

AirMagnet® WiFi Analyzer PRO

User Guide

FLUKE
networks.

© 2002-2011 Fluke Corporation. All rights reserved.

AirMagnet WiFi Analyzer PRO User Guide.

This *User Guide* is furnished under license and may be used or copied only in accordance with the terms specified in the license. The content of this document is for information only and should not be construed as a commitment on the part of AirMagnet, now part of Fluke Networks.

No part of this document may be reproduced, transmitted, stored in a retrievable system, or translated into any language in any form or by any means without the prior written consent of AirMagnet. Further, AirMagnet reserves the right to modify the content of this document without notice.

AIRMANET SHALL NOT BE HELD LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THIS CONTENT.

This product includes software developed by David Young. Copyright 2003, 2004. All rights reserved.

This product includes software developed by Atsushi Onoe. Copyright 2001. All rights reserved.

This product includes software developed by Sam Leffler, Errno Consulting. Copyright 2002-2005. All rights reserved.

This product includes software developed by Bill Paul <wpaul@ctr.columbia.edu>. Copyright 1997, 1998, 1999. All rights reserved.

This product includes software derived from Iperf Performance Test. Copyright 1999-2006 The Board of Trustees of the University of Illinois. All rights reserved.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm. Copyright 1990-1992 RSA Data Security, Inc. All rights reserved.

AirMagnet® and AirWISE® are registered trademarks, and the AirMagnet logo is a trademark, of AirMagnet. All the other product names mentioned herein may be trademarks or registered trademarks of their respective owners.

AirMagnet
2575 Augustine Drive
Santa Clara, CA 95054
USA

Compiled in the United States of America. December 2011.

Documentation ID: WFA-91-USG-01-120511

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE AIMAGNET SOFTWARE AND RETURN THE UNUSED AIMAGNET SOFTWARE WITHIN THIRTY (30) DAYS TO THE PLACE WHERE YOU OBTAINED IT FOR A REFUND.

1. GRANT OF LICENSE.

Fluke Networks, a division of Fluke Electronics Corporation grants you a non-exclusive right to install and use the full version of the AirMagnet Software on a single computer at a time for use only with the MAC address of the WiFi Card or Ethernet Interface or the unique identifier that you registered with Fluke Networks. The software and documentation accompanying this License whether on disk, in read only memory, on any other media or in any other form (the "AirMagnet Software") are licensed to you by Fluke Networks.

PLEASE NOTE: Activation of the AirMagnet Software requires a license key which Fluke Networks provides you. This license key is generated using the media access control ("MAC") address of either {a} a wireless network interface card (a "WiFi Card") connected to your computer or {b} the Ethernet interface of your computer ("Ethernet Interface") or {c} identifiers of certain AirMagnet adapters. In certain cases, the Ethernet and/or WiFi MAC address option may not be available. DURING THE INITIAL INSTALLATION OF THE AIMAGNET SOFTWARE, YOU WILL BE REQUIRED TO CHOOSE TO LOCK THIS SOFTWARE LICENSE TO THE ETHERNET INTERFACE OF A SINGLE WINDOWS COMPUTER OR TO A SINGLE WiFi CARD OR TO THE UNIQUE IDENTIFIER. THIS CHOICE IS PERMANENT AND CAN NOT BE CHANGED.

You acknowledge and agree that the AirMagnet Software is only authorized for use with the MAC address of the WiFi Card or the Ethernet Interface of your computer or the unique identifier that you registered with Fluke Networks, the licensing mechanism of the

AirMagnet Software prevents use of the AirMagnet Software with other MAC addresses or unique identifiers, and you will not in any way attempt to circumvent the licensing mechanism of the AirMagnet Software. You also acknowledge and agree that to ensure authorized use as described above, each time you use the AirMagnet Software, Fluke Networks may track the following information: your Ethernet and wireless addresses; unique identifier, user, system and domain names; date and time the AirMagnet Software launched; product serial number and serial key. Fluke Networks will not share this information with third parties except with third parties who perform services for it or if compelled by law, if necessary to protect and defend Fluke Networks rights or property or to act in an emergency to protect someone's safety.

2. TITLE, COPYRIGHT AND TRADEMARK.

Software is owned by Fluke Electronics Corporation and is protected by United States copyrights laws and international treaty provisions. Therefore you must treat the Software like any other copyrighted material. You own the media on which the AirMagnet Software is recorded but Fluke Network's and/or Fluke Networks' licensor(s) retain title to the AirMagnet Software. The AirMagnet Software in this package and any copies which this License authorizes you to make are subject to this License.

3. PERMITTED USES AND RESTRICTIONS.

This License does not allow the full version or the limited version of the AirMagnet Software to exist on more than one computer at a time. You may make one copy of the AirMagnet Software in machine-readable form for backup purposes only. The backup copy must include all copyright information contained on the original. Except as expressly permitted in this License, you may not decompile, reverse engineer, disassemble, modify, rent, lease, loan, sublicense, distribute or create derivative works based upon the AirMagnet Software in whole or part or transmit the AirMagnet Software over a network. For certain AirMagnet software products, you may be entitled to a "viewer-only" software license in addition to the full-version of the software to allow you to view information generated by the full-version software on a separate Windows computer.

You may not disclose any information relating to the performance or operation of the AirMagnet Software (including any benchmarking or other testing results) to any third party without Fluke Networks' express prior written consent. You may, however, transfer your rights under this License, provided that you transfer the related documentation, this License and a copy of the AirMagnet Software to a party who agrees to accept the terms of this License and destroy any other copies of the AirMagnet Software in your possession. You acknowledge that the AirMagnet Software contains or is provided with copyrighted software of Fluke Networks' suppliers as identified in associated documentation or other printed materials ("Third Party Software") which are obtained under a license from such suppliers. Your use of any Third Party Software shall be subject to and you shall comply with the applicable restrictions and other terms and conditions set forth in such documentation or printed materials. You may not use or otherwise export or re-export the AirMagnet Software except as authorized by United States law and the laws of the jurisdiction in which the AirMagnet Software was obtained. In particular, but without limitation, the AirMagnet Software may not be exported or reexported (i) into (or to a national or resident of) any U.S. embargoed country or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders. By using the AirMagnet Software, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

4. TERMINATION.

Your rights under this License will terminate automatically without notice from Fluke Networks if you fail to comply with any term(s) of this License.

PLEASE NOTE: If Fluke Networks discovers or has reason to believe that you have breached your obligations under this License, including but not limited to your unauthorized use of the AirMagnet Software, Fluke Networks reserves the right in its sole discretion to (1) disable your access to any copies of AirMagnet Software in your possession or under your control and (2) seek monetary damages against you up to the maximum amount permitted by law. In

connection with any such breach or suspected breach, you will pay all costs, expenses and fees (including but not limited to reasonable attorneys' fees and auditing fees) incurred by Fluke Networks in its enforcement of this provision.

5. LIMITED WARRANTY.

Fluke Networks warrants the media on which the AirMagnet Software is recorded to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of original retail purchase. Fluke Networks does not warrant any downloading errors or that the Software will be error free or operate without interruption. Fluke Networks' entire liability and your exclusive remedy under this paragraph shall be, at Fluke Networks' option, a refund of the purchase price of the product containing the AirMagnet Software or replacement of the AirMagnet Software which is returned to Fluke Networks or an authorized representative with a copy of the receipt. This limited warranty is void if failure of the products has resulted from accident, abuse, or misapplication. Any replacement product will be warranted for the remainder of the 90 day original warranty period or 30 days, whichever is longer.

6. DISCLAIMER OF WARRANTY ON AIMAGNET SOFTWARE.

Other than as provided in the Limited Warranty above, the AirMagnet Software is provided "AS IS" and without further warranty. FLUKE NETWORKS EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE AIMAGNET SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE AIMAGNET SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE AIMAGNET SOFTWARE WILL BE CORRECTED. FURTHERMORE, FLUKE NETWORKS DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE AIMAGNET

SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY FLUKE NETWORKS OR A FLUKE NETWORKS AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL FLUKE NETWORKS BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Fluke Networks' total liability to you for all damages exceed the amounts paid by you hereunder.

8. GOVERNMENT END USERS.

AirMagnet Software is a "commercial item," "commercial computer software" and/or "commercial computer software documentation." Consistent with DFAR section 227.7202, FAR section 12.212 and other sections, any use, modification, reproduction, release, performance, display, disclosure or distribution thereof by or for the U.S. Government shall be governed solely by the terms of this License and shall be prohibited except to the extent expressly permitted by the terms of this License.

9. CONTROLLING LAW AND SEVERABILITY.

This License shall be governed by the laws of the United States and the State of Washington, U.S.A., without reference to its conflict of law principles. The United Nations Convention on the International Sale of Goods shall not apply to this License. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

10. COMPLETE AGREEMENT.

This License constitutes the entire agreement between the parties with respect to the use of the AirMagnet Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Fluke Networks.

Table of Contents

Software License Agreement	i
Chapter 1 Introduction	1
Product Overview	1
AirMagnet WiFi Analyzer Express vs. PRO	2
Main Features	5
Automatically Detect Rogues and Network Vulnerabilities	5
Lockdown Security Policies	6
Perform Live, Interactive Network Tests	6
Perform Continual WiFi Interference Analysis	6
Detailed Packet and Frame Analysis	7
Access the AirMagnet AirWISE® Expert	7
Monitor 802.11n Networks	7
Generate Compliance Reports with AirMagnet WiFi Analyzer PRO	7
Advanced Features with AirMagnet WiFi Analyzer PRO	8
Multiple Form Factor Support	8
802.11n Tools	9
Integration with Windows Wireless Configuration	10
How-To Guide	10
What's New	10
One Touch Connection - Multiple Destinations	10
PCI Compliance Report	10
System Requirements	10
Laptop/Notebook/Tablet PC	11
Apple® MacBook Pro	11
NetBook	12
Fluke Networks OptiView® Series II/III Integrated Network Analyzer	13
Fluke Networks OptiView® XG Network Analysis Tablet	13
Supported WiFi Cards	14

Chapter 2	Getting Started	15
Chapter Summary	15	
Checking Product Package Contents	15	
Product Registration	16	
Preparing for Software Installation	16	
Verify System Requirements	17	
Before you begin	17	
Product Upgrades	17	
Software License	18	
Obtaining a Software License	18	
Binding the License to a MAC address	18	
MAC Address Reset	19	
Backing-up the License File	19	
Supported Wi-Fi Adapters	19	
Support Contract Activation	20	
Installing AirMagnet Software	20	
Upper-layer decode support	21	
Launching the Application for the First Time	22	
License Method	22	
Bind the License to a MAC address	22	
Supply the Serial Number and Serial Key	22	
Special Note for Windows XP Users	24	
Utilizing Multiple Wireless Adapters	24	
Updating Wireless Networking Device Vendor List	27	
Integration with Windows Wireless Configuration	30	
Creating Wireless Configuration on Windows XP	30	
Modifying Wireless Network Security Attributes on XP	34	
Creating Wireless Configuration on Windows Vista and Windows 7	35	
Creating Network Connections in AirMagnet WiFi Analyzer	40	
Modifying Network Connection in Windows Vista and Windows 7	42	
Technical Support	44	
Support Contracts	44	
Contact Customer Support	45	
AirWISE Community	45	
Chapter 3	System Navigation	47
Chapter Summary	47	

Launching AirMagnet WiFi Analyzer.....	48
Navigation Bar	48
View Filter.....	50
Applying Filters.....	51
Channel Tab	51
SSID Tab.....	51
Device Tab	51
AirWISE Tab	51
How-To Guide.....	52
Toolbar	53
Working on Start Screen.....	57
WiFi Dashboard	58
Start Screen UI Components	59
Toolbar Options	60
Text-Search Tool.....	60
Easy View Button	60
OK/R(ogue) Buttons	61
Dashboard Selection.....	61
Tabbed View	62
RF Signal Meter.....	62
RF Signal Quality Codes	63
Expanded RF Graphs	64
802.11n 20-/40-MHz Channels	65
802.11 Information	66
AirWISE Advice	67
Packet Frames Summary.....	67
Device Data	69
Locating a Wireless Device from the Start Screen.....	77
Using Bubble Help	78
AirWISE Details	79
Changing Operating Frequency	79
802.11 Protocols and Operating Frequencies	80
FCC 4.9-GHz Mode.....	81
Changing RF Signal Unit of Measurement.....	81
Worldwide 802.11 a/b/g/n Radio Channel Allocation.....	82
Accessing Data Reports.....	83

Working on Channel Screen.....	83
Channel Utilization and Throughput.....	84
Channel Selection Pane.....	84
Link Speed and Media Type	86
Channel Data Summary.....	86
Device Data Graph.....	87
Analyzing Channel Occupancy	88
Working on Interference Screen.....	90
Interference Score	92
Channel Interference Calculation.....	92
Channel Interference Summary	95
Interfering Devices.....	98
Hidden Devices	99
Graph Pane	99
AirMagnet Spectrum Analyzer Integration	100
RF Spectrum Interferers.....	103
AirMagnet Spectrum Analyzer Graph	103
Working on Infrastructure Screen.....	104
Network Tree Structure	105
Network Infrastructure Color Codes.....	106
Analyzing Data of Individual Devices.....	106
The Infrastructure Data Graphs.....	106
Infrastructure Data Summary	107
Infrastructure Data Pie Chart.....	108
Alarm Status	109
802.11d/h Information	109
Viewing Connections between Devices.....	109
Peer-to-Peer Connections.....	110
Peer-AP-Peer Connections.....	110
Working on AirWISE Screen.....	112
AirWISE Screen Viewing Options	113
Managing Alarm List	114
Analyzing Network Policy Alarms.....	114
Expert Advice	116
Data Analysis.....	116
Viewing All Alarms Generated by a Specific Device	117

Working on Top Traffic Analysis Screen	118
Top Traffic Analysis Screen UI Components	119
Viewing Device Charts	120
Exporting Chart Data	122
Choosing a Graph Option	123
Chart Data Tabulation	123
Viewing Compliance Charts	124
Basel II	125
DOD 8100.2	125
EU-CRD	125
FISMA	126
GLBA	126
HIPAA	126
ISO 27001	127
PCI DSS	127
SOX	128
Viewing Compliance Charts	128
Viewing Compliance Reports	129
Compliance Reports Disclaimer	129
Working on Decodes Screen	129
Add/Remove Columns	131
Filtering Packet Captures	133
Creating a New Filter	133
Applying a Filter	134
Deleting a Filter	134
Conducting Packet Decoding	135
Finding Packets on Decodes Screen	137
Working on Roaming Analysis Screen	137
Device Listing	138
Roaming Event Filter	140
Roaming Pie Chart	141
Analyzing Roaming Details	142
Roaming Instance Table	143
Determining the Roaming Cause	144
Roaming Reasons	145
Device Parameters	146

