID	The <i>Service Set Identifier</i> (SSID) for the Microcell. 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 <i>Network Name</i>. The default SSID is set on the Basic Settings page. See "Configuring Basic Settings" on page 35. New SSIDs are created on the INTERFACE MANAGEMENT > SSID Configuration settings. See "Creating and Managing Multiple Networks (SSIDs)" on page 84.
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 device.
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 device 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 48.)
Rate	Shows the rate (in megabits per second) at which this device 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 device as measured in dBm units.
# of Beacons	Shows the total number of beacons transmitted by this device since it was last booted.

Field (Continued)	Description (Continued)
Last Beacon	Shows the date and time of the most recent beacon was transmitted from the device.
Rates	Shows supported and basic (advertised) rate sets for the neighboring device. 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 48.) The rates shown for a Microcell will always be the rates currently specified in its Radio Settings.

Creating and Managing Multiple Networks (SSIDs)

Each time an SSID is created, the Microcell creates a new bridge that connects all of the selected interfaces. The Microcell 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 Microcell 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..

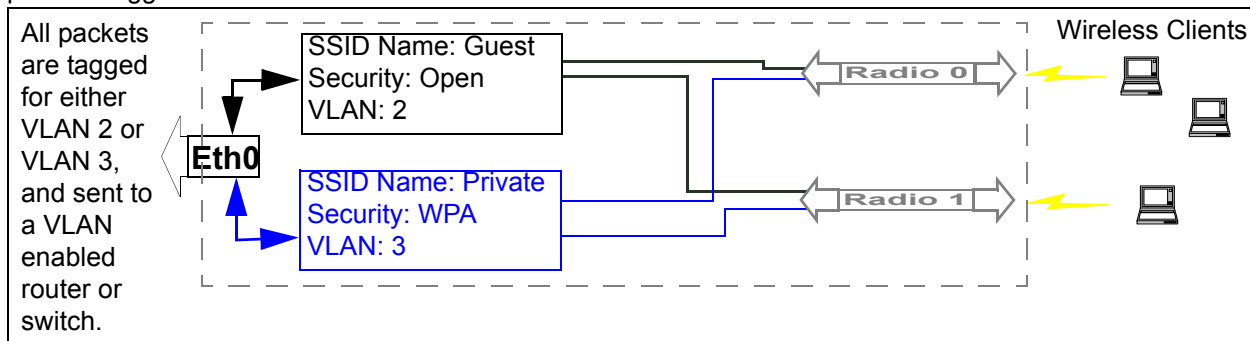


Figure 2 Creating Two Separate Networks Using VLANs

Navigating to Current SSID Settings

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

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

View list of configured SSIDs

SSID NAME	SECURITY MODE	BEACONING	VLAN	RADIOS	BRIDGED WDS	
Vivato Internal Network	plaintext	enabled		0 1	disabled	not deletable Configure
SG-1	wpaRadius	enabled	23	0	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 Microcell or to a base station.
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 86 for descriptions of each SSID feature.

Creating and Editing SSIDs

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

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.
TX Retry Threshold	This is the maximum number of consecutive transmission retries to an associated station before the station is disassociated.
TX Retry Timeout	This is the maximum amount of time (in seconds) that is allowed to elapse between the transmission of a packet to an associated station and receiving a transmission acknowledgement (ack) from that station before the station is disassociated.

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 their 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 send 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 <i>Delivery Traffic Information Map</i> (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 Microcell awaiting pick-up. The DTIM you specify here indicates how often the clients served by this Microcell should check for buffered data still on the VA2410 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 VA2410 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 "" on page 95 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 Microcell 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 switch 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 Microcell. This is done by enabling the Auto VLAN feature on the backhaul interface (Ethernet or WDS) of the Microcell. If the client successfully authenticates, the RADIUS server provides the VLAN assignment for that client to the Microcell, which in turn creates a VLAN of the same ID for the client to use while associating with the Microcell. 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**.

Configuring Security

Each SSID network that you configure on the Microcell has its own Security Mode associated with it. Each client that associates through that SSID must be configured to use those security settings in order to access the network. For information on creating and editing SSIDs, see “Creating and Editing SSIDs” on page 86.

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 802.11b/g Outdoor Microcell 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.

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 124.

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 Microcell, you first must choose the security mode, then enter specific settings for that type of security, such as the authentication algorithm to use.

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 to use the TKIP encryption algorithm or to use one of the other security modes.

Security may not be as much of a priority on some types of networks. If you are only providing Internet and printer access 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 94)

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 VA2410, 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 Microcell setup, or during testing or problem solving.

See Also

For information on how to configure plain text mode, see "Plain-text" on page 96 under "" on page 95.

When to Use Static WEP

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and Microcells 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 802.11b/g Outdoor Microcell). The client stations must have the same key indexed in the same slot to access data on the Microcell.	An RC4 stream cipher is used to encrypt the frame body and <i>cyclic redundancy checking</i> (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 96 under "" on page 95.

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 <i>cyclic redundancy checking</i> (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 802.11b/g Outdoor Microcell 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).

If you have an external RADIUS server on your network, we recommend using it rather than the using the embedded RADIUS server on the VA2410. 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 100 under “” on page 95.

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.	<i>Temporal Key Integrity Protocol</i> (TKIP) <i>Counter mode/CBC-MAC Protocol</i> (CCMP) <i>Advanced Encryption Standard</i> (AES)	<i>Remote Authentication Dial-In User Service</i> (RADIUS) You have a choice of using the Vivato 802.11b/g Outdoor Microcell 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 Microcell. 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 VA2410s 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 (VA2410-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 VA2410-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.

See Also

For information on how to configure WPA with RADIUS security mode, see "WPA with RADIUS" on page 102 under "" on page 95.

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.	• <i>Temporal Key Integrity Protocol (TKIP)</i> • <i>Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES)</i>	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 VA2410 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 107 under "" on page 95.

Does Prohibiting the Broadcast SSID Enhance Security?

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your Microcell (see "Broadcast SSID" on page 87). When the VA2410'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 84 .

Configuring Security Settings

The following configuration information explains how to configure security modes on the Microcell. Keep in mind that each wireless client that wants to exchange data with the Microcell 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 802.11b/g Outdoor Microcell 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 Microcells 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 Microcell 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 100, "WPA with RADIUS" on page 102, or "WPA-PSK" on page 107.)

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

The Microcell 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 Microcell.

Client stations can use different keys to transmit data to the Microcell. (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 Microcell settings:

Security Mode: Static WEP																
Transfer Key Index	1															
Key Length	☐ 40 bits ☒ 104 bits															
Key Type	☐ ASCII ☒ Hex															
Characters Required	26															
	<table border="1"> <thead> <tr> <th></th> <th>Key</th> <th>Key Confirmation</th> </tr> </thead> <tbody> <tr> <td>WEP Keys</td> <td>1: </td> <td> </td> </tr> <tr> <td></td> <td>2: </td> <td> </td> </tr> <tr> <td></td> <td>3: </td> <td> </td> </tr> <tr> <td></td> <td>4: </td> <td> </td> </tr> </tbody> </table>		Key	Key Confirmation	WEP Keys	1:			2:			3:			4:	
	Key	Key Confirmation														
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 Microcell 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. The identical key must also be entered in the Key Confirmation box before it is accepted. Keys are displayed as dots (•) when entered rather than being displayed in clear text. Be sure to record the keys that are entered, since there is no way to read the keys in clear text on the Microcell afterward. 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 Microcell. Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the VA2410. (See "Rules to Remember for Static WEP" on page 98.)

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 Microcell 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 Microcell 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 Microcell. Note that just because a client station is allowed to <i>associate</i> does not ensure it can exchange traffic with a Microcell. A station must have the correct WEP key to be able to successfully access and decrypt data from a Microcell, and to transmit readable data to the Microcell. Shared Key authentication requires the client station to have the correct WEP key in order to associate with the Microcell. When the authentication algorithm is set to "Shared Key", a station with an incorrect WEP key will not be able to associate with the Microcell. 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 Microcell. • Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the Microcell 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 VA2410 in order to de-code VA2410-to-station data transmissions.
- The VA2410 must have all keys used by clients for station-to-VA2410 transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (VA2410 and clients). For example if the VA2410 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 VA2410s cannot decode each other's transmissions.

Example of Using Static WEP

For a simple example, suppose you configure three WEP keys on the Microcell. In our example, the Transfer Key Index for the VA2410 is set to "3". This means that the WEP key in slot "3" is the key the Microcell will use to encrypt the data it sends.

Figure 3 Setting the Transfer Key on the Microcell

The screenshot shows a configuration window for Static WEP. At the top, 'Security Mode' is set to 'Static WEP'. Below this, 'Transfer Key Index' is set to '1'. 'Key Length' has radio buttons for '40 bits' and '104 bits', with '104 bits' selected. 'Key Type' has radio buttons for 'ASCII' and 'Hex', with 'ASCII' selected. 'Characters Required' is set to '13'. There are four rows for 'WEP Keys', each with a 'Key' field and a 'Key Confirmation' field. The first three rows are filled with dots, and the fourth row is empty. At the bottom, 'Authentication Algorithms' is set to '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 VA2410. For this example, we'll set WEP key 1 on a Windows client.

Figure 4 Providing a Wireless Client with a WEP Key

The screenshot shows the 'Wireless network properties' dialog box with the 'Authentication' tab selected. The 'Network name (SSID)' is 'Ivers Clams'. Under 'Wireless network key', it says 'This network requires a key for the following:'. 'Network Authentication' is set to 'Shared' and 'Data encryption' is set to 'WEP'. There are two fields for the 'Network key' and 'Confirm network key', both filled with dots. 'Key index (advanced)' is set to '1'. There is a checkbox for 'The key is provided for me automatically' which is unchecked. At the bottom, there is a checkbox for 'This is a computer-to-computer (ad hoc) network: wireless access points are not used' which is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

If you have a second client station, that station also needs to have one of the WEP keys defined on the VA2410. 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.

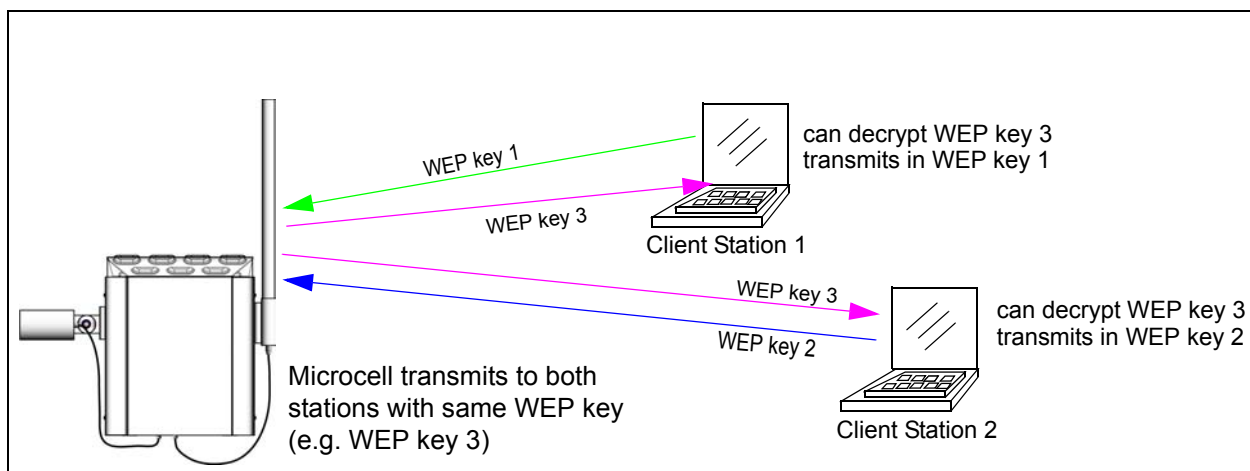
Static WEP with Transfer Key Indexes on Client Stations

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-VA2410 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 VA2410 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 VA2410 and two client stations using multiple WEP keys and a transfer key index.

Figure 5 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, or the configuration of user accounts via the **Network > User Management** tab.

The Microcell requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell 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 Microcell.

MAC filtering can also be used in conjunction with an external RADIUS authentication server to provide a two-tiered approach to authenticating wireless clients. When selected, MAC filtering is performed on the incoming client packets to explicitly allow or deny specific clients. If the filter allows passage of the packet, its authentication request is forwarded to the RADIUS server. If a MAC filter denies passage to a client packet, its authentication request is not forwarded to the RADIUS server.