AP Parameters	147
Channel Parameters	148
Voice Delay	149
Packet Chart	150
Delay Analysis.....	150
Packet Decodes	152
Multiple Adapters	153
Chapter 4 System Configuration	161
Chapter Summary.....	161
Configuring a System Profile	162
Creating a New Profile	162
Exporting a System Profile.....	164
Importing a System Profile.....	165
Packet Capture	165
Configuring General System Settings.....	166
Customizing Event Log Options.....	169
Integration with Windows Wireless Configuration.....	170
Creating Wireless Configuration on Windows XP	170
To create a wireless configuration on Windows XP:.....	171
Modifying Network Security Attributes on XP	174
Creating Wireless Configuration on Windows Vista	175
To use wireless configuration on Windows Vista operating system:	175
Creating Network Connections in AirMagnet WiFi Analyzer:	178
To create network connection from AirMagnet WiFi Analyzer:	178
Modifying Network Security Attributes in Windows Vista	181
To modify a network connection from AirMagnet WiFi Analyzer.....	181
Configuring 802.11 Settings.....	184
Configuring Authentication Mechanisms	187
Configuring WEP settings	189
Configuring LEAP	190
Configuring Advanced Driver Settings	191
Wireless LAN Card RF Calibration	192
RF Calibration in AirMagnet WiFi Analyzer	192
How to Use RF Calibration Options in AirMagnet WiFi Analyzer.....	193
No Calibration	193

Pre-Defined Calibration	194
Custom Calibration.....	196
Configuring Packet Capture Filters.....	198
Setting Up a New Filter	199
Removing an Existing Filter.....	200
Install 3rd Party Decodes Engine.....	201
Configuring Channel Scan Settings	201
Configuring Channel Scanning for Multiple Adapters	204
Scanning Extended 802.11a Channels	205
Configuring System Address Book.....	207
Creating an Address Book.....	207
Removing an Entry from the Address Book.....	210
Adding Site Information	210
AP Grouping.....	212
Auto Group Rules.....	213
Manual Group Rules	214
Customizing the User Interface	216
Chapter 5 Managing Network Policies.....	219
Chapter Summary.....	219
The Policy Management Screen.....	220
The Policy Tree	221
The Policy Description	221
Managing Network Policy Profiles	221
Creating New Policy Rules.....	221
Modifying Existing Policy Rules	225
Deleting an Existing Policy Rule	226
Assigning Notifications to Policies	227
Adding Notification Options to an Alarm	227
Modifying Alarm Notification Options	231
Deleting Existing Alarm Notifications	234
Assigning Policies to ACL or SSID Groups	235
Assigning Policies to ACL Groups	235
Adding Devices to an ACL Group	238
Assigning Policies to SSID Groups	241
Assigning Policies to Existing SSID Groups	241
Modifying Existing SSID Groups	242

Creating a New SSID Group	243
Deleting an Existing SSID Group.....	243
Working with the Policy Wizard	244
Configuring Policies with the Policy Wizard.....	244
Working with the Notification Wizard	249
Assigning Notifications to Policy Alarms	250
Other Controls on Policy Management Screen	252
AirMagnet Policy Management Procedures	253
Chapter 6 WLAN Management Tools.....	255
Chapter Summary.....	255
802.11n Network Tools.....	256
802.11n Efficiency	256
802.11n Analysis	260
Simulating WLAN Throughput	262
Configuring WLAN Throughput Simulator.....	263
Conducting WLAN Throughput Simulations	263
Simulated WLAN Throughput	266
Calculating Device Throughput	268
Analyzing WLAN RF Conditions.....	272
Signal Coverage Tool.....	272
Configuring Signal Coverage Tool Settings.....	273
Measuring Site RF Signal Coverage	274
Signal Distribution Tool	276
Configuring Signal Distribution Tool Settings.....	276
Conducting a Signal Distribution Test	277
Site Survey Tool.....	278
Configuring Site Survey Tool	280
Conducting WLAN Site Survey	281
Configuring Roaming Controls.....	282
WLAN Connection Tools	284
Diagnosing Network Connectivity Issues	285
One-touch Connection Test Tools	287
Configuration	288
Generate Report	288
Connection Test Config Screen	289
Multiple Destinations	289

Using the Ping Tool	289
Verifying the DHCP Acquisition of IP Address	290
Using the Trace Tool	290
Using the FTP Tool	291
Using the HTTP Tool	292
Roaming Tool	293
Configuring Roaming Tool Settings	293
Conducting a Roaming Test	294
Additional WLAN Tools	295
Throughput/Iperf Tool	296
Downloading and Installing Iperf Software	296
Analyzing Network Bandwidth and Throughput with Iperf	299
Using Advanced Iperf Properties	301
Find Tool	304
Locating Rogue Devices	304
Jitter Tool	306
Configuring Jitter Tool	307
Conducting a Signal Jitter Test	308
GPS Tool	310
Configuring the GPS Log Tool	310
Collecting GPS Data	312
Chapter 7 Managing Data Files	315
Chapter Summary	315
Saving Captured Data	316
AirMagnet-supported File Formats	316
Saving a New File	317
Saving an Existing File in a Different Name or Format	317
Opening a Saved File	318
Viewing Recently Opened Files	321
Exporting Database Files	322
Chapter 8 Managing WLAN Reports	327
Chapter Summary	327
AirMagnet WiFi Analyzer WLAN Reports	328
Reports Screen UI Components	329
Compiling a Report Book	330

Adding Reports to Book	332
Adding an Open Report to Book	333
Dragging Default Reports to Book.	333
Adding Custom Reports to Book	333
Modifying Book Properties	335
Modifying Report Properties.	336
Deleting Reports from a Report Book	337
Printing Out Reports.	338
Exporting a Report or Report Book	339
Searching Text through a Report.	339
Chapter 9 Scanning 4.9-GHz Spectrum	341
Chapter Summary.	341
About the 4.9-GHz Band.	342
Monitoring 4.9-GHz Band.	342
Supported 4.9-GHz Wireless Network Adapters	343
Setting AirMagnet WiFi Analyzer in 4.9-GHz Mode	343
Chapter 10 Solving 802.11n Issues	347
Chapter Summary.	347
How to Find Out 802.11n Features on an AP?.	349
What 802.11n Features Are Not Used on an AP or STA?	351
What Happens If a Particular 802.11n Feature Is (Not) Used?	352
How Much Traffic Is Sent Using 40-MHZ Channel Width?.	353
What Channel Settings Should I Use If I Have a New AP?	354
How to Find Out the Maximum Throughput of an Installed AP?.	356
Why Am I Not Getting the Expected Throughput from an AP?.	357
What Is the Expected Device Throughput for an AP?	359
What Should Be Taken into Consideration When Configuring New APs?	361
What Change in Network Throughput Is Expected When Deploying New APs and/or STAs on the Network?	362
How to Find Out the Network Throughput Between an AP and a STA?	364
How Can I Know If My 802.11n AP is Associated with Any Legacy Devices? .	365
How Much Overhead Does an 802.11n AP Use to Support Legacy Devices? .	367
How Will Associated Legacy Devices Decrease 802.11n Device Throughput? .	368
How Many Legacy APs Can be Added to an 802.11n Network?	369
How Will 802.11n STAs Affect an Existing 802.11a Network?	371

Chapter 11	Integration with Fluke INA	373
Chapter Summary	373	
Fluke Networks OptiView® Integrated Network Analyzer	373	
Software Installation	375	
Supported Wireless Network Adapters	375	
Software Usability	375	
Using Tap and Hold	375	
Using the Full Screen/Restore Screen Button	376	
Using the MyTTouch Soft Keyboard	378	
Miscellaneous UI Changes	378	
Chapter 12	Analyzing WiFi Roaming	379
Viewing Wireless Roaming	379	
Device Listing	380	
Roaming Event Filter	381	
Roaming Pie Chart	382	
Analyzing Roaming Details	383	
Roaming Instance Table	384	
Determining the Roaming Cause	385	
Roaming Reasons	386	
Device Parameters	387	
AP Parameters	388	
Channel Parameters	388	
Voice Delay	389	
Packet Chart	389	
Delay Analysis	390	
Packet Decodes	392	
Appendix A	Abbreviations & Acronyms	393
Appendix B	Glossary	397
Appendix C	Third-Party Copyrights	411
Iperf Copyright	411	
D. Young Copyright	412	
A. Onoe & S. Leffler Copyright	413	
S. Leffler Copyright	414	
B. Paul Copyright	415	

Appendix D Upper-layer decode support license	417
Index	431

Chapter 1: Introduction

Product Overview

802.11-based wireless local area networks (WLANs) have quickly emerged as one of the most important assets in the enterprise networking technology landscape. Low ownership costs and the need to extend existing wired networks to a rapidly growing mobile user base have fueled the adoption of WiFi across all industries. With the IEEE's imminent ratification of the 802.11n standard – the next generation of WiFi which promises more than five times the throughput and twice the range of the current 802.11g standard – the demand for wireless networking will become even greater and widespread. However, much like the evolution of the Ethernet in its early days, the rate of 802.11 implementations has outpaced the development of professional tools and practices needed to properly manage the WLAN. As a result, IT and network security professionals suddenly find themselves in a situation where they have to deal with an ever-increasing influx of network security and performance issues with outdated tools originally designed for the wired network.

Unlike their wired counterparts, WLANs are rather fluid and have virtually no physical boundaries. As such, IT and network security professionals are in dire need of tools that are specifically tailored for WLANs to help them identify and solve WLAN-specific performance and security issues in a timely manner. This is exactly what Fluke Networks AirMagnet WiFi Analyzer (AirMagnet WiFi Analyzer hereafter) is for.

Designed to make the WLAN as secure and reliable as the Ethernet, AirMagnet WiFi Analyzer brings together the industry's most advanced tools and intelligence in a single mobile application, striking the right balance among network monitoring, analysis, and diagnostics. Its core competencies include site survey and audit, connection troubleshooting, and security and performance management. At the heart of the solution lies the AirMagnet Wireless

System Expert (AirWISE) —AirMagnet’s patent-pending analytical engine—that automatically alerts IT and network professionals to more than 200 attack tools and strategies and provides context-sensitive, case-specific analysis and advice.

AirMagnet WiFi Analyzer Express vs. PRO

AirMagnet WiFi Analyzer comes in two versions: AirMagnet WiFi Analyzer Express and AirMagnet WiFi Analyzer PRO. Each requires a separate software license. While both share most of the features described in this document, AirMagnet WiFi Analyzer PRO offers many advanced features that are not available in AirMagnet WiFi Analyzer Express. The table below provides a brief feature comparison between the two:

Table 1-1: AirMagnet WiFi Analyzer Express vs. PRO

Features	Basic Features in Express and Pro	Added Features in Pro
See WiFi Devices	• See all 802.11a/b/g/n devices	<ul style="list-style-type: none">• Automatically identify and group virtual APs• Detection of device in non-standard channels• Detection of device in non-standard channels• Detection of 4.9 GHz devices• Scan 200+ channels in 5GHz spectrum• Simultaneous channel scanning based on multi-adapter support (Max. 3)

Table 1-1: AirMagnet WiFi Analyzer Express vs. PRO

Features	Basic Features in Express and Pro	Added Features in Pro
Automated Analysis - Network and Security Problems	<ul style="list-style-type: none"> • Performance and reliability alarms • Expert analysis and explanation of each alarm • Rogue AP detection • Detection of improper security settings 	<ul style="list-style-type: none"> • Automated analysis of 11n security and performance issues • Detection of intrusions, hacking tools and DoS attacks (40+ addtl. security alarms) • Detailed, professional security and regulatory compliance reports • QoS and voice analysis • How To Guide for common 11n problems
Active Troubleshooting Tools	<ul style="list-style-type: none"> • Find tool for tracking down any WiFi Device • One-Touch Connection Audit tool to verify network connectivity and application performance 	<ul style="list-style-type: none"> • Complete suite of 16 active testing and troubleshooting tools including: • 11n efficiency measurements • 802.11n analysis diagnostics • Connection Diagnostic tool • 802.11 performance calculator • 802.11 throughput simulator • Signal quality analysis • iPerf performance testing

Table 1-1: AirMagnet WiFi Analyzer Express vs. PRO

Features	Basic Features in Express and Pro	Added Features in Pro
WiFi Traffic and Device Analysis	<ul style="list-style-type: none"> • Device and channel utilization • Wireless frame decodes • Packet decodes • Frame and Traffic summary (Data vs Mgmt frames) • Basic traffic stats (signal, noise, retries) 	<ul style="list-style-type: none"> • Twice as many diagnostic charts • Frame and traffic detail - probes, beacons, acks • Twice as many available traffic stats (% errors, utilization by media, etc.) • View live frame details without stopping capture • Multiple channel simultaneous frame capture and decodes • Dedicated WLAN Client roaming analysis screen • Capture packet data to disk by three methods: Capture to disk, Use multiple capture files and Enable non-stop capture.
Interference Analysis	<ul style="list-style-type: none"> • Basic Visibility into signal and noise in the environment 	<ul style="list-style-type: none"> • Aggregate channel interference scoring • Dedicated Interference Analysis page • Integration with AirMagnet Spectrum XT, AirMagnet Spectrum Analyzer, Fluke Networks AnalyzeAir & Cisco AirMagnet Spectrum Expert • Multipath detection • Hidden node analysis by channel

Table 1-1: AirMagnet WiFi Analyzer Express vs. PRO

Features	Basic Features in Express and Pro	Added Features in Pro
Summary and Reporting	<ul style="list-style-type: none"> • Connection audit report • Basic chart of the top devices only 	<ul style="list-style-type: none"> • Top talker charts for APs, stations and channels • 50+ security, performance and device reports • Professional Compliance Reports for major regulations
RF and AirMagnet Spectrum Analysis	<ul style="list-style-type: none"> • Detect and plot noise and co-channel interference 	<ul style="list-style-type: none"> • Integration with AirMagnet Spectrum XT, AirMagnet Spectrum Analyzer, Fluke Networks AnalyzeAir and Cisco AirMagnet Spectrum Expert • Identify areas where AirMagnet Spectrum interferers were detected

Main Features

AirMagnet WiFi Analyzer is the industry's most popular mobile field tool for troubleshooting enterprise WiFi networks. AirMagnet WiFi Analyzer helps IT staff make sense of end-user complaints to quickly resolve performance problems, while automatically detecting security threats and other network vulnerabilities. Although compact, AirMagnet WiFi Analyzer has many of the feature-rich qualities of a dedicated, policy-driven wireless LAN monitoring system.

Automatically Detect Rogues and Network Vulnerabilities

AirMagnet WiFi Analyzer automatically identifies hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS, as well as dozens of wireless intrusions and hacking strategies, including Rogue devices, Denial-of-Service attacks, Dictionary Attacks, Faked APs, RF Jamming, "Stumbler" tools, and many more. AirMagnet WiFi Analyzer also offers a convenient "Find

Tool” that enables you to quickly track down rogue APs and non-complying devices that compromise network security. Also use Find Tool to align signals between antennas to quickly optimize reception in line-of-sight bridging.

Lockdown Security Policies

AirMagnet WiFi Analyzer enables you to set detailed security policies for all devices in your network. Designate your encryption and authentication methods then monitor your wireless LAN to check all devices for compliance with those policies. Also validate that the encryption methods themselves function correctly over the WLAN. Establish an even higher level of organized security by designating a list of approved APs for client access, and monitoring for exposed wireless stations, ad-hoc devices, and other vulnerabilities.

Perform Live, Interactive Network Tests

In addition to the issues that AirMagnet WiFi Analyzer automatically locates for you, a suite of active troubleshooting tools are available at your fingertips to help you quickly pinpoint network problems—RF interferences, traffic/infrastructure overloads, hardware failures, connectivity issues and more. Test connections with traditional tools such as DHCP, ping, and traceroute or use AirMagnet's Diagnostic Tool to view the step-by-step progress of a connection between a client and AP to pinpoint exactly where the process has broken down. Run AP performance tests to identify mismatched settings in the network, coverage, multi-path interference, jitter and roaming.

Perform Continual WiFi Interference Analysis

Interference can stem from a variety of sources including competition from other WiFi devices, so-called “hidden nodes” in the network, and even non-802.11 wireless devices. The AirMagnet WiFi Analyzer's Interference screen tracks all these components of interference and plainly displays them by channel. This enables you to quickly see the impact of competing WiFi devices, identify any hidden nodes affecting the channel, and track noise in the RF environment. AirMagnet WiFi Analyzer PRO users can also integrate with the [AirMagnet Spectrum Analyzer](#)* to identify non-802.11 sources of interference for even deeper Layer 1 analysis.

Note: AirMagnet Spectrum Analyzer is sold separately.

Detailed Packet and Frame Analysis

AirMagnet WiFi Analyzer shows real-time packet flows for any WiFi asset. Track data and management packets live, watch CRC errors, utilization, packet speed, media type and more. View a real-time decode page for detailed network analysis: AirMagnet WiFi Analyzer decodes the most popular protocols such as FTP, HTTP, SMTP, POP, and Telnet, with advanced filtering options that allow you to focus on particular conversations based on IP address or port number.

Access the AirMagnet AirWISE® Expert

AirMagnet AirWISE® is your encyclopedia source for understanding the threats and performance issues at work in your WiFi environment. All system alarms are explained for you in plain-English detail, including why they are important and what steps you should take to resolve issues.

Monitor 802.11n Networks

AirMagnet WiFi Analyzer identifies and classifies all 802.11n-capable devices in the network (including differentiating between standards-compliant and pre-standard 802.11n devices). It supports monitoring for 20 MHz and 40 MHz channels and also detects and classifies higher data rates used by the 802.11n devices. With AirMagnet WiFi Analyzer, users can classify and decode Non-HT (legacy) and HT mixed format traffic and identify backward compatibility issues with legacy 802.11a/b/g devices operating in the same environment. Users can locate 802.11n rogue devices, which are often invisible to non-802.11n analyzers and decode new information elements/wireless frame types.

Generate Compliance Reports with AirMagnet WiFi Analyzer PRO

AirMagnet provides detailed compliance reports for a variety of regulatory standards set by governing agencies in the respective countries. They include Sarbanes-Oxley, Basel II, EU-CRD (Cad 3), ISO 27001, FISMA, HIPAA, PCI-DSS, DoD 8100.2, and GLBA. Reports provide a step-by-step pass/fail assessment of each section of the standard, enabling you to complete work in a fraction of the time. AirMagnet WiFi Analyzer also offers an integrated reporting tool that enables you to turn your WiFi analysis sessions into

professional customized reports. Choose from a library of pre-built reports or generate your own targeted reports by selecting specific items of interest from the user interface, such as RF statistics, channel reports, device reports, or security and performance issue reports.

Advanced Features with AirMagnet WiFi Analyzer PRO

AirMagnet WiFi Analyzer PRO software version contains all the functionality of the basic AirMagnet WiFi Analyzer version plus an additional set of features tailored to the needs of the wireless expert, such as:

- 802.11n features and alarms
- Integration with Iperf
- Support for 200+ 802.11a channels
- Integration with AirMagnet Spectrum Analyzer
- 4.9 GHZ (Public Safety Band) monitoring
- Session sharing between two AirMagnet WiFi Analyzers
- Advanced Session Reporting and Compliance Reporting

Note: AirMagnet Spectrum Analyzer is sold separately.

Multiple Form Factor Support

AirMagnet WiFi Analyzer can be installed on a variety of platforms including Windows-based laptops, Tablet PCs, Apple® MacBook® Pro (with Atheros-based wireless adapters only) and Ultra Mobile PCs. UMPC support enables end-users and resellers – for the first time – to monitor, audit and troubleshoot all aspects of the WLAN with a PC that can fit in their pocket. It gives users the flexibility of walking about the physical premises to audit and troubleshoot enterprise WiFi networks using a light-weight handheld solution. AirMagnet WiFi Analyzer is supported on the OQO Model 02/e2 UMPC.

802.11n Tools

AirMagnet WiFi Analyzer 9.0 comes with 802.11n tools that allow the user to analyze the performance of the 802.11n wireless network – the next generation of wireless networking technology that offers unprecedented network throughput, range, and stability. The tools are designed to help the user to understand and troubleshoot the most common 802.11n-related issues they may encounter. The tools are:

- **Efficiency** – The 802.11n wireless network protocol introduces substantial enhancements in WLAN efficiency at both the physical (PHY) and the medium access control (MAC) layers. The Efficiency tool is intended to provide the basic knowledge that the user needs in order to take full advantage of the benefits of the 802.11n network.
- **Analysis** – The Analysis tool provides detailed explanation and analysis about the 802.11n wireless network.
- **WLAN Throughput Simulator** – The WLAN Throughput Simulator is a utility for calculating network, node and media throughput, utilization and overhead (as measured at the 802.11 Link Layer) under various network and node configurations. It allows the user to add and configure up to fifty 802.11a, 802.11b, 802.11g and/or 802.11n nodes on a “virtual channel”. The Simulator’s engine applies additional network and node parameters based upon the type and settings of the nodes present. The Simulator runs in a “perfect” environment, assuming that all nodes can “hear” each other (negating the possibility of packet collisions and frame retries) and that all nodes transmit as much (and as fast) as they possibly can (based upon their individual and overall network parameters). The result of such simulation provides a baseline measurement of the (somewhat theoretical) maximum link-layer throughput that can be achieved for a particular configuration.
- **Device Throughput Calculator** – The Device Throughput Calculator is a utility for calculating a device’s theoretical throughputs. The user simply clicks to specify the parameters such as MCS index, SGI, bandwidth, max frame size, block ACK, least capable device, and/or protection mechanism used, and AirMagnet will calculate the

maximum PHY rate, maximum data rate, percentage of overhead, the number of spatial frames, and the modulation coding rate in a flick of second. It also displays 802.11 frame exchange data in a graph which showing the percentage of DIFS, preamble/PLCP, Data, SIFS, preamble/PLCP, and ACK frames.

Integration with Windows Wireless Configuration

Allows the user to take advantage of Windows wireless profiles that have been created in Windows Vista or XP operating system and use them directly with AirMagnet WiFi Analyzer's active tools (e.g., Site Survey, Performance, Connect, Roaming, etc.).

How-To Guide

A Microsoft Office Assistant-like How-To guide that helps the user to move up to speed quickly with the major functions of the application. The Guide is available on all major user interfaces and can be accessed with a click of the button.

What's New

New features in AirMagnet WiFi Analyzer :

One Touch Connection - Multiple Destinations

For each of the One Touch Connection tests, multiple destinations may be run during the test. For example, you may run a ping test against multiple domains.

PCI Compliance Report

Payment Card Industry Data Security Standard Compliance Report (PCI) has been updated to the 2.0 standard.

System Requirements

AirMagnet WiFi Analyzer requires the following system requirements, depending on the platform being used:

[1]: 64-bit Operating System supported on Windows 7 for certain wireless adapters. Please refer to supported adapter list for more details.

[2]: Use Windows XP (SP2) if AirMagnet Spectrum Analyzer is installed and used as a standalone application on the same laptop/PC.

Laptop/Notebook/Tablet PC

- Operating Systems: Microsoft® Windows 7 Enterprise/Professional/Ultimate, Vista Business/Ultimate (SP2), XP Professional(SP3), or Microsoft Windows Tablet PC Edition 2005 (SP3);
- Intel® Pentium M 1.6 GHz (Intel Core 2 Duo 2.00 GHz or higher recommended);
- 1 GB memory (2 GB recommended) for Windows XP. 2 GB or higher required for Windows Vista and Windows 7;
- 500 MB free disk space;
- A CardBus, ExpressCard slot, USB port, or mini PCI slot (whichever applicable);
- Multiple slots in the PC when using multiple adapters. AirMagnet recommends the use of its multi-adapter kit;
- AirMagnet-supported wireless network adapter(s);
- Optional AirMagnet Spectrum adapter and license (required for viewing AirMagnet Spectrum data and non WiFi devices; AirMagnet WiFi Analyzer Pro only). Integration supported with AirMagnet Spectrum XT, AirMagnet Spectrum Analyzer, Fluke Networks AnalyzeAir or Cisco AirMagnet Spectrum Expert. Note: AirMagnet Spectrum XT adapter is in the USB form-factor, while the other AirMagnet Spectrum products are based on a CardBus (PCMCIA) adapter.;

Apple® MacBook Pro

- Operating systems: MAC OS X Leopard [running Windows XP Pro (SP3) using Boot Camp];

- Intel-based 1.26 GHz or higher (1.6 GHz or higher recommended);
- 1 GB memory (2 GB recommended)
- 500 MB free hard disk space;
- A CardBus, ExpressCard slot, USB port, or mini PCI slot (whichever applicable);
- Built-in Atheros-based Airport Extreme 802.11n wireless adapter or any AirMagnet-supported wireless network adapter (whichever applicable);
- Multiple slots in the PC when using multiple adapters. AirMagnet recommends the use of its multi-adapter kit;
- Optional AirMagnet Spectrum adapter and license (required for viewing AirMagnet Spectrum data and non WiFi devices; AirMagnet WiFi Analyzer Pro only). Integration supported with AirMagnet Spectrum XT, AirMagnet Spectrum Analyzer, Fluke Networks AnalyzeAir or Cisco AirMagnet Spectrum Expert. Note: AirMagnet Spectrum XT adapter is in the USB form-factor, while the other AirMagnet Spectrum products are based on a CardBus (PCMCIA) adapter.;

NetBook

- Operating Systems: Microsoft Windows XP™ Home; Windows 7 Home Premium & Windows 7 Starter edition
- Intel Atom N270/1.6 GHz CPU or N470 Processor (1.83 GHz, 667MHz FSB)
- 1 GB (2 GB recommended) memory;
- 500 MB free hard disk space;
- 1024X600 resolution;
- A CardBus, ExpressCard slot, USB port, or built-in slots (whichever applicable);

- Multiple slots in the PC when using multiple adapters. AirMagnet recommends the use of its multi-adapter kit;
- AirMagnet-supported wireless network adapter(s).

Fluke Networks OptiView® Series II/III Integrated Network Analyzer

- Microsoft Windows Professional (SP3);
- Intel Pentium M 600 MHz;
- 512 MB memory;
- 500 MB free hard disk space;
- One of the following CardBus adapters: AirMagnet 802.11a/b/g/n Wireless PC card, Fluke Networks 802.11 a/b/g/n, or Fluke Networks 802.11 a/b/g/n.

Multi-adapter not supported on Fluke Networks OptiView Integarted Network Analyzer.

Fluke Networks OptiView® XG Network Analysis Tablet

- Microsoft Windows 7, Professional, SP1
- Intel Pentium 1.2 GHz
- 4 GB memory
- 128 GB removable solid state drive
- 2 internal Atheros®-based 802.11a/b/g/n adapters
- 1 internal RF spectrum adapter
- 3 USB ports
- 1024 x 768 touch display

Supported WiFi Cards

An AirMagnet-supported WiFi card is required in order to operate AirMagnet WiFi Analyzer software. For a complete, up-to-date listing of AirMagnet-supported wireless adapters, visit http://www.airmagnet.com/products/wifi_analyzer/.

Chapter 2: Getting Started

Chapter Summary

This chapter discusses the following topics:

- Checking product package contents
- Preparing for software installation
- Installing the software
- Integration with Windows Wireless Configuration
- Updating wireless networking device vendor list
- Backing up your license file
- Obtaining a software license file
- Registering your product
- Seeking technical support

Checking Product Package Contents

Before you start, make sure that the following items are included in the product package:

- *AirMagnet WiFi Analyzer CD.*
- *AirMagnet Software License Agreement.*
- *AirMagnet WiFi Analyzer Read Me First.*
- A software certificate bearing the serial number and serial key of your AirMagnet product.

- If a support contract was purchased, a support contract with a support serial number and serial key.

Note: The AirMagnet WiFi Analyzer User Guide, Release Notes and AirMagnet WiFi Analyzer Policy Reference Guide in PDF format are also available on the software CD.

In case any items are missing or damaged, contact your AirMagnet authorized reseller or AirMagnet Technical Support immediately. See “[Technical Support](#)” on page 44.

Product Registration

It is highly recommended that you create a MyAirMagnet account and register your AirMagnet software. By registering your purchased software, you are entitled to a free MyAirMagnet.com account with the following benefits:

- Users can download software updates/upgrades to the software when available.
- Access product documentation (FAQs, best practices, release notes, user guides, etc.)
- Download wireless adapter drivers.
- Access technology notes/white papers.
- Access to AirMagnet forums.
- Access training program options.

To register your product and create a MyAirMagnet account, go to:

http://airmagnet.flukenetworks.com/support/register_product

Preparing for Software Installation

It is strongly recommended that you review this information before starting product installation.

Verify System Requirements

Be sure that the computer you plan to install the software on complies with the system requirements. See “[System Requirements](#)” on page 10.

Before you begin

The following are a few things to consider before installing, launching and using the software:

- Be sure to have active Internet connection when launching the software for the first time.
- The user must have administrative rights on the machine running AirMagnet software.
- Be aware certain firewall settings or antivirus software may interfere with the AirMagnet software.
- Network software that utilizes a wireless adapter may cause a conflict with AirMagnet software.

Product Upgrades

If the machine running the software application has an active Internet connection and a product upgrade is available, a notification dialog will be displayed during product launch indicating that a newer version of the software is available. Click **Yes** to proceed to your MyAirMagnet account where you can access the software upgrade download. The product upgrade will be listed in Registered Products / Downloads section under Software Download.

An active support contract is required in order to upgrade from an older version to a newer version of the product. All existing customers wishing to install a newer release of the product should verify the status of their product support contract before starting the installation.

The status of your support contract may be viewed under the Registered Products section of your MyAirMagnet account. See “[Product Registration](#)” on page 16. For information about support contracts, see “[Technical Support](#)” on page 44.

Software License

You will be required to install a unique software license in order to successfully run the software application. You will be prompted to install the license when the product is launched for the first time.

Obtaining a Software License

Your Software License Certificate includes a Serial Number (S/N) and a Keycode (Serial Key). When the application is launched for the first time, you will be required to supply this information to proceed. This Serial Number / Serial Key combination enables you to obtain a software license compatible with the software version of your product and in accordance with your support contract.