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

Radius MAC Filtering: ☐	
NAS IP Address	. . .
NAS Identifier	
Primary Radius:	
Radius IP	. . .
Radius Key	
Radius Key Confirmation	
☐ Enable radius accounting	
Secondary Radius:	
Radius IP	. . .
Radius Key	
Radius Key Confirmation	
☐ Enable radius accounting	
Update	

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 802.11b/g Outdoor Microcell. 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 802.11b/g Outdoor Microcell, the RADIUS server User Datagram Protocol (UDP) ports used by the Microcell are not configurable. (The Vivato 802.11b/g Outdoor Microcell 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 VA2410 to first use the MAC Filtering settings on the VA2410 to filter clients that are specifically allowed or denied authentication. See "Navigating to MAC Filtering Settings" on page 54. 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. NOTE: This function is only available when an external RADIUS authentication server is used.
NAS IP Address	If used, enter the IP address of a connected network access server (NAS).
NAS Identifier	Enter the identifier string for the network access server.
Radius IP	Enter the Radius IP in the text box. The <i>Radius IP</i> is the IP address of the RADIUS server. (The Vivato 802.11b/g Outdoor Microcell internal authentication server is 127.0.0.1.) For information on setting up user accounts, see "Managing User Accounts" on page 42.
Radius Key	Enter the Radius Key in the text box. The <i>Radius Key</i> 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 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell 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: ☐

NAS IP Address . . .

NAS Identifier

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 Microcells. 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 Microcell. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the VA2410: • 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 VA2410. 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

Field (Continued)	Description (Continued)
Authentication Server	Select one of the following from the drop-down menu: • Built-in - To use the authentication server provided with the Vivato 802.11b/g Outdoor Microcell. 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 802.11b/g Outdoor Microcell, the RADIUS server User Datagram Protocol (UDP) ports used by the Microcell are not configurable. (The Vivato 802.11b/g Outdoor Microcell is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)
Radius MAC Filtering	When unchecked, client (station) authentication requests are passed directly to the specified RADIUS server(s). Checking this box causes the VA2410 to first use the MAC Filtering settings on the VA2410 to filter clients that are specifically allowed or denied authentication. See "Navigating to MAC Filtering Settings" on page 54. 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. NOTE: This function is only available when an external RADIUS authentication server is used.
NAS IP Address	If used, enter the IP address of a connected network access server (NAS).
NAS Identifier	Enter the identifier string for the network access server.
Radius IP	Enter the Radius IP in the text box. The <i>Radius IP</i> is the IP address of the RADIUS server. (The Vivato 802.11b/g Outdoor Microcell internal authentication server is 127.0.0.1.) For information on setting up user accounts, see "Managing User Accounts" on page 42.

Field (Continued)	Description (Continued)
Radius Key	Enter the Radius Key in the text box. The <i>Radius Key</i> 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 802.11b/g Outdoor Microcell 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 Microcells. 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 Microcell. WPA clients must have one of the following to be able to associate with the VA2410: • A valid TKIP key • A valid CCMP (AES) key Clients not configured to use WPA-PSK will not be able to associate with VA2410.
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 hexadecimal characters (a-f, 0-9).

Field	Description
Key	The <i>Pre-shared Key</i> 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**.

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 VA2410's configuration.

Navigating to the Management Interfaces Settings

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

Set Management Interfaces	
Non-Management Interfaces eth0 wlan0 "Vivato Internal Network" wlan0wds0 wlan0 "SG-1" wlan1 "Vivato Internal Network"	Management Interfaces eth0 "vlan 23"
Update	

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

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 change² and monitor settings within the Microcell. The Microcell 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 Microcell 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-VA2400-AGT-CAP-MIB.txt
- VIVATO-VA2410-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

System Location

System Contact

System Description

Read Only Community String

Read/Write Community String

Trap Hosts

Host Name	Community Name	Trap Host Type
		Trap Sink

2. The VA2410 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 Microcell in your network.
System Location	Enter the physical location of this Microcell. This may be used to distinguish it from another Microcell located in the same area.
System Contact	Enter the name of the person who is responsible for maintaining the configuration of the Microcell.
System Description	Enter a description of the system that this Microcell 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.

BASIC SETTINGS STATUS Interfaces Wireless Interfaces Events Transmit / Receive Statistics Client Association Table Rogue Access Points SSID Table Mesh Status INTERFACE MANAGEMENT Global Network Settings Interface Network Settings Wireless Configuration (Radio) SSID Configuration Wireless Distribution System Auto VLAN Settings Management Interfaces Mesh Interfaces TRAFFIC MANAGEMENT MAC Filtering Quality of Service SYSTEM MANAGEMENT User Management Password Management SNMP Time Protocol System Logging	<i>Log Server Configuration</i> Log ☒ Enable ☐ Disable Server: Port: 514 Update
--	---

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**.

Mesh Network Operation

A mesh network consists of two or more wireless devices (such as Microcells and Wi-Fi base stations) that work together to provide a network backhaul connection to clients. It is similar in many ways to using WDS links, but includes the ability to dynamically create data links between Microcells and base stations as new ones are added or when one of them is shut down.

A mesh network relies on one or more “root nodes” - a device connected directly to the wired network. Other nodes in the mesh network are referred to as a “parent” or as a “child” (also referred to as “downlink” and “uplink” radios, respectively). A parent is a radio that provides the uplink connection to the root for a child, and can also be used to service clients within its operating area. Because the root node provides a downlink to at least one child node, it is also considered a parent node. A child receives the downlink signal from the parent, and can only be served by one parent at any time - it cannot multiplex frames from two or more parents. To help prevent data loops, only one radio can be configured as a child on any mesh device.

Vivato base stations are always used as a root/parent node during mesh operation. The VA2410 Microcell can be configured as a child, a parent, or as a root. As a child, it can receive a downlink signal from a parent while also providing client connections and a downlink signal to another Microcell.

Several parent and child nodes can be used in sequence to send frames serially back and forth between clients and the root node. The number of times the frames are passed on from one mesh device to another are referred to as “hops”. The greater the number of hops, the slower the network connection, due to the latency associated with the reception and re-transmission of the frames.

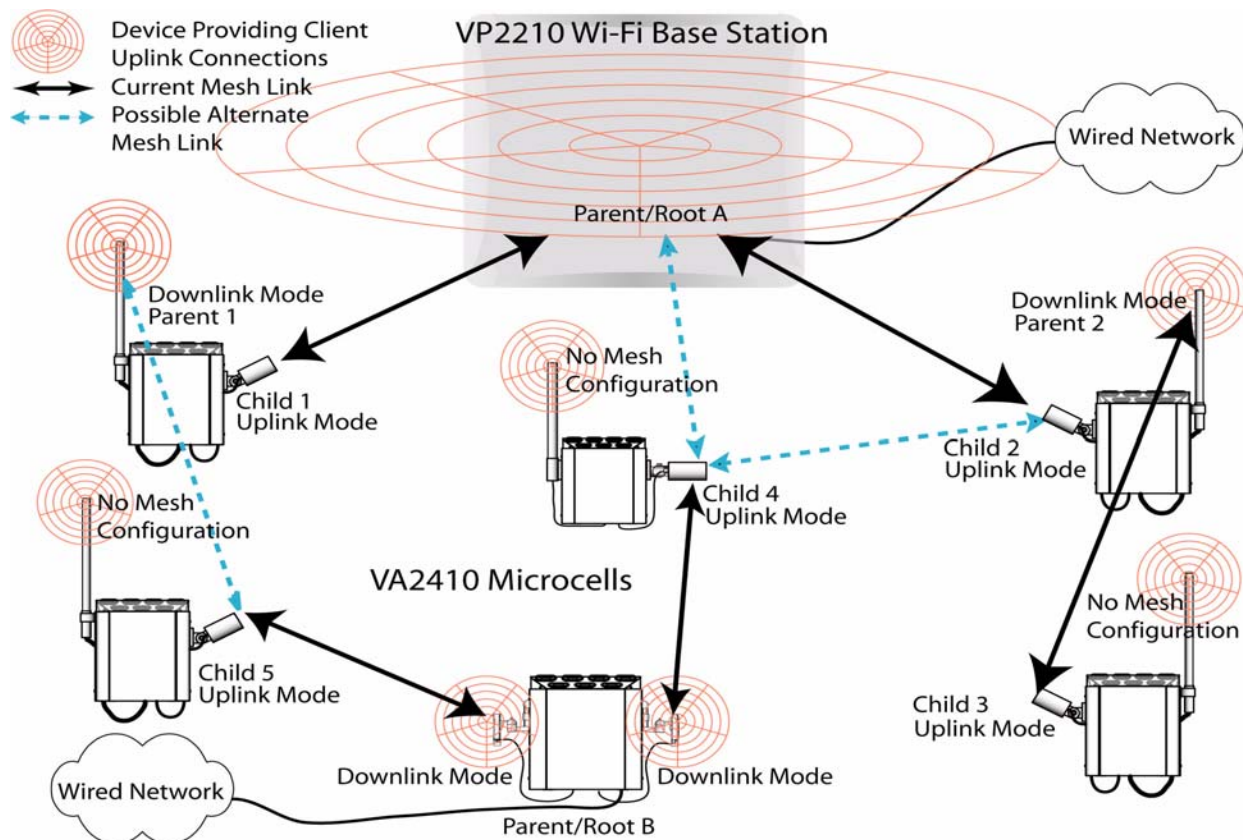


Figure 6—Example Mesh Network

In the example illustrated above, two parent/root nodes (labeled A and B) are used to provide a path to the same wired network. The figure shows that Parent/Root A is currently providing a backhaul connection to Child 1 through a single hop. It is also providing the backhaul to Child 2 through a single hop, which in turn uses its second radio to provide the backhaul to Child 3 (resulting in two hops to that child).

Parent/Root B is currently providing the backhaul path to Child 4 and Child 5 through a single hop to each device.

The dashed lines show that both parents could provide alternative root paths to the child nodes. Which parent a child uses depends on several factors. Some settings can be used to force a child to only select from a configured list of parents. A parent node periodically measures the rate at which it can transfer frames back and forth to the root node and advertises that “root path cost” in its mesh beacons. Child nodes look at the mesh beacons to determine which parent will provide the lowest root path cost, and therefore the fastest link to the wired network.

Important 	Using static WDS links and mesh networking at the same time can result in duplicate links to the same node, producing data loops that will prevent the network from working and prevent further access to the mesh devices except through a direct serial port connection. Although static WDS links and mesh operation can be used at the same time in some network setups, careful planning must be used to prevent creating loops. Therefore, whenever possible, do not use static WDS links when mesh networking is enabled.
---	---

Mesh Operation and the Impact on Client Data Throughput

Periodic mesh configuration signals use the same rules for sharing wireless signal bandwidth that all other Wi-Fi devices (including clients) must use. Therefore, absolute maximum data throughput to/from a single client associating to a mesh node is limited by the 802.11 mode being used (11 Mbps for 802.11b and 54 Mbps for 802.11g) minus the overhead traffic messages used for mesh operation. As more mesh devices are added to the mesh network, more signals are being sent out by those devices in order to maintain integrity of the mesh network. These signals use a certain amount of network time that could otherwise be used to serve clients. For example, if a Microcell that has 25 clients associated to it is added to the mesh network, the traffic of all 25 clients, plus the additional mesh network maintenance traffic, must be passed through the mesh network to the root node. This significantly decreases the average level of wireless client data throughput throughout the mesh network.

VLAN Operation Through Mesh Nodes

In order to pass VLAN traffic to/from clients, each node in the mesh network must be configured with VLANs of the same IDs used by the wired network to serve those clients. In the VP2410, this requires creating an SSID for each VLAN to which clients may be associated. For example, if wireless clients are part of a local network with VLANs 1, 2, and 3, you would create three SSIDs with VLAN IDs of 1, 2, and 3. In order to operate in the mesh network, each SSID would include the Radio Interfaces used for mesh operation and have the Ethernet port that is connected to the wired network as the Bound Interface. See “Creating and Editing SSIDs” on page 86.

Rebooting After Changing Mesh Settings and After Firmware Upgrades

Mesh setting changes do not take effect until after the base station has been rebooted. Therefore whenever you change your mesh configuration, you must reboot the product.

When updating the firmware or mesh configuration in multiple devices in the mesh network, always update the nodes that are farthest from the root/parent first, then upgrading the next furthest nodes until the root/parent node is updated last. For example, in Figure 6—“Example Mesh Network” on page 114, the device labeled “Child 3” would be updated first, then “Child 2”, “Child 4”, and “Child 1”, and then “Parent/Root A”. Updating the other part of the network would be done the same way; “Child 5” would be updated, followed by “Parent/Root B”.

Configuring Mesh Operation

Mesh operation uses global level and wireless interface level settings:

- Global level mesh settings are used to enable/disable mesh operation and configure this device to work with other devices in the mesh network. This screen also lists the present mesh settings for each wireless interface and provides a link to change those settings. See “Navigating to Global Mesh Settings” on page 116.
- Wireless interface mesh settings control how each interface operates in the mesh network, or whether it is not used for mesh operation. See “Navigating to Wireless Interface Mesh Settings” on page 119.
- Current mesh operation can be viewed on the Mesh Status screen. See “Navigating to the Mesh Status Screen” on page 121.

Navigating to Global Mesh Settings

To access the global mesh network configuration settings, navigate to the **SYSTEM MANAGEMENT > Mesh** tab.

BASIC SETTINGS	<i>Mesh Configuration</i>	
STATUS		
Interfaces		
Wireless Interfaces		
Events		
Transmit / Receive Statistics		
Client Association Table		
Rogue Access Points		
SSID Table		
Mesh Status		
INTERFACE MANAGEMENT		
Global Network Settings		
Interface Network Settings		
Wireless Configuration (Radio)		
SSID Configuration		
Wireless Distribution System		
Auto VLAN Settings		
Management Interfaces		
Mesh Interfaces		
TRAFFIC MANAGEMENT		
MAC Filtering		
Quality of Service		
SYSTEM MANAGEMENT		
User Management		
Password Management		
SNMP		
Time Protocol		
System Logging		
Mesh		
Upgrade Firmware		
Reset Configuration		
Reboot System		

General Configurations

Mesh Functionality: ☐ Enable ☒ Disable

Mesh Maximum Hops:

Mesh Root Node: ☐ > Enable ☐ > Disable

SSID Configuration

ESSID:

Encryption:

Passphrase:

Confirm Passphrase:

Interval Configuration

BPR Interval (in seconds 1-20):

Cost Configuration

Base Cost (0-10000):

Mesh Interfaces

Radio 0 ([Configure](#))

Channel	1
Mode	DOWNLINK
Scan Interval (1-86400)	10
Cost threshold (1-100000)	300
ACL Status	DENY
MAC ACL Addresses	0

Radio 1 ([Configure](#))

Channel	1
Mode	DOWNLINK
Scan Interval (1-86400)	10
Cost threshold (1-100000)	300
ACL Status	DENY
MAC ACL Addresses	0

Update

Field	Description
Mesh Functionality	Select Enable or Disable to turn mesh operation on or off, respectively.
Mesh Maximum Hops	Enter the maximum number of hops that can be used by a client node to reach a root node. This setting is only used for wireless interfaces that are configured to operate as mesh uplink (child) nodes.
Mesh Root Node	Root node operation can be used when a wired backhaul connection is provided to the Microcell. Enabling root node operation causes this device to identify itself in mesh beacons as a root node in the mesh network.

Field (Continued)	Description (Continued)
ESSID	Enter the mesh network name used by all devices configured in the network. The name must be in the range of 1 to 32 characters. <i>A mesh node will only associate with another node configured with the same mesh ESSID.</i> The mesh ESSID is only seen by other mesh nodes, and is not displayed on a client's list of available wireless networks. Important! <i>Be sure to change this setting from its default value in order to help secure your mesh network.</i>
Encryption	This is the type of encryption to use for securing mesh link traffic. All devices in the mesh network must use the same encryption type and passphrase in order to authenticate and associate with each other in the network. • NONE: Do not encrypt the data on mesh links. • WEP: Use wired equivalent privacy (WEP) security on the mesh links. • AES: Use advanced encryption standard (AES) security on the mesh links.
Passphrase	Enter the encryption key to use for securing all mesh connections. The same key must be used by all mesh nodes in the network, and be in the range of 8 to 32 ASCII characters. Enter the same key for the Confirm Passphrase value. Important! <i>Be sure to change this setting from its default value in order to help secure your mesh network.</i>
BPR Interval (in seconds 1-20)	Enter the interval (in seconds) between sending mesh beacons that advertise this node's mesh settings. Longer intervals may allow more traffic to be passed, whereas shorter intervals may help the mesh network to reconfigure itself more quickly when a change in signal levels or topology occurs. The default value is 1 second.
Base Cost (1-10000)	"Root path cost" is a relative measure of how fast the packets can transfer between a mesh child node and the root node through which it connects to the wired network. It is measured periodically by transferring frames between the root and the child. The faster that frames are transferred, the lower the root path cost. Increasing the number of hops between the child and its root node slows down the effective frame transfer rate, increasing the root path cost. When a device is configured as a parent node or as a root node, it advertises its root path cost periodically so that downstream nodes can determine which parent to use to provide the best service to their clients. In some situations, it may be preferable to increase the base cost in order to bias child nodes to connect to another root node with that has a faster backhaul connection.

Updating Settings

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

Navigating to Wireless Interface Mesh Settings

The following sections describe how to configure wireless interface mesh settings:

To access the wireless interface mesh network configuration settings, navigate to the **INTERFACE MANAGEMENT > Mesh Interfaces** tab. De-select the appropriate **Use Current** settings box to be able to change a setting.

BASIC SETTINGS	<i>Set Mesh Interfaces</i>		
STATUS			
Interfaces	Radio Interfaces:	☒ Radio 0	☐ Radio 1
Wireless Interfaces			Select All
Events	Mode:	Uplink	☒ Use Current
Transmit / Receive Statistics	Channel list (seperated by comma)	1	☒ Use Current
Client Association Table	Scan Interval (in seconds 1-86400):	10	☒ Use Current
Rogue Access Points	Cost Threshold (0-100000):	300	☒ Use Current
SSID Table	MAC ACL Mode:	Deny	☒ Use Current
Mesh Status	MAC ACL List		☒ Use Current
INTERFACE MANAGEMENT			
Global Network Settings			
Interface Network Settings			
Wireless Configuration (Radio)			
SSID Configuration			
Wireless Distribution System			
Auto VLAN Settings			
Management Interfaces			
Mesh Interfaces			
TRAFFIC MANAGEMENT			
MAC Filtering			
Quality of Service			
SYSTEM MANAGEMENT			
User Management			
			Update

Field	Description
Radio Interfaces	Select the interfaces to configure by selecting the appropriate check boxes, or choose Select All to configure all wireless interfaces at the same time.
Mode	Select if this wireless interface should be used for mesh operation: • Uplink: Use this interface to connect to a downlink radio from a root node or a parent node. When configured as a child, this interface cannot be used to provide wireless client access. • Downlink: Use this interface to provide a downlink to a mesh device configured as a child node, while still providing client access to clients associating to an SSID that is using this interface. • Disable: Do not use this interface for mesh operation. This interface can still be used for normal wireless client connections.
Scan Interval	Enter the uplink scan interval (in seconds) in the range of 1 to 86400). This determines how often a child looks for the best signal from a parent node in order to provide the best downlink signal. A short period reduces the delay in providing a better signal to the child if the previous parent's signal is reduced, but also increases the amount of time that the child's radio is scanning instead of passing uplink traffic. Conversely, a longer period causes the client to not react to a change in parent signal levels as quickly, but reduces the amount of time that the clients spends scanning for a better uplink signal.
Cost Threshold	This command tells a child node at what point it should leave the currently assigned parent node and connect to the root through another parent or root node; it is based on the relative root path cost of the two nodes. For example, if a value of 500 is specified, the root path cost of the alternate parent node must be at least 500 less than the cost of the currently connected parent node in order for the child to switch to using the alternate parent node.

Updating Settings

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

Navigating to the Mesh Status Screen

To view an overview of mesh operation on the Microcell, navigate to STATUS > Mesh Status.

- BASIC SETTINGS
- STATUS
 - Interfaces
 - Wireless Interfaces
 - Events
 - Transmit / Receive Statistics
 - Client Association Table
 - Rogue Access Points
 - SSID Table
 - Mesh Status

View Mesh Status

INTERFACE	MAC	MODE	STATE	ASSOCIATION	PARENT	HOPS	CHANNEL	MESH SSID	CHILDREN
wlan0	000b331bc920	Downlink	No-Connections	allow	none	0	1	vivatomesh	
wlan1	000b331bc930	Downlink	No-Connections	allow	none	0	11	vivatomesh	

Field	Description
INTERFACE	The wireless interfaces on the Microcell.
MAC	The MAC address of the wireless interface on the Microcell.
MODE	This is the type of mesh operation configured on this interface. Downlink is the only mesh operation supported; disable is selected when an interface is not used in a mesh network.
STATE	This column lists if this wireless interface is currently connected to another node (device) in the mesh network.
ASSOCIATION	This column lists whether this interface allows or denies client associations when used as a mesh node.
PARENT	This column indicates the MAC address of a node acting as a parent when this interface is configured as a child node. This feature is not currently supported.
HOPS	This is the number of hops from the root node to this wireless interface when configured as a child node. This feature is not currently supported.
CHANNEL	This is the RF channel that this interface is using for this mesh connection.
MESH SSID	This is the ESSID used by all devices in the mesh network. Only mesh devices using the same mesh ESSID can associate with each other.
CHILDREN	This column lists the MAC addresses of child nodes to which this wireless interface is acting as a parent.

System Recovery

The VA2410 uses the Linux operating system. Whenever a setting on the VA2410 is changed using the web interface and "Update" is selected, a file called "apconfig.xml" is automatically updated to include the changes. This includes changes to the administrator password and IP address used to access the VivatoVision web interface along with any other configuration changes. Those settings continue to be used for the current session, and are restored using the apconfig.xml file whenever the VA2410 is rebooted.

If changes to the configuration result in disabling access to the VA2410 web interface or cause networking problems that cannot be resolved, there are two methods that can be used to regain control:

- **Reset to full factory defaults after boot-up:** If the VA2410 boots-up normally, but the web interface cannot be accessed using a known IP address through any of its ports, access can be regained by holding in the Reset button for at least 5 seconds and then releasing it. This deletes the apconfig.xml file and reboots the VA2410 to restore it to the factory default state. You can then use the default IP address of 169.254.20.1 and default user name and password of "admin" and "vivato" (respectively) to access the web interface and reconfigure the VA2410.
- **Reset to full factory defaults if the VA2410 won't fully boot-up:** If the apconfig.xml file should become corrupted, the VA2410 will not boot-up. If this happens, connect a serial cable to the VA2410 and configure a terminal emulator to monitor the boot sequence. (See "Serial Port Communication Settings:" on page 21 for settings to use on the terminal emulator.) After establishing a terminal emulator session with the VA2410, delete the apconfig.xml file using the following steps:

1. Disconnect power to the VA2410.
2. Press *and hold* the Reset button.
3. Re-apply power to the VA2410 while continuing to press the Reset button until a login prompt appears (see below).

```
Freeing unused kernel memory: 76k freed
Using /lib/modules/2.4.18-mips/misc/ldt-reset.o
Entering Recovery Mode
Initializing random number generator... done.
Using /lib/modules/2.4.18-mips/net/80211.o
Using /lib/modules/2.4.18-mips/net/oahu.o
Using /lib/modules/2.4.18-mips/net/sch_pktpri.o
wireless modules loaded
```

Many lines of the boot-up sequence are displayed prior to accessing the Linux operating system....

```
User Access Verification
login: admin
Password:
Jan 1 00:00:34 login[123]
```

Hold the Reset button in until the login prompt is displayed, then release the button. Enter "admin" for the login, and enter "vivato" for the password.

```
Welcome to Spirit
```

```
~ # rm apconfig.xml
~ # reboot
```

Enter "rm apconfig.xml" to delete the configuration file, then enter "reboot" to reboot to default settings.

4. When prompted, use the default login of "admin" and the default password "vivato" to enter the Linux operating system.
5. Enter the command "rm apconfig.xml" to remove the configuration file.
6. Enter "reboot" to reboot the VA2410.

7. After full reboot (~30 seconds), use the default IP address of 169.254.20.1 and the default user name and password of "admin" and "vivato" (respectively) to access the web interface and reconfigure the VA2410.

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 VA2410s are online and detectable in that location.³ Once a VA2410 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 wireless network (VA2410) 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 Microcell, and (2) configure security on each of the wireless clients. We expect that initially, you will connect to a Microcell that has no security set (plain text mode) from an unsecure wireless client. With this initial connection, you can go to the Microcell VivatoVision Web pages and configure a security mode (INTERFACE MANAGEMENT > SSID Configuration). When you re-configure the Microcell with a security setting and click "Update", your wireless client will be disassociated and you will lose connectivity to the VA2410 VivatoVision Web pages. In some cases, you may need to make additional changes to the VA2410 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 802.11b/g Outdoor Microcell.

- 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 802.11b/g Outdoor Microcell

3. The exception to this is if the Microcell 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 802.11b/g Outdoor Microcell.

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 802.11b/g Outdoor Microcells with security that uses the *Built-in Authentication Server* on the VA2410. This will mean setting up the VA2410 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 802.11b/g Outdoor Microcell 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 131.
- If the Vivato 802.11b/g Outdoor Microcell 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 137.