Once you enter the Serial Number and Serial Key, you will be prompted to obtain the license:

License Download: If the machine is connected to the Internet, you may choose to obtain the license by download. In this case the system will automatically download the license and install it.

Browse to License: If the license is accessible on your network (previously downloaded), you may choose to browse to it. The name of the license file is “serial number.lic”

For example: A1150-04280450.lic.

The license will be copied to your AirMagnet product directory.

For example: c:\Program Files\AirMagnet Inc\AirMagnet Laptop.

Binding the License to a MAC address

Note: Binding the license step is not applicable to users of Fluke Networks OptiView XG Network Analysis Tablet.

AirMagnet mobile products permits one software license per MAC address. The license may be bound to a specific machine (laptop) or to a removable wireless adapter. This provides flexibility in how the product may be used and shared.

During product installation, you will be prompted to choose which option to use. Depending on your choice, the application automatically captures the MAC address of the machine or adapter.

Note: If you choose to bind the software license to a removable adapter, the adapter must be active on the machine at the time you launch the application.

MAC Address Reset

Should you desire to reset the MAC address to a different machine or adapter, you may request a MAC address reset by choosing “Mac Address Reset” from your MyAirMagnet account.

Backing-up the License File

It is strongly recommended that you register your product, download the license file and save it in a safe location. Having a backup license file makes it easy to reinstall the application anytime, if needed because you can simply browse to the file to install it.

Supported Wi-Fi Adapters

AirMagnet WiFi Analyzer and AirMagnet Survey requires a supported WiFi adapter be operating on the machine running the application in order to capture WiFi data.

AirMagnet mobile products categorizes supported WiFi adapters into two types: preferred adapters and limited support adapters.

Preferred Adapters: these adapters have been comprehensively tested by the AirMagnet support team and are recommended for use with AirMagnet products. The list of preferred adapters and driver packages is located under the Documents/Drivers section of your MyAirMagnet account.

Limited Support Adapters: These adapters have been known to work with AirMagnet products, however, they have not been extensively tested. Fluke Networks recommends using preferred adapters with AirMagnet products.

A complete, up-to-date listing of AirMagnet-supported wireless adapters is located here:

http://www.airmagnet.com/support/supported_adapters/

Support Contract Activation

If you purchased a support contract for your product, you will need to activate the contract.

- When launching the product for the first time: You will be prompted to supply the support contract serial number and serial key.
- To add a new support contract to an existing software license, register your product. In the Registered Products / Downloads section of your MyAirMagnet account, under Product Version, click “Register Support Contract.” You will be prompted to enter the support contract serial number and serial key.

Note: The support contract serial number and serial key is not the same as your product serial number and serial key.

Installing AirMagnet Software

AirMagnet software is available two ways:

- On the CD that is shipped to the customer.
 - As a download from your MyAirMagnet account under Registered Products. If you have a current support contract, the download will be the most current version of the product, otherwise it will be the version you are entitled to download.
- 1) Run the application installer:
- **CD installation:** Insert the CD in the PC's CD-ROM drive. If autorun is enabled on your machine, the installer should begin automatically. If autorun is disabled, double-click the Autorun.exe file.

- **Download installation:** From the Registered Products page of your MyAirMagnet account, click the software download and run or save the file. If the file was saved, double-click the .exe file to begin running the installer.
- 2) Agree to the Software License Agreement. To proceed with installation, you must agree to the Software License Agreement. See “[Software License Agreement](#)” on page i.
 - 3) Set the installation destination folder. Accept the Program Files default or browse to a different location.
 - 4) Click Finish to complete the installation. At this point you may select another option from the installer or click Exit to close the installer.

Upper-layer decode support

AirMagnet WiFi Analyzer provides a 3rd party decodes engine feature that will decode the upper layers of your capture files. You may choose to install this feature as part of product installation.

To install the 3rd party decodes engine:

- 1) During software installation, you will be presented with an option to install 3rd Party Decodes. Click Yes. See [Figure 2-1](#).

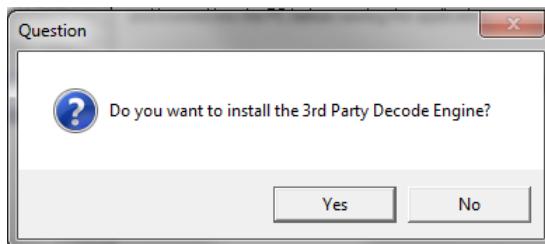


Figure 2-1: Installing 3rd party decodes

- 2) You must agree to the GNU Library General Public License to proceed with 3rd party decodes installation. See “[Upper-layer decode support license](#)” on page 417.

- 3) You may also choose to permit everyone who uses the computer to access this feature.

Note: Should you choose not to install 3rd party decodes at this time, you may choose to install it from within the application in the Configuration dialog>Filter tab.

Launching the Application for the First Time

When you launch the application for the first time, you will need validate your license and install it.

License Method

Choose which method to use for installing the software license:

- **Download the license:** you must be connected to the Internet and have an active Internet connection.
- **Browse to a license:** You will be prompted to browse to the file.

For more information about license, see “Software License” on [page 18](#).

Bind the License to a MAC address

Choose to bind the license to either the MAC address of the machine running the application or to the MAC address of a removable WiFi adapter. To bind the license to a WiFi adapter, it must be active on the machine running the application. See “Binding the License to a MAC address” on [page 18](#).

Note: Binding the license step is not applicable to users of Fluke Networks OptiView XG Network Analysis Tablet.

Supply the Serial Number and Serial Key

When launching the software for the first time, you will also be required to supply a valid serial number and serial key. If you have a support contract for this product, you should also supply it here.

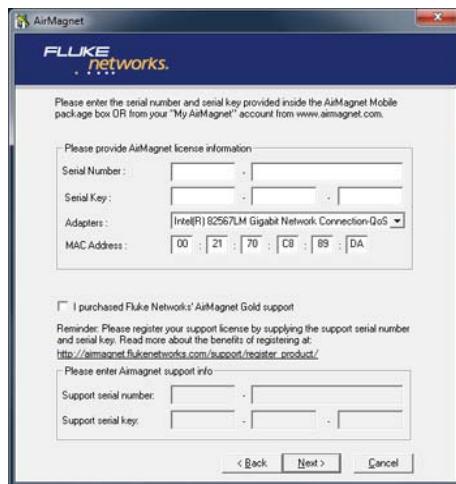


Figure 2-2: Serial Number validation

If the license file does not support the installed version of the product, an error message will be displayed indicating “Invalid License File” or “This serial number is currently out of support.”

If you receive an error when attempting to install the software license. Here are a couple reasons the license selection may produce an error message along with what you can do:

- Your license does not support a newer version of the product. In this case, you may purchase a support contract that entitles you to run the newer software. See “[Technical Support](#)” on page 44.
- The license file you chose is for a different product. Verify that the license file name has the same serial number as the serial number for your product. See “[Obtaining a Software License](#)” on page 18.

If you receive an “Invalid License” or “This serial number is currently out of support” message and believe this to be incorrect, contact Technical Support. You will be asked to provide the serial number and serial key for the product in question.

Special Note for Windows XP Users

If you want to take advantage of AirMagnet WiFi Analyzer's integration with Windows Wireless Configuration on a laptop PC running on Microsoft Windows XP operating system with an 802.11n wireless network card, you must be running Service Pack 3 (SP3) or do the following:

- 1) Download and install the Microsoft Core XML (MSXML 6.0) at <http://www.microsoft.com/downloads/details.aspx?FamilyId=993c0bcf-4009-be21-27e85e1857b1&displaylang=en>.
- 2) Download and install the Microsoft Wireless LAN API (KB918997) at [http://www.microsoft.com/downloads/details.aspx?FamilyId=52A43BAB-DC\\$E-413F-AC71-158EFD1ADA50&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyId=52A43BAB-DC$E-413F-AC71-158EFD1ADA50&displaylang=en).

Utilizing Multiple Wireless Adapters

If the AirMagnet WiFi Analyzer machine has multiple AirMagnet-supported wireless adapters connected at the time the application is launched, the user will be prompted to select the adapters that should be utilized by the process.

As AirMagnet WiFi Analyzer is able to support different AirMagnet-supported adapters in multi-adapter usage, the launch dialog guides the user through what adapter combinations are valid for use.

Please see Chapter 4, Configuring Channel Scan Settings for information on Configuring Channel Scanning.

When a combination of multi-adapter capable and non-capable adapters are detected:

The user decides whether to use single or multi-adapter mode. See Figure 2-3.

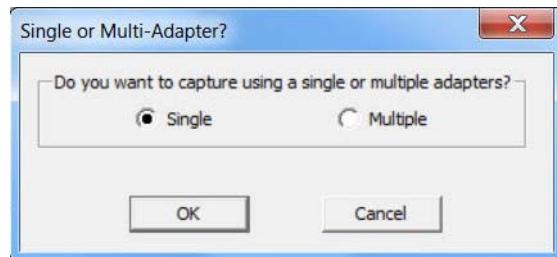


Figure 2-3: Selecting Single or Multiple Adapters

If the user selects single adapter mode, see [Figure 2-3](#).

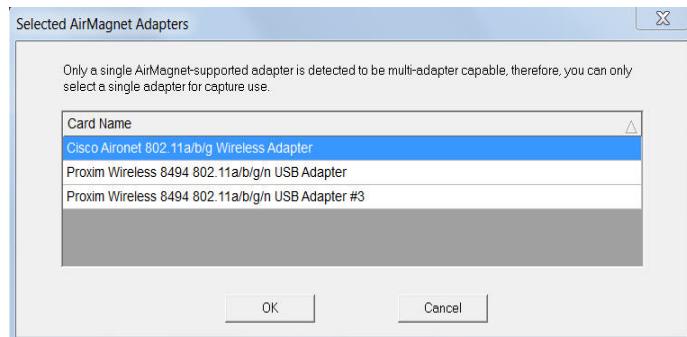


Figure 2-4: Selecting a Single Adapter

If the user selects multi-adapter mode, see [Figure 2-5](#).

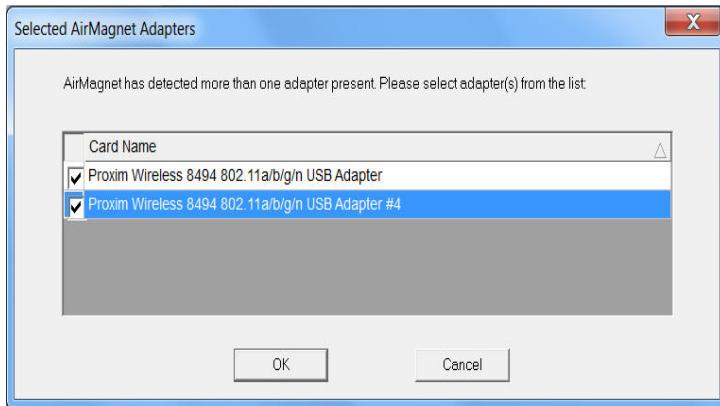


Figure 2-5: Selecting multiple adapters

When all adapters detected are multi-adapter capable:

The user can specify utilization of up to three adapters at any given time. When running in multi-adapter mode, each active wireless adapter will focus on a single channel, allowing the user to monitor all traffic on the selected channels simultaneously. [Figure 2-6](#).

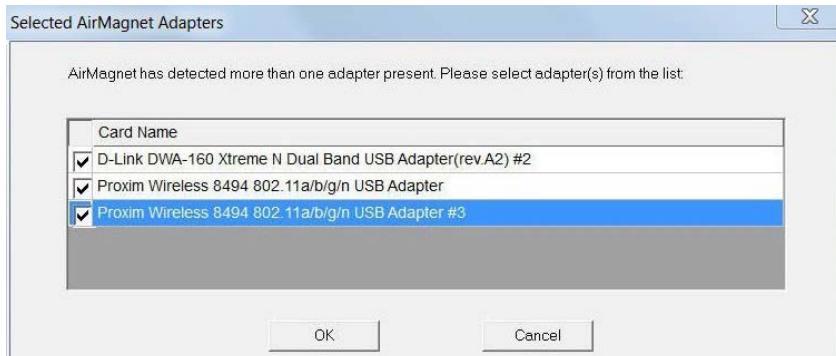


Figure 2-6: Selecting Multiple Adapters

Updating Wireless Networking Device Vendor List

During the course of the AirMagnet WiFi Analyzer installation, a file named “LANCardVendorsFile.txt” is automatically copied to the AirMagnet WiFi folder, as shown [Figure 2-7](#).

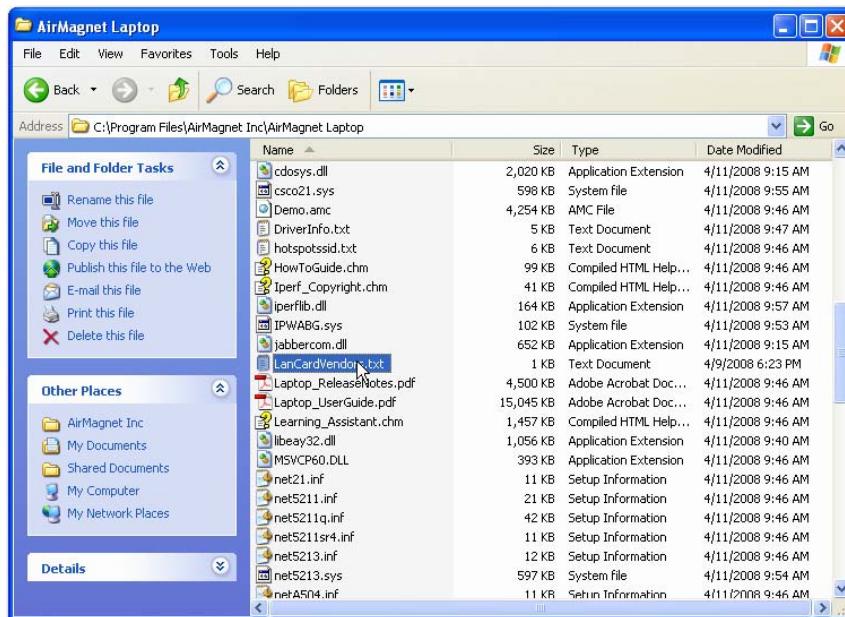


Figure 2-7: Locating LANCardVendorsFile.txt file

The LANCardVendorsFile.txt file contains information for mapping (Organizationally Unique Identifiers) OUIs in MAC addresses of networking devices with the names of the vendors who manufacture them. Creating such MAC-vendor pairs makes it easier to categorize and recognize the numerous networking hardware devices used on the network.

MAC (Media Access Control) address, also known as Ethernet Hardware Address (EHA), hardware address, or adapter address is a quasi-unique identifier attached/assigned to a network adapter, i.e., network interface card (NIC). A MAC address is a number that serves as the name of a particular network adapter. According to the IEEE 802 standard, a MAC address consists of six groups of two hexadecimal digits, separated by colons (:). MAC addresses can be “universally administered” or “locally administered”. A universally

administered address is uniquely assigned to a device by its manufacturer, sometimes called “burned-in address” (BIA). The first three octets (in transmission order) of a MAC address identify the manufacturer that issued the MAC address and is known as the Organizationally Unique Identifier (OUI).