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 134
- “WPA with RADIUS Client Using EAP-TLS Certificate” on page 140
- “Configuring an External RADIUS Server to Recognize the Vivato 802.11b/g Outdoor Microcell” on page 146
- “Obtaining a TLS-EAP Certificate for a Client” on page 149

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:

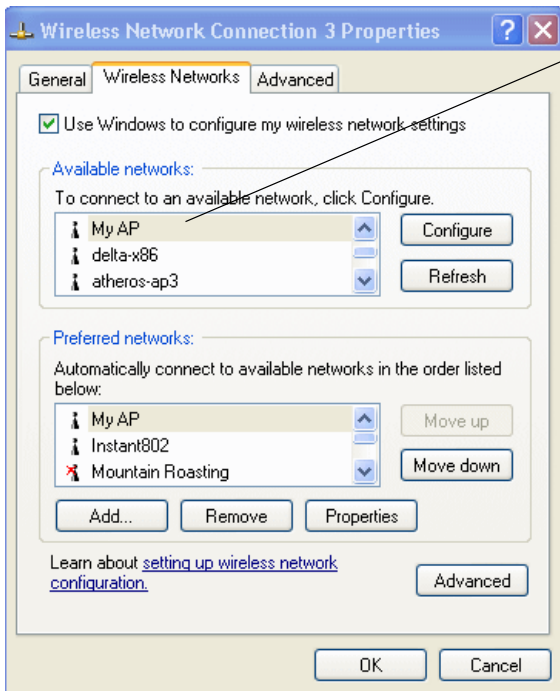
- › Right-click on the Wireless connection icon in your Windows task bar and select **View available wireless networks**.
- › Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

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.



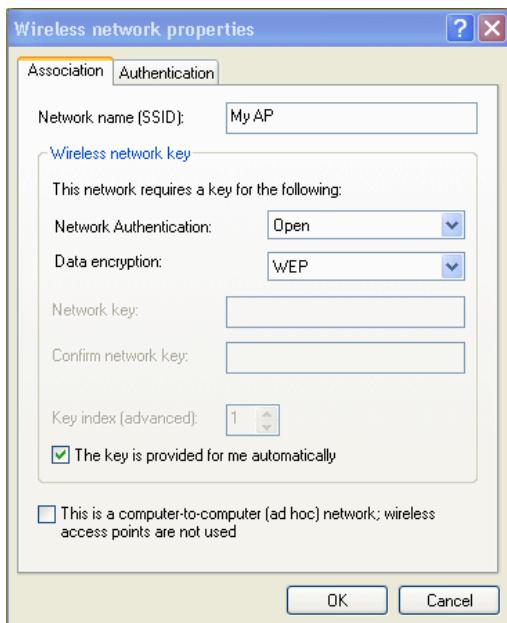
List of available networks will change depending on client location. Each network (or Microcell) that that is detected by the client shows up in this list. ("Refresh" updates the list with current information.)

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 Microcell 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.

- 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.



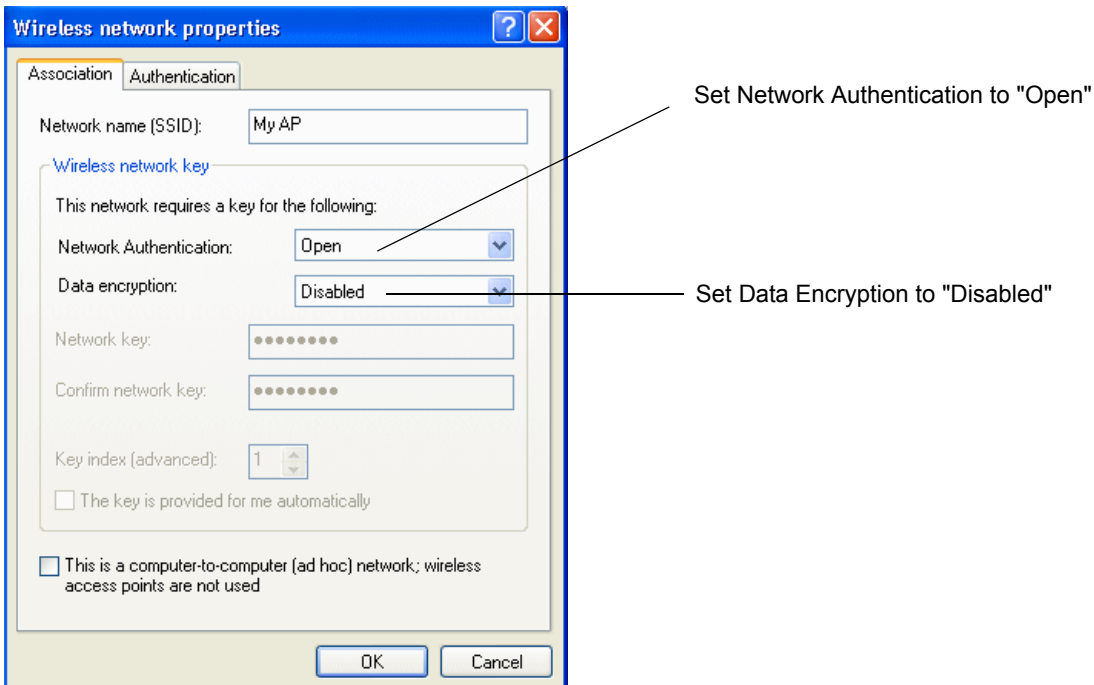
Use this dialog for configuring all the different types of client security described in the following sections. Make sure that the Wireless Network Properties dialog you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

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

If the Microcell 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 Micro-cell security configurations.

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



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 Microcell uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the Microcell. Different clients can use different keys to transmit data to the Microcell. (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 802.11b/g Outdoor Microcell 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.

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

OK Cancel

Choose Open or Shared

Choose WEP as the Data Encryption mode

Enter a network key that matches the WEP key on the Microcell 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 Microcell

Disable auto key option

Association Tab	Network Authentication	"Open" or "Shared", depending on how you configured this option on the Microcell. Note: When the Authentication Algorithm on the Microcell is set to "Both", clients set to either Shared or Open can associate with the VA2410. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the VA2410. Clients configured to use WEP as an Open system can associate with the VA2410 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 Microcell.
	Data Encryption	WEP
	Network Key	Provide the WEP key you entered on the Microcell Security settings in the Transfer Key Index position. For example, if the Transfer Key Index on the Microcell is set to "1", then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the Microcell.
	Key Index	Set key index to indicate which of the WEP keys specified on the Microcell Security page will be used to transfer data from the client back to the Microcell. For example, you can set this to 1, 2, 3, or 4 if you have all four WEP keys configured on the Microcell.
	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 Microcell. 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 802.11b/g Outdoor Microcell uses Protected *Extensible Authentication Protocol* (EAP) referred to here as "EAP/PEAP".

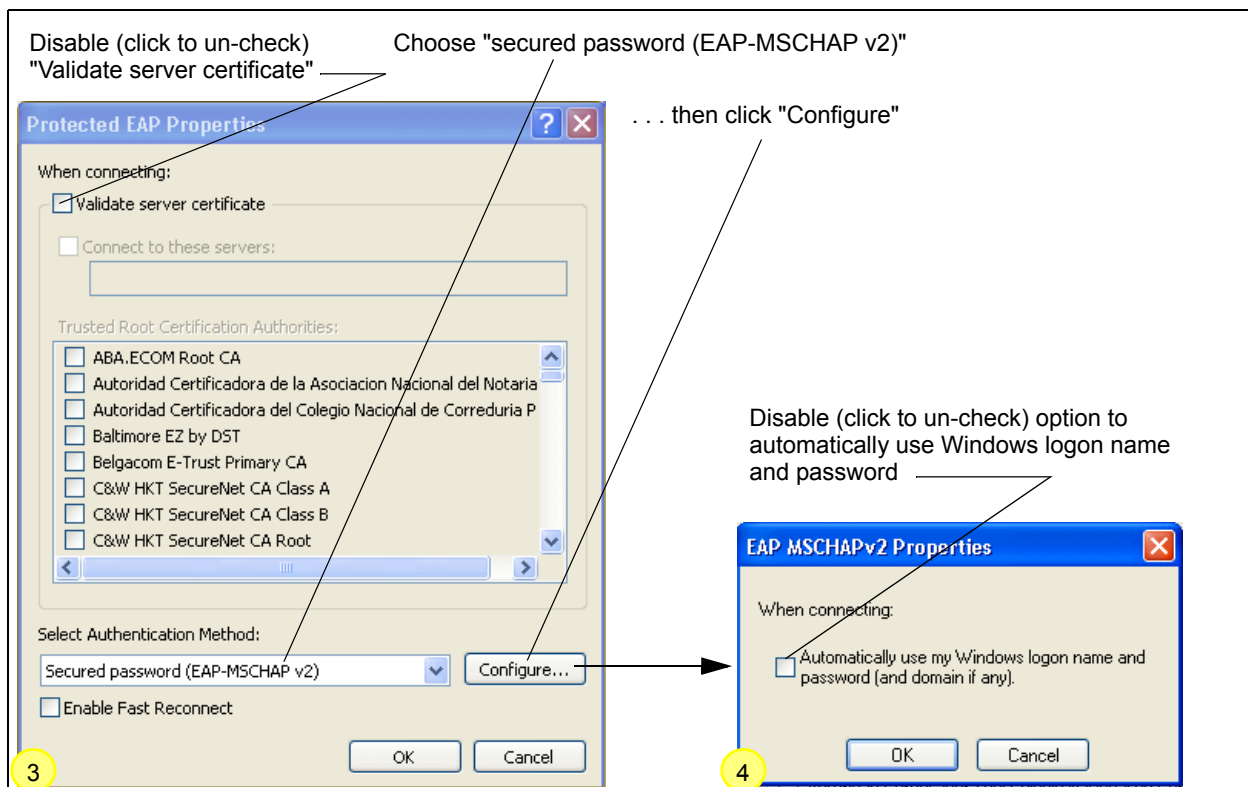
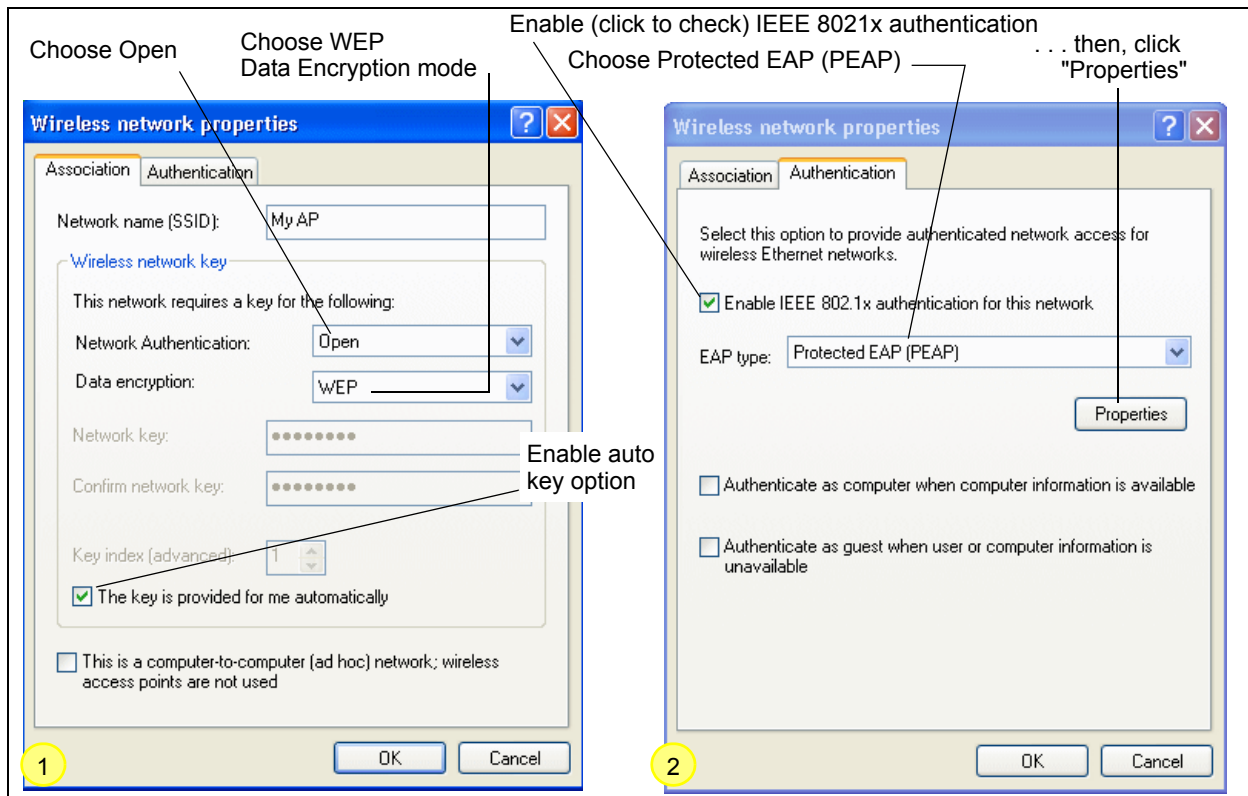
- If you are using the Built-in Authentication server with "IEEE 802.1x" security mode on the Vivato 802.11b/g Outdoor Microcell, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the Vivato 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell. If you are setting up EAP/PEAP on a client of a VA2410 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 802.11b/g Outdoor Microcell 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.



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 VA2410. If you are setting up EAP/PEAP on a client of an VA2410 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 Microcell. 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 <i>Public Key Authority Infrastructure (PKI)</i> server, including a <i>Certificate Authority (CA)</i>, 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.
-------------	---

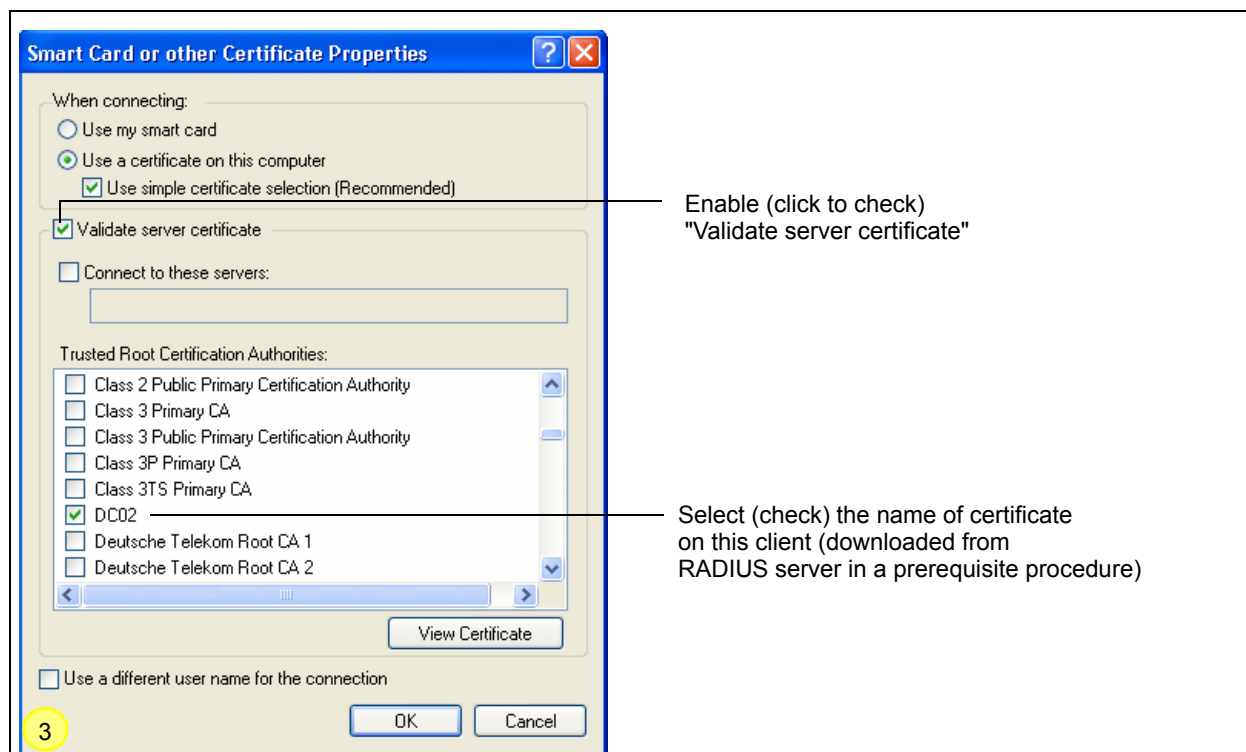
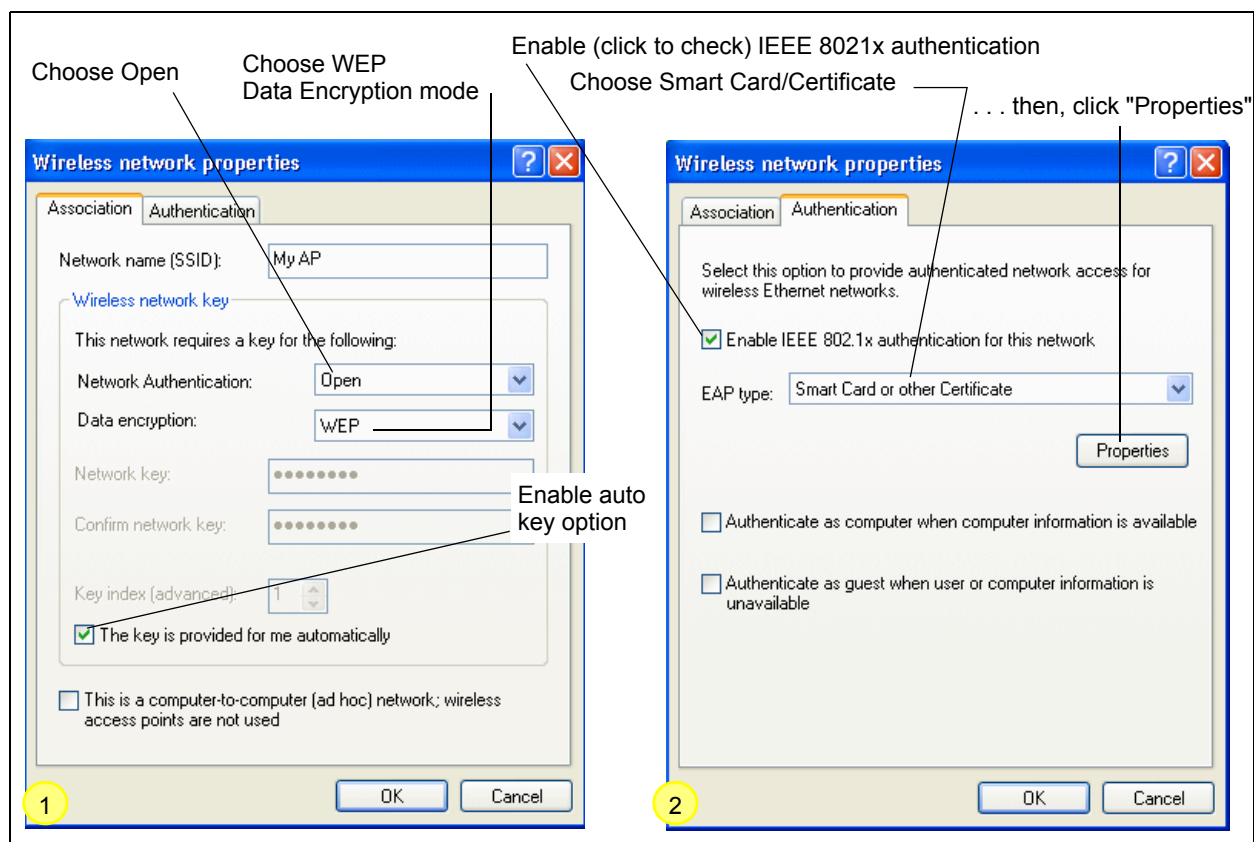
To use this type of security, you must do the following:

1. Add the Vivato 802.11b/g Outdoor Microcell to the list of RADIUS server clients. (See "Configuring an External RADIUS Server to Recognize the Vivato 802.11b/g Outdoor Microcell" on page 146.)
2. Configure the Vivato 802.11b/g Outdoor Microcell 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 149.

If you configured the Vivato 802.11b/g Outdoor Microcell 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.



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 149.

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 Microcell 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 Microcell.

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

The Vivato 802.11b/g Outdoor Microcell 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 Microcells.

So, if you configure the network (Microcell) 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 (Microcell) 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 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell, 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 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell. If you are setting up EAP/PEAP on a client of an VA2410 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 802.11b/g Outdoor Microcell 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 Microcell (**User Management**). . .

BASIC SETTINGS

STATUS

Interfaces

Wireless Interfaces

Events

Transmit / Receive Statistics

Client Association Table

Rogue Access Points

SSID Table

Mesh Status

INTERFACE MANAGEMENT

Global Network Settings

Interface Network Settings

Wireless Configuration (Radio)

SSID Configuration

Wireless Distribution System

Auto VLAN Settings

Management Interfaces

Mesh Interfaces

TRAFFIC MANAGEMENT

MAC Filtering

Quality of Service

SYSTEM MANAGEMENT

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 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 authentication server is chosen. See the Help panel for more information.

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
☐	[Edit]	amanda	(null)	disabled
☐	[Edit]	oneil	(null)	disabled

Selected users:

Enable

Disable

Remove

Add a user...

To add a user, fill in the fields below and click "add account".

User Name

tealc

Real Name

christopher

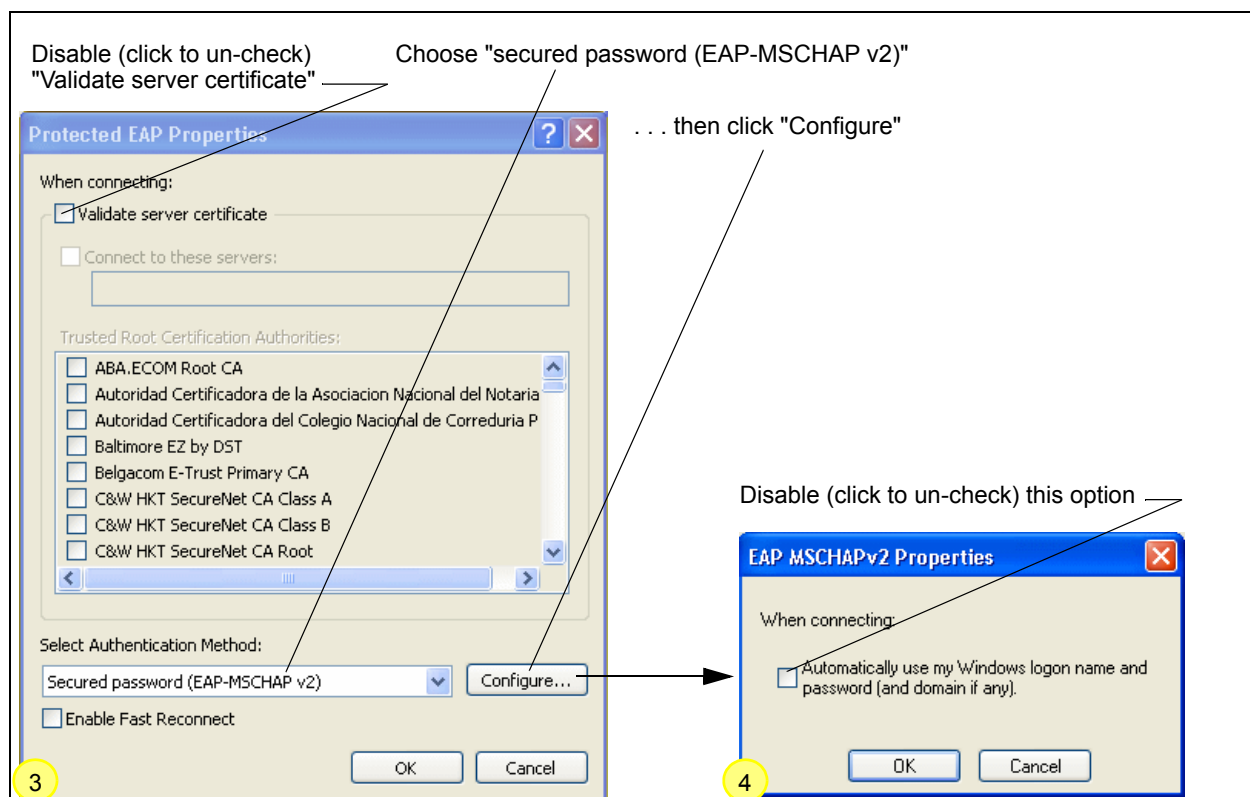
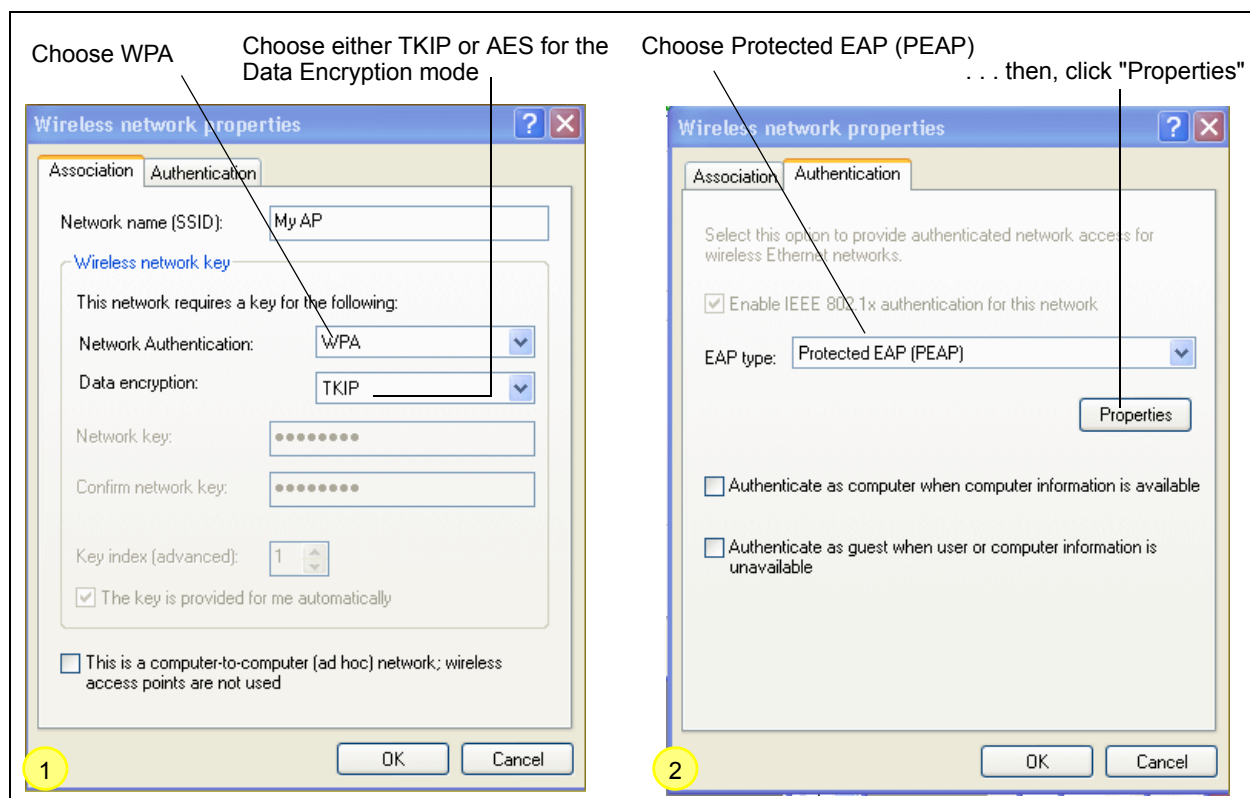
Password