The other three octets are assigned by that manufacturer in almost any order it wishes, but subject to the constraint of uniqueness. A locally administered MAC address, on the other hand, is assigned to a device by a network administrator. Locally administered addresses do not contain OUIs. [Figure 2-8](#) illustrates the structure of a universally unique address.

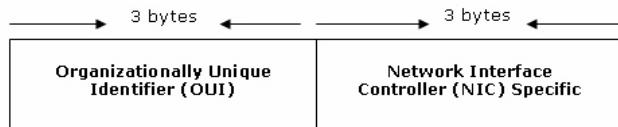


Figure 2-8: Structure of MAC address

By default, MAC addresses of all existing wireless networking devices are already mapped with the names of their respective vendors. [Figure 2-9](#) is a partial screen capture of AirMagnet WiFi Analyzer’s Start screen which reflects such mappings. AirMagnet periodically updates the MAC-vendor name mappings used in its products as new hardware devices come to the market. The LANCardVendorsFile.txt file is intended solely to help users who want to create the MAC-vendor name mappings on their own, without waiting for AirMagnet’s update.

	Device	MAC	.11	(S)	(N)	Security	SSID	Act	BI	
1	QA_VoFi_2	00:14:A8:44:13:20	g	51	2	Encrypted	N	QACiscoVoice	R	100
1	Edimax:0B:8C:C4	00:1F:1F:0B:8C:C4	n	0	2	Encrypted	N	anygate	R	100
1	QA_VoFi_2	00:0F:34:A7:78:13	g	0	0	Encrypted	N	QAVocera	OK	100
1	AP-10(BG)	00:14:69:F3:16:31	g	34	2	WPA-P	N	AirMagnetGuest	R	100
1	QA_VoFi_2	00:0F:34:A7:78:12	g	0	0	WPA2-P	N	QAFOFI	OK	100
1	AP-10(BG)	00:14:69:F3:16:30	g	35	2	WPA2-E	N	Air2	R	100
1	QA_VoFi_2	00:0F:34:A7:78:11	g	0	0	WPA-P	N	QASpectralink	R	100
1	QA_VoFi_2	00:0F:34:A7:78:10	g	0	0	Encrypted	N	QACiscoVoice	R	100
1	D-Link:EC:5D:CB	00:1B:11:EC:5D:CB	g	0	2	WPA2-P	N	Amicus_G1	R	100
1	DeltaNet:15:C4:E9	00:30:AB:15:C4:E9	b	0	0	Open	N	Wireless	R	100
3	Netgear:9E:85:48	00:18:4D:9E:85:48	g	31	2	WPA-P	N	chopper	R	100
4	Cisco-linksys:DB:88:81	00:12:17:DB:88:81	g	35	3	WPA-P	N	QA-linksys-WRT54G-LAB	R	100
4	Symbol:9E:A7:29	00:A0:F8:9E:A7:29	b	27	3	Open	N	qa_symbol@QA_lab_in_s...	R	100
4	AP-12(BG)	00:11:5C:4D:E8:F1	g	15	3	WPA-P	N	AirMagnetGuest	R	100
4	AP-12(BG)	00:11:5C:4D:E8:F0	g	10	3	WPA2-E	N	Air2	R	100
5	00:11:22:33:44:55	00:11:22:33:44:55	g	0	0	802.1x	N	wIPS_Attack	R	1
5	00:11:22:33:44:66	00:11:22:33:44:66	g	0	0	Open	N	wIPS_Attack	R	69
6	Cisco-Linksys:95:48:E9	00:1D:7E:95:48:E9	n	36	3	Open	N	linksys	R	100
6	Cisco-Linksys:0F:BB:F0	00:1D:7E:0F:BB:F0	g	27	3	Open	N	linksys-g-tv	R	100
6	1200-Calibratio	00:14:A8:53:66:40	g	0	0	Encrypted	N	1200-calibration	R	20
7	AP-11(BG)	00:11:5C:44:5E:B1	g	16	2	WPA-P	N	AirMagnetGuest	R	100
7	AP-11(BG)	00:11:5C:44:5E:B0	g	17	2	WPA2-E	N	Air2	R	100
7	AP-13(BG)	00:11:5C:4D:E9:11	g	6	2	WPA-P	N	AirMagnetGuest	R	100

Figure 2-9: All Devices screen showing MAC-vendor name mapping

To map MAC addresses with vendor names:

- From your laptop PC, locate and open the **LanCardVendorsFile** i.e. **.txt** file as shown in Figure 2-10.

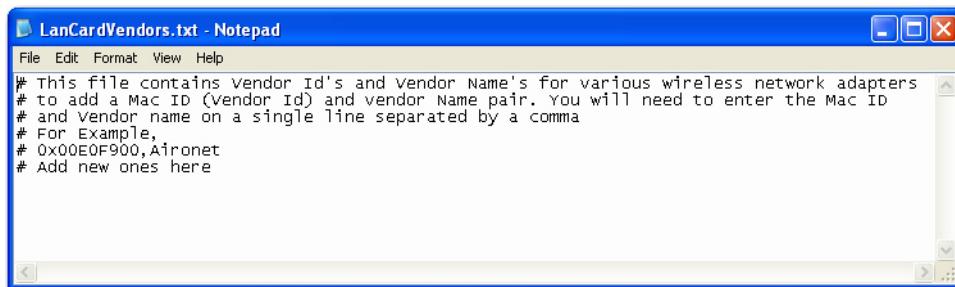


Figure 2-10: Content of LanCardVendorsFile.exe file

- Follow the instructions in the file to map the OUIs (in MAC addresses) of the hardware devices used on your network with the names of their respective vendors.

- 3) Click File>Save to save the mappings you have created.
- 4) Close the file.

Integration with Windows Wireless Configuration

This feature allows AirMagnet WiFi Analyzer users to take advantage of Windows wireless profiles that they have created on Windows and use them directly with AirMagnet WiFi Analyzer's active tools (i.e., Site Survey, Performance, Connect, Roaming, etc.). It should be noted that this feature applies to Microsoft Windows XP, Vista and Windows 7 operating systems only. Also, the configuration and modification of Windows wireless profiles must and can only be done inside the Windows operating systems.

If you want to use AirMagnet WiFi Analyzer's auto configuration feature on a laptop PC running on Microsoft Windows XP operating system with an 802.11n wireless network adapter, you must do the following:

- 1) Download and install the Microsoft Core XML Services (MSXML 6.0) from <http://www.microsoft.com/downloads/details.aspx?FamilyId=993c0bcf-3bcf-4009-be21-27e85e1857b1&displaylang=en>.
- 2) Download and install the Microsoft Wireless LAN API (KB918997) from <http://www.microsoft.com/downloads/details.aspx?FamilyId=52A43BAB-DC4E-413F-AC71-158EFD1ADA50&displaylang=en>.

Creating Wireless Configuration on Windows XP

Integration of AirMagnet WiFi Analyzer with Windows Wireless Configuration on Windows XP operating system requires an 802.11n wireless network adapter and the Microsoft Core XML Services (MSXML 6.0) and Microsoft Wireless LAN API (KB918997) installed

on the same machine on which AirMagnet WiFi Analyzer is installed and operated. Any addition, modification, and/or deletion of wireless networks (SSIDs) used for integration with Windows XP must and can only be done inside Windows XP operating system.

When configuring wireless networks (SSIDs) in Windows XP, make sure that AirMagnet WiFi Analyzer is closed (stopped).

To create a wireless configuration on Windows XP:

- 1)** Make sure that AirMagnet WiFi Analyzer is closed.
- 2)** Make sure that an 802.11n wireless network adapter is inserted in the laptop PC's wireless card slot.
- 3)** From the desktop of your PC, click Start>Control Panel >Network Connections.
- 4)** Right-click an 802.11n wireless network and select Properties from the drop-down menu.
- 5)** From the Wireless Network Connection Properties dialog box, click Wi-Fi Networks.
- 6)** Click Add. . . . The Wireless Network Properties dialog box appears. See [Figure 2-11](#).

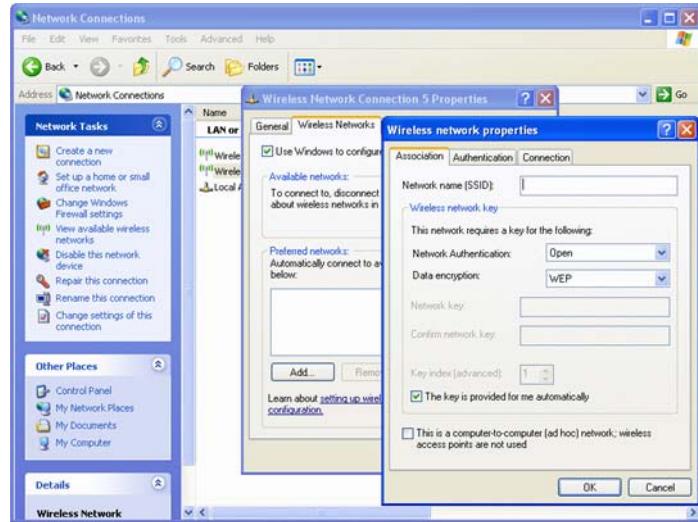


Figure 2-11: Configuring network settings in XP

- 7) Make the required entries and/or selections and click OK. See Figure 2-12.

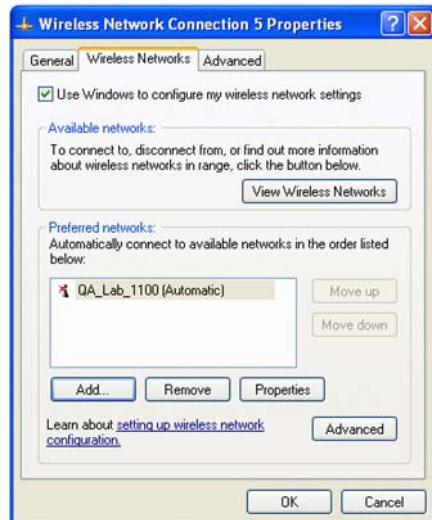


Figure 2-12: New network connection in XP

- 8) Repeat Step 6 through 7 to add all wireless network connections as applicable.
- 9) When all wireless connections are added, make sure that Use Windows to Configure my wireless network settings is selected and click OK.
- 10) Close the Network Connections dialog box.
- 11) Launch AirMagnet WiFi Analyzer.
- 12) Select File>Configure>802. 11. See Figure 2-13.

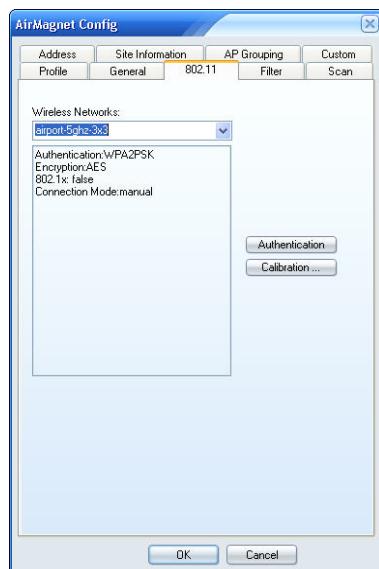


Figure 2-13: Available wireless networks

All wireless network connections (SSIDs) you have added on Windows XP are available in the AirMagnet Config dialog box under the 802.11 tab. You can choose to use any of them by clicking the down arrow and selecting the one of your choice. See Figure 2-14.

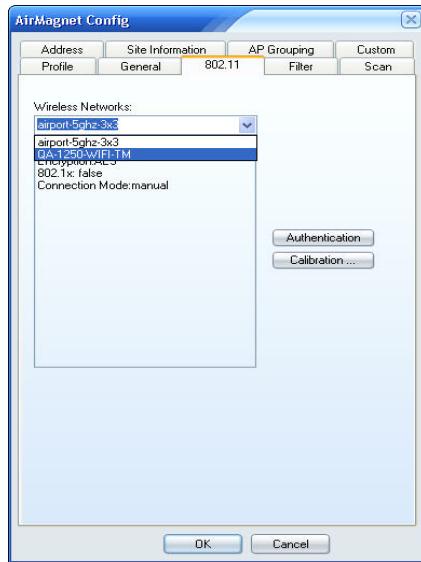


Figure 2-14: Selecting a wireless network

- 13) Select the wireless network of your choice and click OK.

Once a Windows wireless network connection (SSID) is selected, its security attributes (i.e., authentication, encryption, etc.) are shown in the dialog box. If you want to change any of these attributes, you must do it in the Wireless Network Connection Properties dialog box on Windows XP. See the section below.

Modifying Wireless Network Security Attributes on XP

To make changes to the security attributes of a wireless network:

- 1) Make sure that AirMagnet WiFi Analyzer is closed (stopped).
- 2) From click Start>Control Panel >Network Connections.
- 3) Right-click the 802.11n wireless network and select Properties from the drop-down menu.

- 4) From the Wireless Network Connection Properties dialog box, click **Wireless Networks**.
- 5) Highlight the wireless network of interest and click **Properties**. The dialog box then displays the properties of the selected wireless network.
- 6) Make the desired changes and click **OK**.
- 7) Click **OK** to close the Wireless Network Connection Properties dialog box.

*If you want to remove a wireless network connection (SSID), simply highlight it in the Wireless Network Connection Properties dialog box and click **Remove**. Then click **OK** on the Wireless Network Connection Properties dialog box to implement the change.*

Creating Wireless Configuration on Windows Vista and Windows 7

This feature applies to all wireless network adapters based on the Atheros chipset.

To create wireless configuration on Windows Vista and Windows 7:

- 1) Make sure that a wireless network adapter is inserted in the card slot of your laptop PC.
- 2) From your desktop, click **Start > Control Panel > Network and Sharing Center**. The Manage Wireless Networks dialog box appears. See [Figure 2-15](#).



Figure 2-15: Adding wireless connection on Windows Vista and Windows 7

- 3) Click Add. The Manually create a wireless connection dialog box appears. See [Figure 2-16](#).

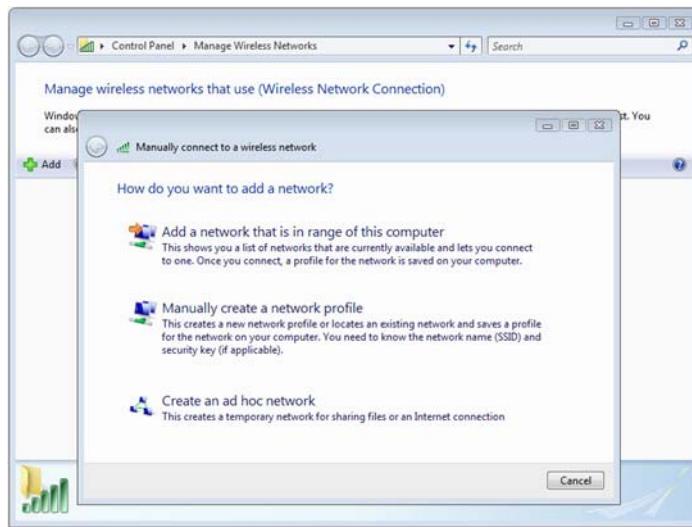


Figure 2-16: Manually creating a network profile

- 4) Click **Manually create a network profile**. The **Manually connect to a wireless network** dialog box appears. See **Figure 2-17**.