Password (again for safety)

Cancel

Add Account

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



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 Microcell.
Note: When the Cipher Suite on the Microcell 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 Microcell. For more information, see Users Guide and Online Help on the Microcell.		

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).
	Select Authentication Method	Choose "Secured password (EAP-MSCHAP v2)"
Note: This example assumes you are using the Built-in Authentication server on the VA2410. If you are setting up EAP/PEAP on a client of an VA2410 that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.		

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 Microcell. 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 net-

work 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 <i>Public Key Authority Infrastructure</i> (PKI) server, including a <i>Certificate Authority</i> (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.
-------------	---

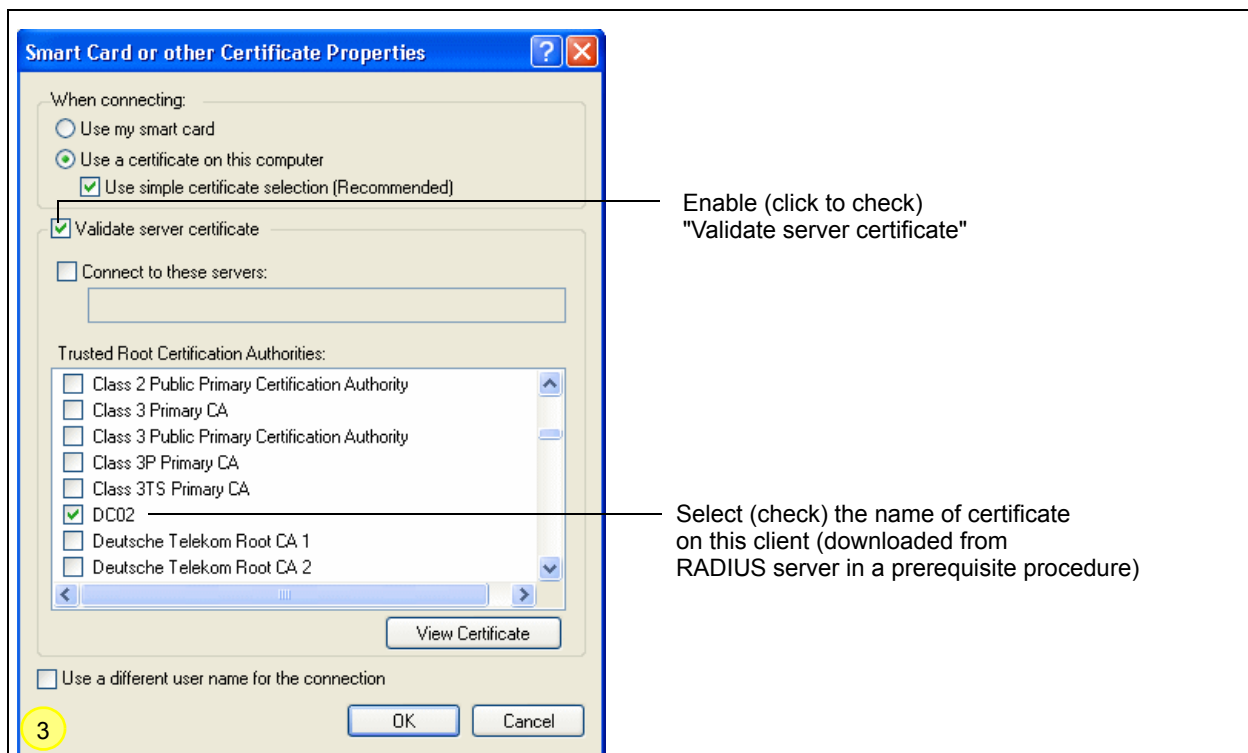
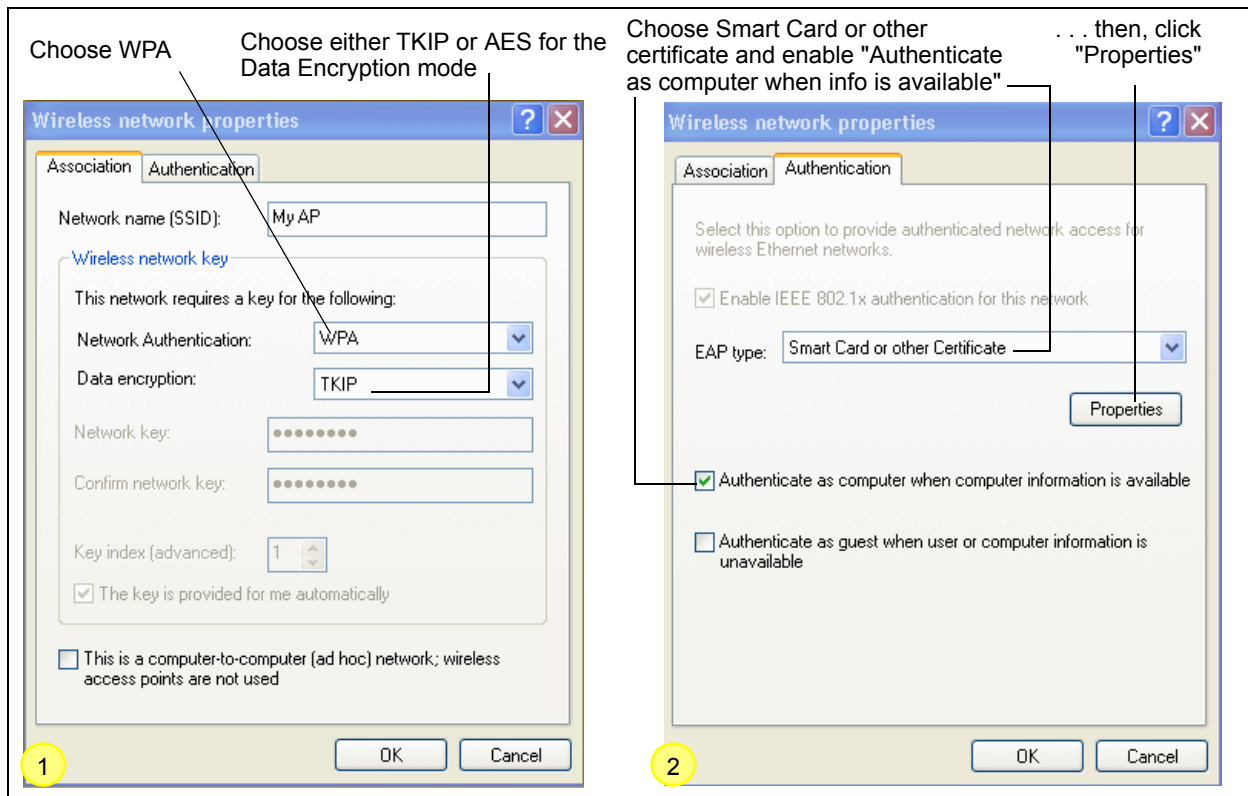
To use this type of security, you must do the following:

1. Add the Vivato 802.11b/g Outdoor Microcell to the list of RADIUS server clients. (See "Configuring an External RADIUS Server to Recognize the Vivato 802.11b/g Outdoor Microcell" on page 146.)
2. Configure the Vivato 802.11b/g Outdoor Microcell 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 149.

If you configured the Vivato 802.11b/g Outdoor Microcell 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.



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 Microcell. Note: When the Cipher Suite on the Microcell 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 Microcell. For more information, see Users Guide and Online Help on the Microcell.
--	-----------------	---

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 149.

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

WPA clients should now be able to connect to the Microcell 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 802.11b/g Outdoor Microcell 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.

Wireless network properties

Association | **Authentication**

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

OK Cancel

Choose WPA-PSK

Choose either TKIP or AES for the Data Encryption mode

Enter a network key that matches the one specified on the Microcell (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 Microcell.

Note: When the Cipher Suite on the Microcell 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 Microcell. For more information, see Users Guide and Online Help on the Microcell.

	Network Key	Provide the key you entered on the Microcell Security settings for the cipher suite you are using. For example, if the key on the Microcell 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 Microcell. 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 802.11b/g Outdoor Microcell

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 Microcell 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 802.11b/g Outdoor Microcell.

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 802.11b/g Outdoor Microcell 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 802.11b/g Outdoor Microcell as a "client" to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the VA2410. This procedure is required *per Microcell*. If you have more than one Microcell with which you plan to use an external RADIUS server, you need to follow these steps for each of those VA2410s.

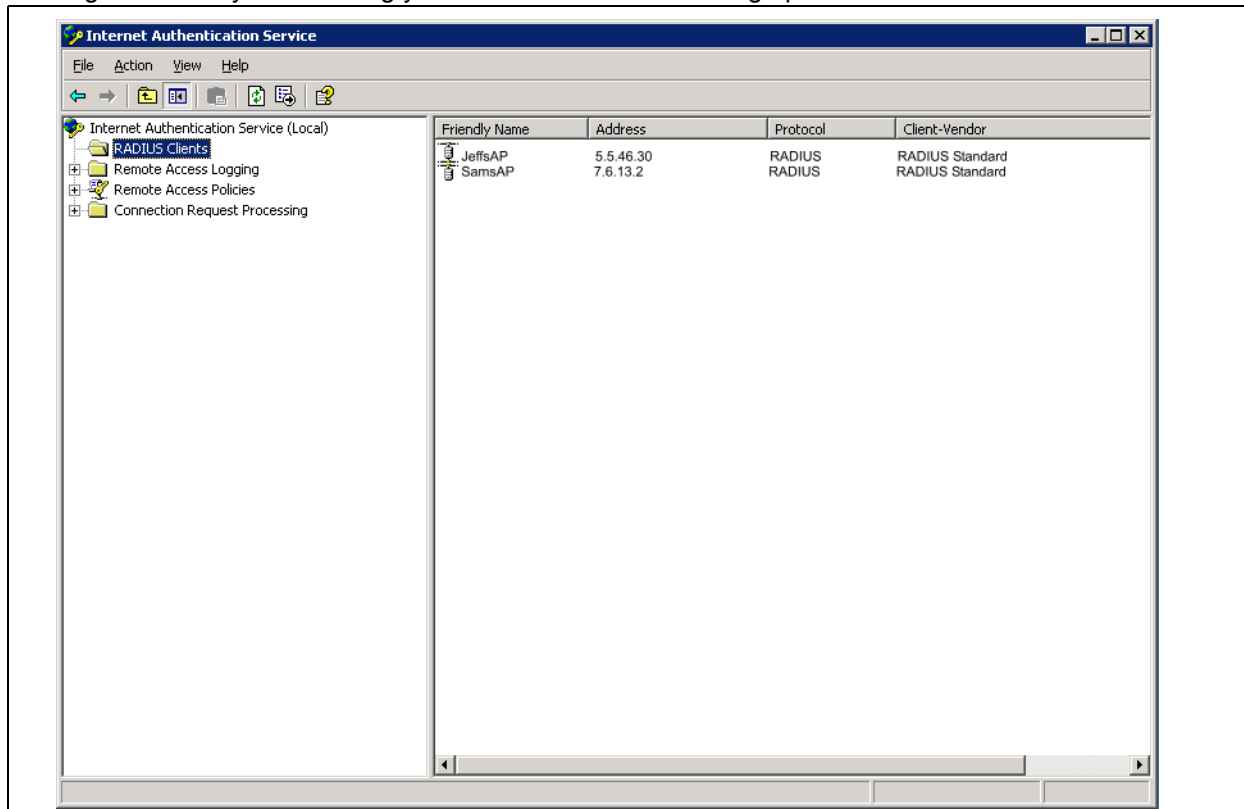
Keep in mind that the information you need to provide to the RADIUS server about the Microcell corresponds to settings on the Microcell (SSID Configuration) and vice versa. You should have already provided the RADIUS server IP Address to the VA2410; in the steps that follow you will provide the Microcell IP address to the RADIUS server. The RADIUS Key provided on the VA2410 is the "shared secret" you will provide to the RADIUS server.