*You can also use **Add a network that is in range of this computer**.*

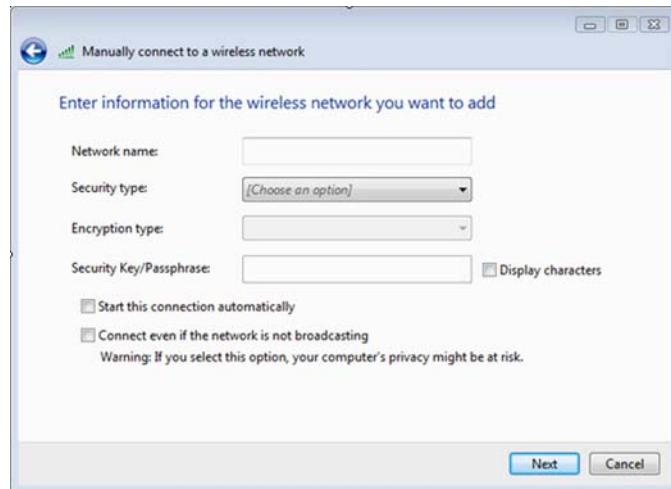


Figure 2-17: Creating a network profile

- 5) Make the required entries and/or selection and click Next.
- 6) Repeat Steps 2 through 5 to create as many wireless network profiles as applicable.

All wireless network profiles you have created appear in the Manage Networks dialog box on Windows Vista and Windows 7 as well as in the AirMagnet Config dialog box under the 802.11 tab. See below.

- 7) From AirMagnet WiFi Analyzer, click File>Configure...>802.11. See [Figure 2-18](#).



Figure 2-18: Selecting a Windows network profile

- 8) Click the down arrow, select a wireless network from the drop-down menu, and click OK.

Creating Network Connections in AirMagnet WiFi Analyzer

Unlike integration with Windows XP operating system, integration with Windows Vista and Windows 7 operating system allows the user to create wireless network connections directly from inside AirMagnet WiFi Analyzer.

- 1) From AirMagnet WiFi Analyzer, select File>Configure...>802.11>New.... The Create Wireless Network dialog box appears. See Figure 2-19.



Figure 2-19: Creating network connection in AirMagnet WiFi Analyzer

- 2) Enter a name for the wireless network connection and click OK.

The Windows Vista and Windows 7's Manage Wireless Networks dialog box appears, showing the new network connection you have just created on top of the list of all available network connections, as shown in Figure 2-20.

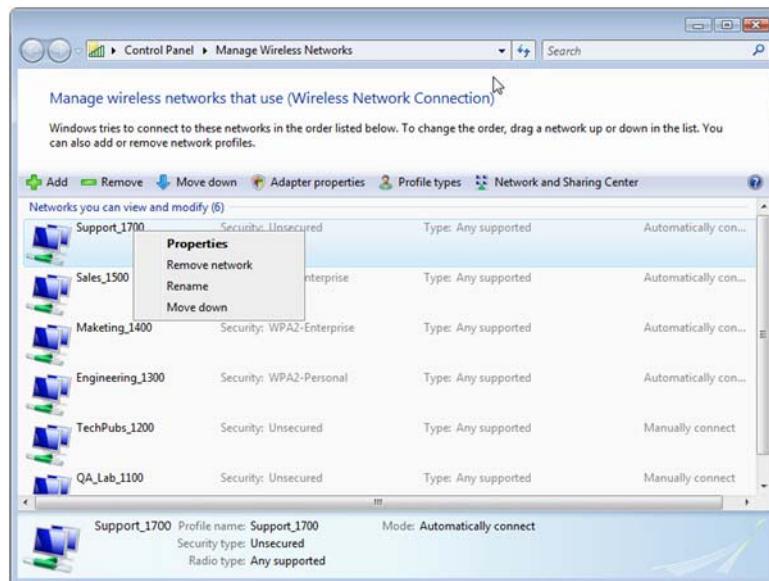


Figure 2-20: Configuring network connection in Windows Vista and Windows 7

- 3) Right-click the new connection you have just created and click **Properties** from the pop-up menu.

A dialog box with the name of the network connection on its title bar appears. Since the connection has not been configured yet, it does not have any security attributes. Therefore, the user needs to add the desired security attributes to it. See Figure 2-21.

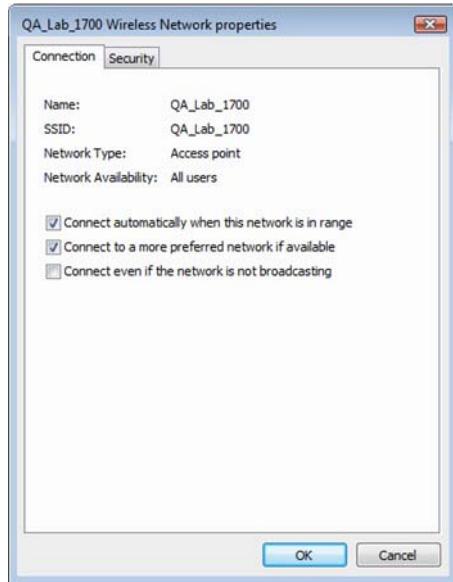


Figure 2-21: Configuring network properties in Windows Vista and Windows 7

- 4) Click the Security tab make the desired entries and/or selections, and click OK.

Now you have just created a new network connection in AirMagnet WiFi Analyzer. It can be used the same way as connections created in Windows Vista and Windows 7.

Modifying Network Connection in Windows Vista and Windows 7

Just as you can create network connections directly from AirMagnet WiFi Analyzer, you can make changes to existing network connections from inside AirMagnet WiFi Analyzer as well.

To modify a network connection in AirMagnet WiFi Analyzer:

- 1) From AirMagnet WiFi Analyzer, click File > Configuration... > 802.11.
- 2) Select the connection of interest and click Edit.... The Wireless Connection Properties dialog box appears.
- 3) Click the Security tab. See [Figure 2-22](#).

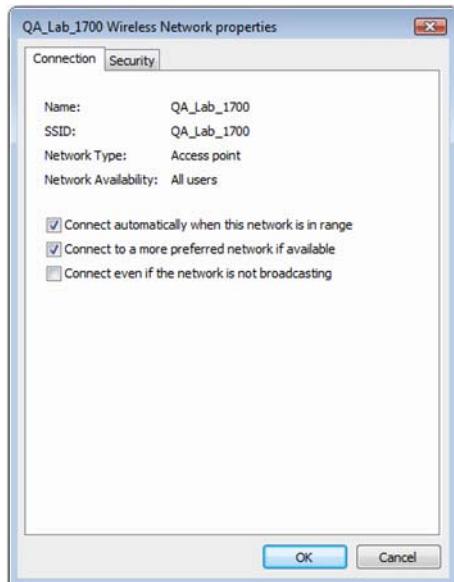


Figure 2-22: Modifying network security attributes

- 4) Make the desired changes and click OK
- 5) Click OK to close the AirMagnet Config dialog box.

Technical Support

Support Contracts

Fluke Networks' Gold Support is our comprehensive support and maintenance program that offers expanded coverage for all AirMagnet products. All existing AirMagnet customers with products under the annual maintenance and support program are automatically migrated to the new Fluke Network's Gold Support program.

Benefits of the Gold Support program include:

- Access to live 24 X 7 technical support.*
- Highly trained technical experts to help with product installation, configuration, best practices & troubleshooting on call 24 hrs a day including weekends and through the night.
- Multilingual technical support team.**
- Free software updates/upgrades (new features and product enhancements) when available.
- Hardware support, repair and replacement for AirMagnet products.***
- Free access to "AirMagnet Certified Professional" web-based training for certain AirMagnet products.
- MAC Address Reset assistance.

* Except United States holidays (New Years Day, Memorial Day, Labor Day, 4th of July, Thanksgiving, Christmas)

** Multilingual support not available on weekends

*** Must meet terms and conditions as defined in the hardware warranty.

Support contracts may be purchased or renewed by visiting the AirMagnet eStore or by contacting your sales representative. To view the status of your support contract, first sign-in to your MyAirMagnet account and visit the eStore located here:

<http://airmagnet.flukenetworks.com/estore/>

Contact Customer Support

- Navigate to http://www.airmagnet.com/my_aimagnet/ and log in to MyAirMagnet to access the “Exclusive” Gold-member only phone numbers for your region.
- Submit a support request.
- Send email to support@AirMagnet.com.

AirWISE Community

From the help menu, users can directly link to the AirWISE Community at <http://www.airwisecommunity.com> created by AirMagnet for wireless experts. The AirWISE Community includes discussion forums, blogs and additional resources for the security, performance and compliance of wireless networks.

Chapter 3: System Navigation

Chapter Summary

This chapter discusses AirMagnet WiFi Analyzer's basic navigation controls, major screen options and their key functions. It covers the following topics:

- Launching AirMagnet WiFi Analyzer
- Navigating through the program
- Viewing overall WLAN health
- Viewing RF data by channel
- Analyzing RF Interference
- Viewing RF data by WLAN nodes
- Solving WLAN issues using AirMagnet AirWISE
- Identifying top WLAN issues
- Decoding WLAN data packets
- Working on Roaming Analysis Screen

Launching AirMagnet WiFi Analyzer

To launch AirMagnet WiFi Analyzer:

- 1) From your desktop of your laptop PC, click Start>All Programs>AirMagnet>AirMagnet. The AirMagnet WiFi Analyzer's Start screen appears. See Figure 3-1.

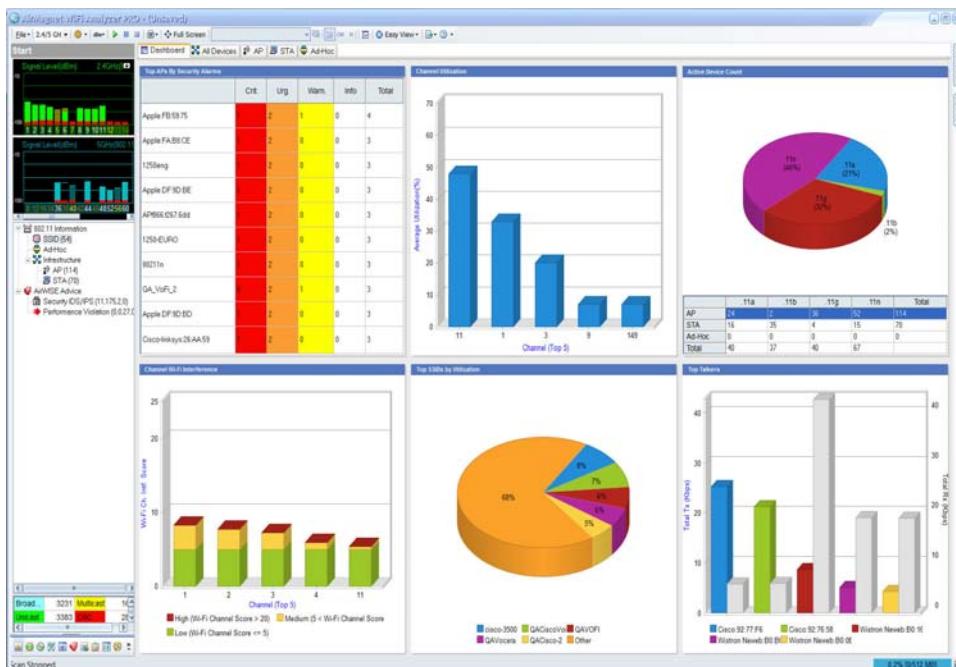


Figure 3-1: Start screen

Navigation Bar

At the bottom left of the AirMagnet WiFi Analyzer screen is the program's navigation bar, which contains navigation buttons for accessing different screens and tools. You can navigate from one screen to another using these buttons. See Figure 3-2.

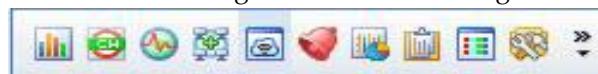


Figure 3-2: Navigation Bar

You can expand the navigation bar for easier viewing by clicking and dragging the dotted line across the top of the buttons upwards. Depending on your computer's screen size and resolution, this may cause the pie chart above the navigation bar to vanish.

Table 3-1 contains brief descriptions of each of these buttons.

Table 3-1: Navigation Bar and Buttons

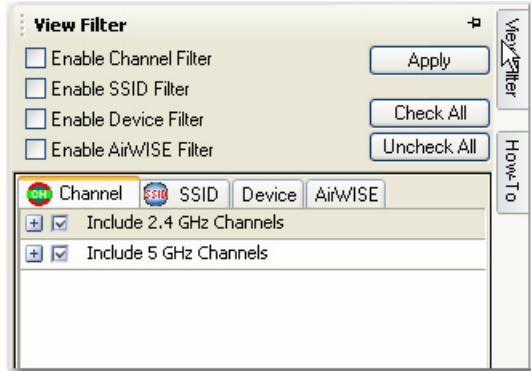
Button	Description
 Start	Start button opens the Start screen, which shows the overall health of the wireless LAN environment.
 Channel	Channel button opens the Channel screen, which allows you to visualize 802.11 traffic by channel.
 Interference	Interference button opens the Interference screen, which allows you to view the levels of interference each channel on your network is experiencing.
 Infrastructure	Infrastructure button opens the Infrastructure screen, which displays the WLAN's structure and components.
 AirWISE	AirWISE button opens the AirWISE screen, which lists the performance and security alarms detected by AirWISE.
 Roaming Analysis	Roaming Analysis button opens the Roaming Analysis screen, which allows you to troubleshoot roaming issues.
 Top Traffic Analysis	Top Traffic Analysis button displays the top 10 bandwidth consumers in the wireless LAN, and allows you to view many other common charts.
 Reports	Reports button allows you to view custom and default reports, including compliance and alarm detail pre-generated reports.

Table 3-1: Navigation Bar and Buttons

Button	Description
 Decodes	Decodes button opens the Decode screen, which displays the 802.11 packet summary in real time.
 WiFi Tools	WiFi Tools button opens the Tools screen, which contains more than a dozen easy-to-use WLAN tools for you to choose from.

View Filter

The View Filter tab located in the top right portion of AirMagnet WiFi Analyzer user interface provides the user with an easily accessible means of filtering the data displayed. To access the different filter options, simply move the mouse cursor over the tab and the View Filter pane will expand. See Figure 3-3.

**Figure 3-3: View Filter Pane**

The View Filter pane automatically collapses when you click an area outside of it. You can anchor the pane to keep it visible by clicking the thumbtack icon in its upper-right corner.

Applying Filters

As shown in Figure 3-3, the View Filter pane contains four tabs: Channel, SSID, Device, and AirWise, each representing a specific type of filters. You may filter on any or any combination of the four categories. By default, all filters are turned off. If you wish to enable a given filter category, you must first check the corresponding check box in the top portion of this pane. Then you need to click to open the corresponding filter tab below to select the entries to be filtered, i.e., channels, SSIDs, devices, or AirWISE alarms. You then need to make your desired selections individually or use the Check All button. Finally, you need to click the Apply button to activate your filters.