The screenshot shows a configuration window with the following fields:

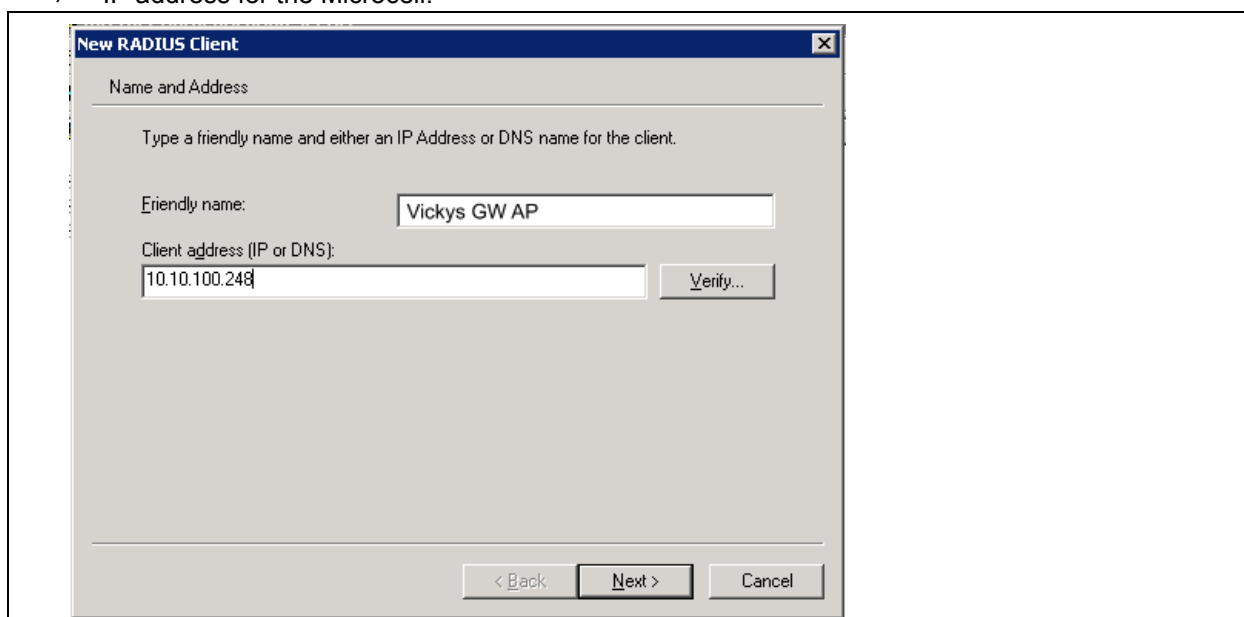
- Security Mode:** A dropdown menu currently showing "IEEE 802.1x".
- Authentication Server:** A dropdown menu currently showing "External".
- Radius IP:** Four input boxes containing the IP address "172", "254", "0", and "250" separated by dots.
- Radius Key:** A text box containing ten dots, indicating a masked password.
- Enable radius accounting:** A checkbox that is checked, with the text "Enable radius accounting" to its right.

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 802.11b/g Outdoor Microcell, the RADIUS server <i>User Datagram Protocol</i> (UDP) ports used by the Microcell are not configurable. (The Vivato 802.11b/g Outdoor Microcell 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.



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 802.11b/g Outdoor Microcell to which you want your clients to connect:
 - › A logical (friendly) name for the Microcell. (You might want to use DNS name or location.)
 - › IP address for the Microcell.



Click **Next**.

4. For the "Shared secret" enter the RADIUS Key you provided to the Microcell (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: xxxxxxx

Confirm shared secret: xxxxxxx

☐ Request must contain the Message Authenticator attribute

< Back Finish Cancel

5. Click **Finish**.

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 Microcell 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 <i>Public Key Authority Infrastructure</i> (PKI) server, including a <i>Certificate Authority</i> (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:

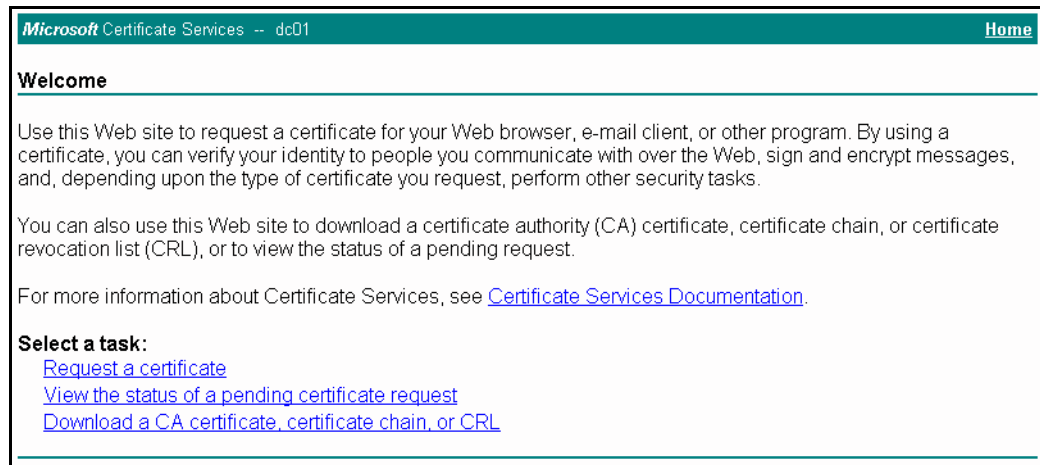
`https://IPAddressOfServer/certsrv/`

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.



The Welcome screen for the Certificate Server is displayed in the browser.

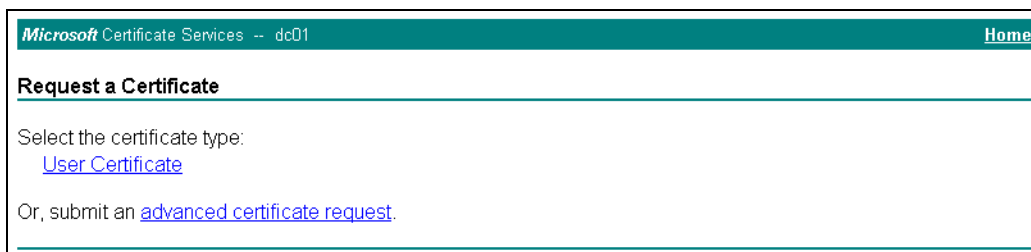


3. Click "Request a certificate" to get the login prompt for the RADIUS server.
4. Provide a valid user name and password to access the RADIUS server.

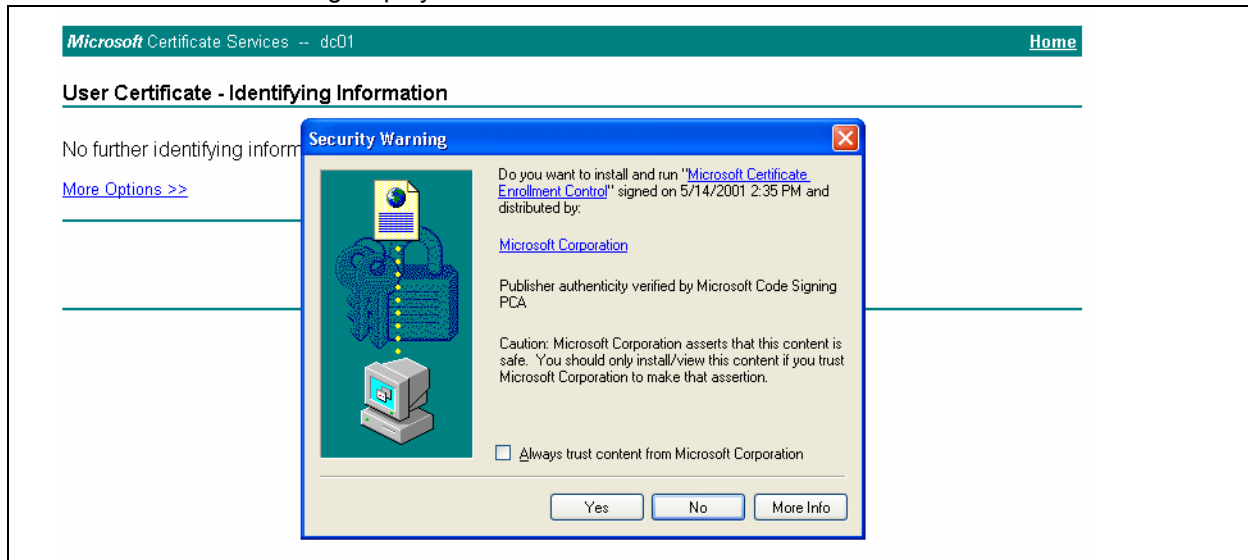


Note The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.

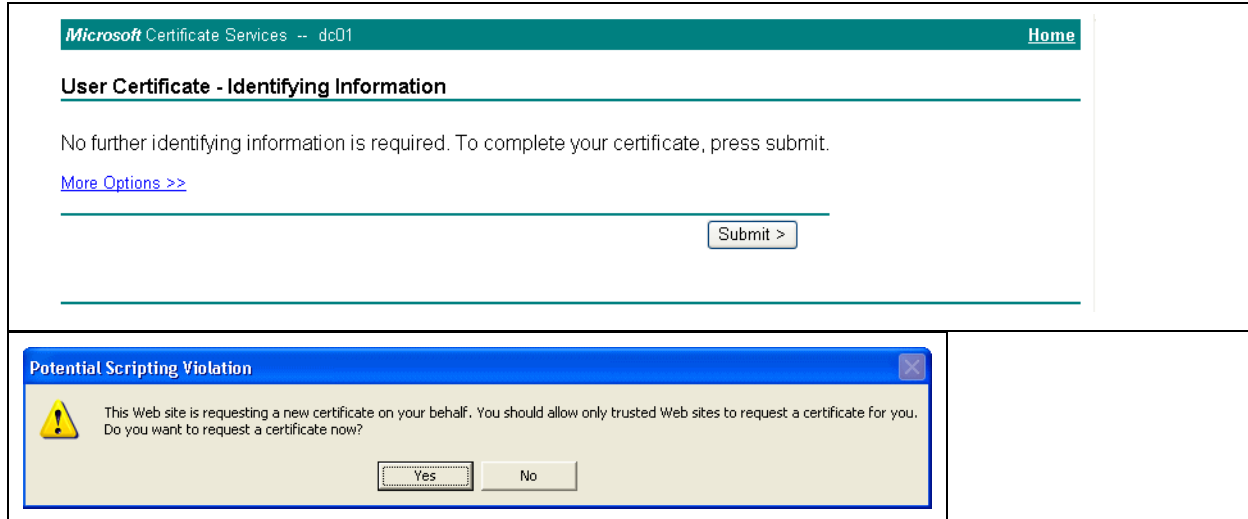
5. Click "User Certificate" on the next page displayed.



6. Click "Yes" on the dialog displayed to install the certificate.



7. Click "Submit" to complete and click "Yes" to confirm the submittal on the popup dialog.



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.)

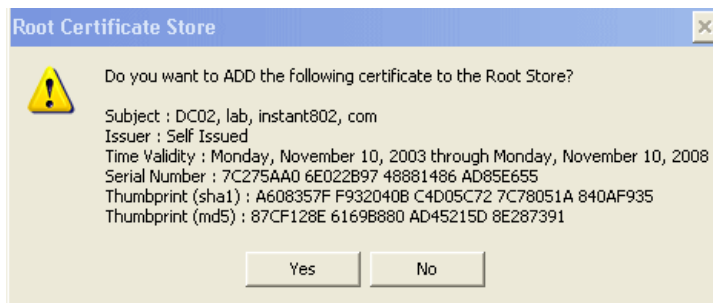
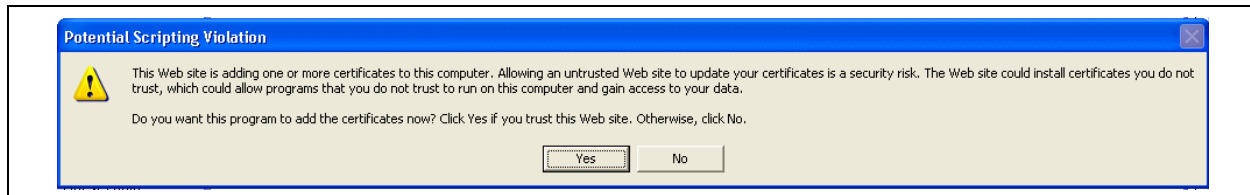
Microsoft Certificate Services -- dc01 [Home](#)

Certificate Issued

The certificate you requested was issued to you.



[Install this certificate](#)



A success message is displayed indicating the certificate is now installed on the client.

Microsoft Certificate Services -- dc01 [Home](#)

Certificate Installed

Your new certificate has been successfully installed.

Appendix B: Assessing Traffic and Interference

The Vivato Microcell 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 802.11b/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.

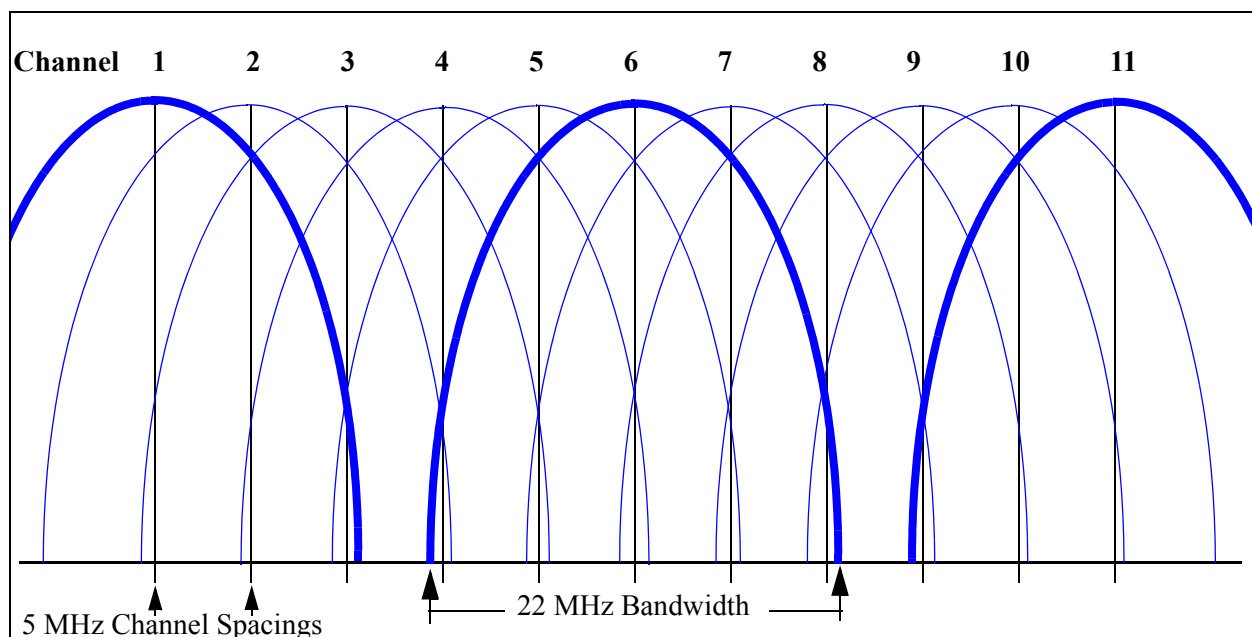


Figure 7—ISM Band Channel Spacings for Channels 1 to 11

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 Microcell or W-Fi Base Station 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 Microcell.	

Sources of Noise and Interference

Interfering signals can be broken down into four basic types: in-channel 802.11b/g signals, non-overlapping out-of-channel 802.11b/g signals, overlapping out-of-channel 802.11b/g signals, signals produced by non-802.11b/g devices.

Every 802.11b/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 802.11b/g system is using the same channel, the Microcell (and therefore the clients that it serves) must wait for a clear channel before sending data. Conversely, while the Microcell or one of its clients is transmitting, the devices on the other 802.11b/g system should withhold transmission. This reduces the total packet rate through the Microcell.

Due to a Vivato Wi-Fi Base Station's high antenna gain, the interfering signal may come from an access point (AP) or a client that is a large distance from the base station. This makes it impossible to

guarantee any level of service unless the channel assignments of all of the 802.11 devices within the coverage area can be coordinated.

The carrier sense function also applies to non-802.11b/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 802.11b/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 Microcell 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 Microcell's operation to the one remaining non-overlapped channel.

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 Microcell or angle its antennas down.

Out-of-Channel 802.11b/g Signals

Only three 802.11b/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 Microcell is set to use channel 1 on one or both wireless interfaces, a system transmitting on channel 3 would overlap its signals. The Microcell'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 both of the Microcell's wireless interfaces to channel 11 to prevent operation on channel 3 from interfering with the Microcell's operation.

Signals on a non-overlapping channel minimizes interference with operation on other non-overlapping channels. However, if other 802.11b/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 802.11b/g devices. Some of these devices occupy a single channel, while others may occupy several channels. Because these signals are not recognized as 802.11b/g signals, these signals are seen by 802.11b/g receivers as noise. As with out-of-band 802.11b/g signals, these signals can raise the level of noise high enough to reduce the SNR to unusable levels, disabling 802.11b/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 802.11b/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 $\frac{1}{2}$ 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.

Measuring Interfering Signal Levels

Two methods can be used to measure the level of noise and isolate its source: spectral analysis and the Rogue Access Points 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.

Rogue Access Points is a feature in the Vivato Microcell that displays the received signal level and channel number on each of the 6 pointing directions. Neighboring Microcells can provide very useful results by letting you know which channels are being used, their signal strengths at the Microcell, and the direction of the origin of these signals.

Using the Rogue Access Point Feature to Analyze Interfering Signals

The Microcell's Rogue Access Point feature is used when the Microcell 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 μsec) 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 access point protocol (IAPP) for AP/Bridges and Microcells (wireless hubs) in an extended service set (ESS). The standard defines how Microcells 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 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. 802.1Q 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.

Microcell

A Microcell 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 Microcell 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 Microcell 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 Microcell. 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 Microcell.

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 Microcell 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 Microcells, forming a single subnetwork that can support more clients than a basic service set (BSS). Each Microcell 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 "XbaseY", 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 Microcell 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 Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the Microcells 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 Microcells.

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 Microcell. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The Microcell is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single Microcell (BSS) or a number of Microcells (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 Microcell to a client and vice versa. It can also occur when data is transmitted from Microcell 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.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Microcell 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 Microcell 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 obscuring 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.

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 Microcell, 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 Microcell, and is especially useful for performance tuning on a Microcell 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 Microcells. 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 802.11b/g Outdoor Microcell to provide configuration control over *Quality of Service* (QoS) queues for data

transmitted from the VA2410 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 Microcell 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 802.11b/g Outdoor Microcell supports the configuration of a wireless VLAN. This technology is leveraged on the Microcell 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 Microcell is connected to a wired LAN. WDS allows Microcells to be connected wirelessly. The Microcells 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 Microcells 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 Microcell in an Infrastructure Mode network. A single Microcell creates an infrastructure basic service set (BSS) whereas multiple Microcells 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 Microcell and its clients. WME provides an interim, standards-based QoS solution. WME is not supported on the Microcell 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 73
- administrator
 - platform 26
- administrator password 71
 - on Network > Basic Settings 37
- antenna connectors 20
- associated wireless clients 76
- authentication
 - in different security modes 90
- authentication server
 - for IEEE 802.1x security mode 100
 - for WPA with RADIUS security mode 102
- Auto VLAN Settings 88

B

- backup links
 - WDS 64
- beacon interval
 - configuring 49
- bridges
 - WDS 63

C

- certificate
 - obtaining TLS-EAP certificate for client 149
 - security for IEEE 802.1x client 134
 - security for WPA with RADIUS client 140
- channel
 - configuring 49
- Channel Spacing 153
- client
 - platform 28
 - security 124
 - See also *stations* 49
- connectors 20
- Customer Support 14
- customer support 14

D

- DCF
 - as related to QoS 58
- default gateway 39
- Default Settings 25
- default settings
 - defined 25
 - resetting to 77

- DNS servers, specifying 40
- documentation feedback 14
- DTIM period
 - configuring 49

E

EAP-PEAP

- configuring on IEEE 802.1x client 131
- configuring on WPA with RADIUS client 137
- encryption in different security modes 90
- event log 74
- events
 - monitoring 74
- extended service set
 - with WDS bridging 63

F

- factory defaults
 - described 25
 - returning to 77
- features
 - overview 18
- feedback, documentation 14
- firmware
 - upgrade 78
- firmware upgrade 78
- fragmentation threshold
 - configuring 49
- front panel indicators 20

G

- gateway, default 39
- global network settings 39

I

- IEEE 802.11a
 - configuring 49
- IEEE 802.11a Turbo
 - configuring 49
- IEEE 802.11b
 - configuring 49
- IEEE 802.11g
 - configuring 49
- IEEE 802.1x radio mode
 - configuring 49

IEEE 802.1x security mode

- client configuration 131
- configuring 100
- when to use 91

IEEE rate set

- configuring 49

Interference 153

interframe spaces

- as related to QoS 58

IP address, setting 41

K

key management

- security 90

L

LED indicators 20

logging (syslog) 109, 112

logon

- administration Web pages 30

loops

- WDS 64

M

MAC filtering 54

- configuring 56

management interface, specifying 109

management password 71

manual feedback 14

Mesh Networks 114

N

neighboring access points 81

networking

- features overview 19

Noise, interfering 154

NTP server

- configuring AP/Bridge to use 47

P

password

- configuring administrator 71
- network setting for administrator 37
- on Network > Basic Settings 37

password recovery 122

PEAP

- configuring on IEEE 802.1x client 131

- configuring on WPA with RADIUS client 137

plain text security mode

- client configuration 128

- configuring 96

- when to use 90

platform

- administrator requirements 26

- client requirements 28

power connection 20

Q

QoS 57

quality of service 57

queueus

- configuring for QoS 60

R

radio 48

- configuring 49

Radio Settings 48

RADIUS server

- configuring to acknowledge AP/Bridges 146

- See also *authentication server*

recovery, password 122

remote logging 112

reset access point to factory defaults 77

rogue access points 81

RTS threshold

- configuring 49

S

security 89

- authentication server 146

- certificates on client 149

- comparison of modes 90

- configuring on the access point 95

- configuring on wireless clients 124

- features overview 18

- IEEE 802.1x 100

- plain text 96

- pros and cons of different modes 89

- static WEP 96

- WEP 96

- WPA with RADIUS 102

- WPA-PSK 107

- SNMP Network Management 110
- spanning tree protocol (STP) 64
- Spectrallink Voice Priority (SVP) 57
- starting the network 38
- static WEP security mode
 - configuring 96
 - on WDS bridge 65
 - when to use 91
- stations
 - configuring maximum allowed 49
 - See also *client*
- Support Contacts 14
- support contacts 14
- support, customer 14
- supported platforms
 - administrator 26
 - client 28
- System Recovery 122

T

- time
 - configuring an AP/Bridge to use NTP server 47
- TLS-EAP
 - configuring on IEEE 802.1x client 134
 - configuring on WPA with RADIUS client 140
 - obtaining certificate for client 149
- ToS
 - as related to QoS 58
- transmit power
 - configuring 49
- transmit/receive
 - monitoring 75
- transmit/receive information 75

U

- upgrading the firmware 78
- user accounts
 - for built-in authentication server 42
- user authentication
 - configuring on IEEE 802.1x client 131
 - configuring on WPA with RADIUS client 137
- user management 42

V

- Voice over IP
 - improved service with QoS 57

W

Warranty and End User License 3

WDS

- configuring 67

- example 68

- explanation 63

- rules 67

WDS bridging 63

WEP security mode

- client configuration 129

- configuring 96

- when to use 91

wired

- settings 39

wireless

- overview of VWBS features 17

- settings 53

wireless settings 53

WPA with RADIUS security mode

- client configuration 137

- configuring 102

- when to use 92

WPA-PSK security mode

- client configuration 144

- configuring 107

- when to use 93