Channel Tab

The Channel filter allows you to define the channels whose data are shown on the screen. It differs from changing the channel scan settings (see “[Configuring Channel Scan Settings](#)” on page 201) in that by using the View Filter, you are simply altering the data that will be displayed, not the data that are actually processed. In other words, AirMagnet WiFi Analyzer will continue to monitor the unchecked channels, but it will not display data from them until you disable the filter.

SSID Tab

The SSID filter allows you to display data regarding specific SSIDs of interest. As with the channel filter, it affects the data display only. Once you disable the filter, data detected from other SSIDs will appear onscreen as well.

Device Tab

The Device filter allows you to define the devices of interest to be shown on the screen. For example, you can filter out devices that have been inactive for a certain period of time or those whose signal strength fall below a certain value.

AirWISE Tab

The AirWISE filter allows you to specify alarms to be shown onscreen based on the level of severity you specify. This way, you can focus your attention more on alarms that are of great interest to you.

How-To Guide

The tab located below the View Filter opens up an interactive guide that helps the user troubleshoot problems or configuration issues for the wireless environment. The guide contains links that allow the user to select from a variety of common wireless network scenarios. The major categories are:

- Device Monitoring Issues
- AirMagnet WiFi Analyzer Configuration
- Troubleshooting WLAN Networks
- Security Auditing
- Performance Auditing
- 802.11n Troubleshooting

After selecting the desired option, the user is presented with a step-by-step process for analyzing and repairing the issue at hand. Links contained within the steps help the user easily navigate to the necessary screens within AirMagnet WiFi Analyzer itself. You can activate the How-To guide from any major AirMagnet WiFi Analyzer screen by clicking the tool button along the right edge of the user interface, as shown in Figure 3-4.

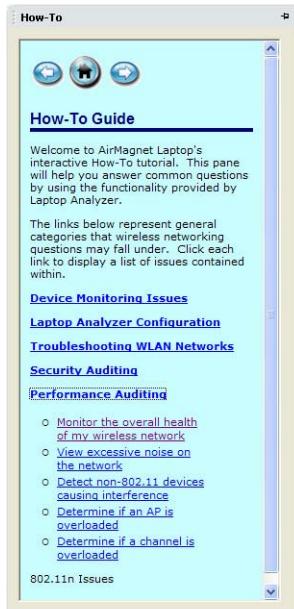


Figure 3-4: How-To guide main page

Toolbar

Across the top of AirMagnet WiFi Analyzer is a toolbar that contains a collection of buttons and drop-downs that provide tools for using the program. While some contents of the toolbar may be available only on certain screens, the major options remain the same on all major screens. Figure 3-5 shows the common options on the toolbar.



Figure 3-5: Common tools

Table 3-2 describes the common tool options on the toolbar and their functions.

Table 3-2: Common Toolbar Options

Tool	Description
	<p>The File menu provides the following command options:</p> <ul style="list-style-type: none"> • Open . . . – brings up the Open dialog box which allows you to browse for and open a file in a .amc, .ecp, or .cap format. • Close – closes the file currently opened on the screen. • Save – saves the data the application has captured as a file using any of the supported formats. See Open above. • Save As . . . – saves the file currently opened on the screen using a different file name or format. • Configure . . . – Opens the AirMagnet Config dialog box which allows you to set or change the settings of the application. • Policy Management . . . – Opens the AirMagnet Policy Management screen where you can create or modify policy profiles for your network. • Operation Mode . . . – opens the AirMagnet Operation Mode dialog box which allows you to switch between AirMagnet WiFi Analyzer Mode and Remote AirMagnet WiFi Analyzer Mode. • Connect To . . . – opens the Login dialog box which allows you to connect either to a Remote AirMagnet WiFi Analyzer (another laptop PC) or a Cisco AP/Scanner (Sensor). • Disconnect – disconnects the application from a laptop PC running in Remote Analyzer Mode or a Cisco AP running in a normal AP mode or Scanner mode (like an AirMagnet Sensor). • Recent Files – Shows a list of recently opened files. • Reset – This option erases all collected data from the buffer, effectively restarting AirMagnet WiFi Analyzer. • Exit – Closes the application.

Table 3-2: Common Toolbar Options

Tool	Description
	<p>The Band button allows you to select one of the following 802.11 bands you wish to scan:</p> <ul style="list-style-type: none"> • 2.4 GHz (for 802.11b/g/n channels) • 5 GHz (for 802.11a/n channels) • 2.4/5 GHz (for 802.11a/b/g/n) • 4.9 GHz <p>Note: The above options are available when an 802.11a/b/g card is used. However, you will see 2.4 GHz only when using an 802.11n wireless network card.</p>
	<p>The Configure button contains two options in its drop-down menu: Configure... and Policy Management....</p> <p>Note: Clicking this button directly open the AirMagnet Config dialog box; clicking the down arrow opens the drop-down menu that shows the two options.</p>
	<p>This button allows you to show data onscreen either by percentage or by dBm.</p>
	<p>These buttons allow you to control the application's live capture mode. They are from left to right, Start Live Capture, Pause Live Capture, and Stop Live Capture.</p> <p>Note: Pause Live Capture applies only to the Decodes screen.</p>
	<p>The View Reports button allows you to view reports based on data on the current screen and to set up your printer settings.</p>
	<p>The Full Screen allows you to toggle back and forth between a full screen view and partial screen view of each of the tabbed screens.</p>
	<p>The Dashboard Selection button allows you to customize the dashboard by selecting from a list of available charts and tables.</p>

Table 3-2: Common Toolbar Options

Tool	Description
	The Easy View button allows you to open a drop-down menu that contains the pre-configured viewing options for you to choose from.
	The Import-Export button allows you to import or export an ACL as well as some important data captured by the application.
	<p>The Help button contains three options in its drop-down menu:</p> <ul style="list-style-type: none"> • Contents... – opens AirMagnet WiFi Analyzer's online Help. • About... – opens the About AirMagnet dialog box which contains important information about this product. • Check Update – allows to check the availability of software update.

Working on Start Screen

AirMagnet WiFi Analyzer's Start screen serves as a dashboard of your WLAN and is loaded with comprehensive, summarized information about RF signal quality, network infrastructure, security and performance status, and frame communication in your wireless LAN environment. You can get to the Start screen when you launch the program or by clicking  from the Navigation Bar if you are on another screen.

By default, AirMagnet WiFi Analyzer starts in live capture mode, as indicated by **Live Capture** on its title bar. (Refer to Figure 3-1.) From the Start screen, one can easily drill down to a specific channel, a WLAN component (e.g., an AP or client station), or a security or performance alarm for further information or analysis. (For more information, refer to Chapter 2, Utilizing Multiple Wireless Adapters and Launch.)

WiFi Dashboard

AirMagnet WiFi Analyzer's usability-focused dashboard interface allows the user to get a quick overview of the traffic in the wireless environment. It is a high-level summary of your WLAN. It presents a quick snapshot of the overall health of your network without the need to dig for details. The user may still dig for details by clicking on the desired statistic. The high-level statistics summary that are available are:

- Channel Utilization
- Channel WiFi Interference
- TopTalkers
- Top SSIDs by Utilization
- Active Device Count
- TOP APs Based on Active Association
- Authorized vs. Rogue Devices
- AP Security Settings
- Top APs by Security Alarms
- Top APs by Performance Alarms
- Device Operating Mode
- Top Ad-Hoc

By default, the Start screen displays the dashboard interface to provide a comprehensive look at traffic. The dashboard can be accessed at any time by clicking the Dashboard tab located at the top of the Start screen. See Figure 3-6.

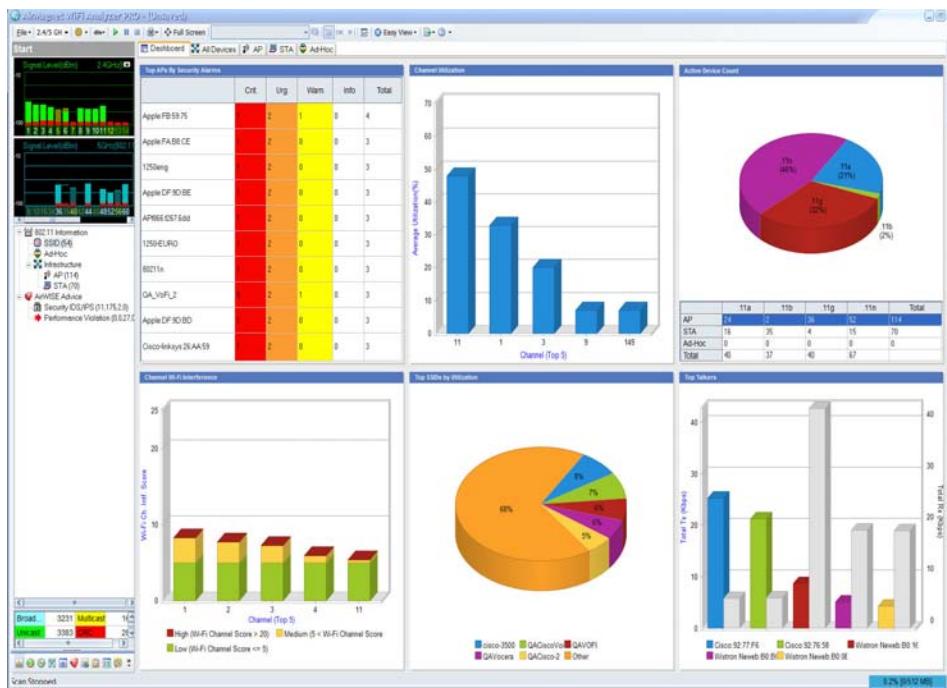


Figure 3-6: Start Screen Dashboard

By clicking the various charts in the dashboard, users will be navigated to the respective screens of AirMagnet WiFi Analyzer's user interface. The charts provided can be customized using the Dashboard Selection button from the toolbar.

Start Screen UI Components

As shown in Figure 3-1, AirMagnet WiFi Analyzer's Start screen can be divided into the following sections as indicated by the boxed areas, each showing a specific type of information of the wireless network. On the left, from top to bottom, are the RF Signal Meter, 802.11 Information and Alarm Summary, and Frame Address Type Table. On the right, from top to bottom, are Device Data and Alarm Details.

Toolbar Options

The Start screen's toolbar contains several tools that are available only on this screen: the text-search tool, the Easy View button, and OK/Rogue buttons. See Figure 3-7.



Figure 3-7: Start Screen Toolbar

Text-Search Tool

The text-search tool allows you to easily find a node based on device name, AP Group, MAC address, or SSID on the Device Data section of the Start screen. Simply enter your search criteria into the box and click the (Find in this view) button. Click the button repeatedly to continue finding the next device that meets your criteria.

Easy View Button

The Easy View button allows you to open a drop-down menu that contains the pre-configured viewing options for you to choose from:

- View by SSID – This option allows you to sort all devices in the Device Data section by SSID.
- View by Device – This option groups all devices by device name. It is especially useful if you have multiple devices using the same name.
- View by Media Type – Devices will be grouped based on their media types: 802.11a devices show up first, then 11b, 11g, and 11n. If your devices use a different media type (such as FCC 4.9GHz), they show up only if your card supports that mode.
- View by Channel – This option sorts devices based on the channel on which they are detected.
- View by Node Type – This (default) option allows you to sort all devices by device type (i.e., AP, STA, or Ad-Hoc).
- View by 802.11n – This option allows the user to view only 802.11n devices currently active. Note that this option only appears if a supported 802.11n adapter is in use.

- Advanced – This option allows you to customize the way devices are sorted. After it is selected, a new grey field will appear above the Device Data pane. You can drag and drop column headings into this field to define your sorting tree structure. For example, if you wish to sort based on Type first, then channel, and then device name, drag the Type column heading into the grey area first, followed by the Channel heading, and finally the Device heading. The devices will be sorted accordingly. To remove a heading from your tree, simply drag it back into the column headings below.

OK/R(ogue) Buttons

The OK and R buttons next to the Easy View drop-down menu allow you to mark a selected device as authorized or rogue device with a click of the button. Simply select the device of interest in the Device Data pane and click the status option (OK or R) you wish to use. The changes will be immediately reflected in the ACL column of the Device Data pane.

Dashboard Selection

The Dashboard Selection button allows you to customize the dashboard by selecting from a list of available charts and tables. Select the charts and tables from the Available Dashboard List and click on the Add button. The user may change the selection of currently shown high-level statistics by using the add-remove dialog. See Figure 3-8. There is also a Restore Default button to restore the selection to a default list of items. See Figure 3-9.



Figure 3-8: Dashboard Selection Screen



Figure 3-9: Dashboard Add Remove buttons

Tabbed View

Data on the upper right side are grouped by tabs - Dashboard, All Devices, AP, STA and Ad-hoc. All Devices/AP/STA/Ad-hoc are detailed device data (See Device Data) while Dashboard is a high-level summary of your WLAN health.



RF Signal Meter

The upper-left part of the Start screen is the RF signal meter, which provides an overview of RF signal quality on all available channels, each represented by a bar. The bars implement a high watermark feature that shows the highest point each channel has reached within a user-specified interval (configurable via the General tab of the Configure menu). See Figure 3-10.



Figure 3-10: Signal meter

RF Signal Quality Codes

As seen from the screen, the channel bars are color-coded, and the colors change dynamically to reflect the changes in RF signal quality. Also note that the color coding schemes for 802.11a and 802.11b/g differ slightly, as shown in Figure 3-10.

For 2.4-GHz (802.11b/g/n) channels, RF signal quality is color-coded as follows: (Refer to the upper part of Figure 3-10):

- **Green** – means that access points (APs) and/or stations (STs) are being detected on the channel. If an unassigned channel shows bright green, it may indicate that there are RF signals coming from APs of a neighboring business or from some other unknown sources, possibly rogue APs. In this case, actions should be taken to look into the sources of all unidentified RF signals.
- **Brown** – denotes cross-channel interference or station probing are being detected on the channel. Cross-channel interference is common in an 802.11 network because 802.11 channels tend to overlap each other. Therefore, an AP transmitting RF signals on Channel 2 will inevitably cause noticeable interference on Channels 1 and 3. This is why APs should be assigned to non-overlapping channels. For example, if you have three APs and Channels 1 through 11 available, you may want to assign the APs to Channels 1, 6, and 11, respectively, to minimize the chances of cross-channel interference.
- **Red** – indicates that noise is being detected on the channel. If you have 2.4-GHz cordless phones, Web cameras, microwave

ovens, or similar devices operating in the same frequency spectrum, you may see a noise level (red bar) above 10% or 75 dBm. Channel noise could cause high packet error rates and disrupt wireless transmission, resulting in poor network performance or unstable network connectivity.

For the 5-GHz 802.11a/g/n channels, RF signal quality is color-coded as follows:

- **Light Blue** – indicates that access points (APs) and/or stations (STs) are being detected on the channel.
- **Dark Blue** – indicates that cross-channel interference or station probing is being detected on the channel.
- **Red** – indicates that noise is being detected on the channel.

Expanded RF Graphs

You can expand the channel view by clicking  (Expand) in the upper-right corner of the signal meter. This allows you to view signal level (Green/Brown), noise level (Red), signal/noise ratio (Yellow), and interference score (Off-white) in separate graphs. See Figure 3-11.

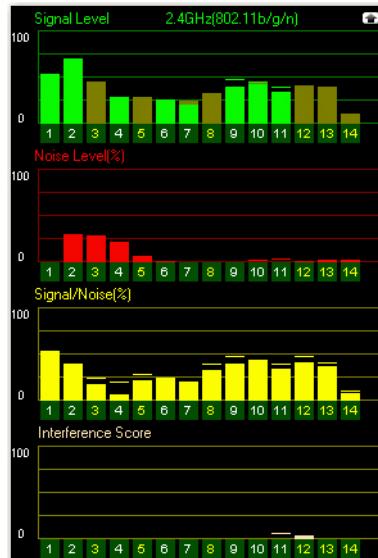


Figure 3-11: Expanded signal meter

The interference score graph gives you a quick view of the interference currently seen on each channel. For a more detailed view, click the channel of interested and you will be taken to the Interference page with that channel selected.

You can customize the channel scan list by eliminating unused channels and changing the scan frequency (see [Configuring Channel Scan Settings](#)). This allows you to focus your attention on capturing traffic on known active channels while still keeping an eye on the other channels for rogue APs and stations.

You can restore the signal meter to its original state by clicking  (Collapse) in the upper-right corner of the expanded signal meter screen. Refer to Figure 3-11.

Tip: Double-clicking a channel in the signal meter will take you directly to the Channel screen.

802.11n 20-/40-MHz Channels

With an AirMagnet-supported 802.11n wireless network adapter, AirMagnet WiFi Analyzer is also able to scan 802.11n data traffic on the 20- and 40-MHz channels. The 40-MHz wide band is denoted by a wide bar in the RF Signal Meter section on the Start screen. See Figure 3-12.

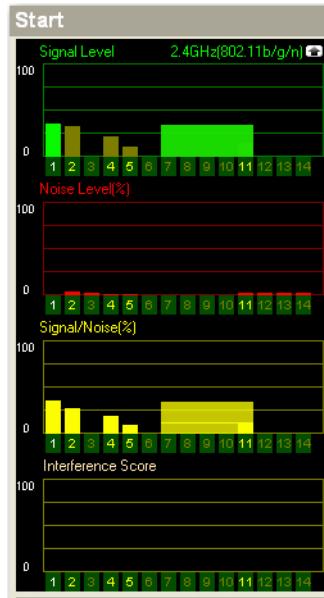


Figure 3-12: 20/40-MHz channels

802.11 Information

The **802.11 Information** is an visual summary of your wireless LAN infrastructure. It categorizes all the components or devices detected on your wireless network and shows the total number of components or devices in each category. See Figure 3-13.

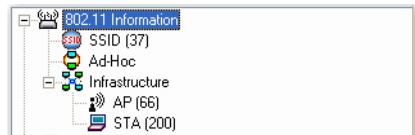


Figure 3-13: 802.11 information

Tip: Highlighting a node such as SSID, Ad-Hoc, AP, or STA allows you to display the network infrastructure information in the pie chart below; double-clicking an entry takes you directly to the Infrastructure screen.

AirWISE Advice

Below the 802.11 Information is a section entitled AirWISE Advice, which categorizes all the alarms detected on your WLAN into security and performance. There are four sets of digits for each category, representing different levels of severity. The digits, from left to right, represent alarms that are Critical, Urgent, Warning, or Informational. See Figure 3-14.



Figure 3-14: AirWISE advice

Highlighting an alarm category allows you to display in the pie chart the percentage of alarms of different severity levels; double-clicking an alarm category takes you directly to the AirWISE screen.

Packet Frames Summary

In the lower-left corner of the Start screen is a tabulation of packet frames AirMagnet WiFi Analyzer has detected. The frames are categorized into four categories: broadcast, multicast, unicast, and CRC. See Figure 3-15.

Broadcast	184004	Multicast	2547
Unicast	226917	CRC	43486
Total Frames	456954	CRC	9.52%

Figure 3-15: Packet frames summary

By default, the packet frames summary pane appears as it does above. To hide: go to File in the toolbar - Configure... - Click on the General tab - Uncheck the box marked Show Frames Statistics.

Table 3-3 briefly describes each of these frames.

Table 3-3: Summary of Packet Frames Transmission

Frame Type	Description
Broadcast	Broadcast is a term used to describe communication where data are sent for one point to all other points. In other words, there is just one sender, but the information is sent to all connected receivers.
Multicast	Multicast is a communication pattern in which a source host sends a message to a group of destination hosts simultaneously.
Unicast	Unicast is a term used to describe communication where data are sent from one point to another point. There are only one sender and one receiver.
CRC	Cyclic Redundancy Checks are used to verify packet information and reduce the potential for errors.

The Total Frames field displays the total number of frames that have been detected on the network so far. The field to its right allows you to view how much (the percentage) each frame type accounts for in the total number of frames. Simply click the down arrow and select from the drop-down menu the frame type you wish to view.

Device Data

Below the toolbar are tabs which includes Dashboard, All Devices, AP, STA and Ad-Hoc. The upper right-hand side of the Start screen is the Device Data section which summarizes the data about all the wireless devices detected on your WLAN. See Figure 3-16.

The screenshot shows a table titled 'Device Data' with the following columns: #, Device, MAC, .11, (S), (N), Security, SSID, ACL, and BI. The table lists numerous wireless devices, each with a unique ID, device name, MAC address, signal strength, security type, and associated SSID. The 'Security' column indicates whether the connection is Encrypted or Open. The 'ACL' and 'BI' columns show the number of clients and the total bandwidth, respectively. The table is scrollable and has a header row.

#	Device	MAC	.11	(S)	(N)	Security	SSID	ACL	BI
1	QA_VoFi_2	00:14:A8:44:13:20	g	51	2	Encrypted	N	QACiscoVoice	R 100
1	Edimax:0B:8C:C4	00:1F:1F:0B:8C:C4	n	0	2	Encrypted	N	anygate	R 100
1	QA_VoFi_2	00:0F:34:A7:78:13	g	0	0	Encrypted	N	QAVocera	OK 100
1	AP-10(BG)	00:14:69:F3:16:31	g	34	2	WPA-P	N	AirMagnetGuest	R 100
1	QA_VoFi_2	00:0F:34:A7:78:12	g	0	0	WPA2-P	N	QAVoFI	OK 100
1	AP-10(BG)	00:14:69:F3:16:30	g	35	2	WPA2-E	N	Air2	R 100
1	QA_VoFi_2	00:0F:34:A7:78:11	g	0	0	WPA-P	N	QASpectralink	R 100
1	QA_VoFi_2	00:0F:34:A7:78:10	g	0	0	Encrypted	N	QACiscoVoice	R 100
1	D-Link:EC:SD:CB	00:1B:11:EC:SD:CB	g	0	2	WPA2-P	N	Amicus_G1	R 100
1	DeltaNet:15:C4:E9	00:30:AB:15:C4:E9	b	0	0	Open	N	Wireless	R 100
3	Netgear:9E:85:48	00:18:4D:9E:85:48	g	31	2	WPA-P	N	chopper	R 100
4	Cisco-linksys:DB:88:81	00:12:17:DB:88:81	g	35	3	WPA-P	N	QA-linksys-WRT54G-LAB	R 100
4	Symbol:9E:A7:29	00:A0:F8:9E:A7:29	b	27	3	Open	N	qa_symbol@QA_lab_in_s...	R 100
4	AP-12(BG)	00:11:5C:4D:E8:F1	g	15	3	WPA-P	N	AirMagnetGuest	R 100
4	AP-12(BG)	00:11:5C:4D:E8:F0	g	10	3	WPA2-E	N	Air2	R 100
5	00:11:22:33:44:55	00:11:22:33:44:55	g	0	0	802.1x	N	wIPS_Attack	R 1
5	00:11:22:33:44:66	00:11:22:33:44:66	g	0	0	Open	N	wIPS_Attack	R 69
6	Cisco-Linksys:95:48:E9	00:1D:7E:95:48:E9	n	36	3	Open	N	linksys	R 100
6	Cisco-Linksys:0F:BB:F0	00:1D:7E:0F:BB:F0	g	27	3	Open	N	linksys-g-tv	R 100
6	1200-Calibration	00:14:A8:53:66:40	g	0	0	Encrypted	N	1200-calibration	R 20
7	AP-11(BG)	00:11:5C:44:5E:B1	g	16	2	WPA-P	N	AirMagnetGuest	R 100
7	AP-11(BG)	00:11:5C:44:5E:B0	g	17	2	WPA2-E	N	Air2	R 100
7	AP-13(BG)	00:11:5C:4D:E9:11	g	6	2	WPA-P	N	AirMagnetGuest	R 100
7	AP-13(BG)	00:11:5C:4D:E9:10	g	0	0	WPA2-E	N	Air2	R 100

Figure 3-16: Device data

Dashboard

The Dashboard screen includes six statistical charts or tables. You can choose from a list of available charts/tables to add or remove in the current Dashboard List. (See WiFi Dashboard).

All Devices

The devices are organized into three categories, as indicated by the collapsible sections: APs, Ad-Hocs, and STAs. You can choose to display a certain category of devices by clicking the '-' button on the fields that you wish to omit to collapse them (for example, to view stations only, collapse the AP and Ad-Hoc sections). The table

contains 30 data fields, including Channel, Device/MAC Address, Display 802.11, Signal Strength, Noise Level, Signal-to-Noise Ratio, Security Mechanisms, TKIP & MIC, Bridge Mode, SSID, ACL Status, Rogue in Network, Beacon Interval, Number of Stations, Preamble, PCF/DCF, Latitude, Longitude, Altitude, Distance, First Seen Time, and Last Updated Time.

You can sort the data by any category simply by clicking the title of that column, e.g., SSID. Use the scroll bar at the bottom of the table to view all the data contained in the table. You can also customize the number of columns of data to be displayed.

In Figure 3-14, “n” in the .11 column denotes an 802.11n device. An 802.11n wireless network adapter is required in order for AirMagnet WiFi Analyzer to detect 802.11n devices on the network.

To add/remove display columns:

- 1) Right-click anywhere in the data display field and select “Set Display Columns” from the menu. The Field Chooser dialog will appear.
- 2) Drag-and-drop the column headings from the dialog box into the columns in the table. The heading you dragged in will be added to the Start page.
- 3) Reverse Step 2 to remove a heading from the table.

Tip: Double-clicking a field in the alarm column takes to the AirWISE screen, which shows all alarms detected from that device; double-clicking in any other column takes you directly to the Infrastructure screen.

Table 3-4 briefly describes the data shown in Figure 3-16.

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
Type	Shows the category of the device which can be one of the following: <ul style="list-style-type: none">• AP• STA• Ad-Hoc
Alarms	Displays alarms involving the device. An alarm (bell) icon appears in this column if the device has triggered alarms.
Channel	All available channels detected on the WLAN: <ul style="list-style-type: none">• Red = Alarms are detected on the channel.• Yellow = No alarm is detected on the channel.
Active Time for Device	Displays the current status of the device. The icon is color-coded to display how long the device has been active: <ul style="list-style-type: none">• Green = Device has been active within the last 5s.• Yellow = Inactive within the last 5-60s.• Red = Inactive within 60-300s.• Grey = Inactive for more than 300s.
AP Group	Shows AP group names if you have set up the AP Grouping feature. See “ AP Grouping ” on page 212 for more information

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
Device	<p>Displays the name of the device. Often, the name will default to the device's MAC address. This field (and the MAC Address field below) is color-coded to display the activity status of the device:</p> <ul style="list-style-type: none"> • Green = The device has been active within the last 5 seconds. • Yellow = The device has been inactive between the last 5~60 seconds. • Red = The device has been inactive between the last 60~300 seconds. • Grey = The device has been inactive for more 300 seconds.
MAC Address	Displays the device's MAC Address. This field uses the same color-coding conventions as the Device field (above).
802.11	Type of 802.11 media, i.e., 802.11b or 802.11g, the device is using. <ul style="list-style-type: none"> • Green = 802.11b • Orange = 802.11g • Blue = 802.11a • Green/Blue = 2.4 GHz 802.11n/5 GHz 802.11n
Signal	Displays the signal strength in % or dBm.
Noise	Displays the noise level in % or dBm.
Signal-to-Noise Ratio	Displays signal-to-noise ratio measured in % or dBm.
Interference Score	Displays the interference score of the channel.

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
Security Mechanisms	<p>Indicates the security mechanisms used on the device:</p> <ul style="list-style-type: none"> • WPA-P = WPA-Personal • WPA-E = WPA-Enterprise • WPA2-P = WPA2-Personal • WPA2-E = WPA2-Enterprise • VPN = PPTP, IPsec, Secure Shell, etc. • Open = no security mechanism in place • Encrypted = packets are encrypted, but the specific encryption mechanism is not known • ? = Security mechanism is unknown <p>Devices utilizing multiple SSIDs will display the security settings for each SSID implemented, separated by commas.</p>
TKIP/MIC	<p>Shows TKIP/ MIC security settings:</p> <ul style="list-style-type: none"> • Y = Enabled; • N = Disabled; • U = Unknown. <p>Devices utilizing multiple SSIDs will display the security settings for each SSID implemented, separated by commas.</p>
Bridge Mode	<ul style="list-style-type: none"> • Y = Bridge Mode; • N = Non-Bridge Mode.
SSID	Displays the SSID of the device.

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
ACL Status	Shows the ACL status of the device. <i>Note: When AirMagnet WiFi Analyzer is launched for the first time upon installation, all devices detected are shown as U (Unknown). The user has to change the ACL status of all the devices one by one. This can be done by right-clicking a device and then selecting Rogue Device if it is a rogue device or Valid Device and then a specific ACL group from the submenu if it is a known, valid device on the network. All valid devices are marked by OK. Once a device's ACL status is marked, it will show up on the Start screen with same ACL status the next time you launch the application if the same device is detected. However, if you all devices are marked R (Rogue), all devices will show up as U (Unknown) if you restart the application after exiting it.</i>
Rogue in Network	Shows rogue devices traced inside the enterprise network.
BI	Shows Beacon Interval (in milliseconds)
Associated AP	Displays the name of the AP that the device is associated with.
#STA	Shows the number of stations associated.
Preamble	Shows the preamble value which can be either of the following: <ul style="list-style-type: none"> • Long • Short
PCF/DCF	Displays whether Point Coordination Function or Distributed Coordination Function is being used.
Latitude	Shows the latitude of the device (GPS only).
Longitude	Shows the longitude of the device (GPS only).
Altitude	Shows the altitude of the device (GPS only).
Distance	Shows the distance of the device (GPS only).
First	Displays the time the first packet was received.

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
Last	Displays the time the last packet was received.
Cell Power	Shows the power level at which the AP is transmitting in dBm.
Note:	<i>The following are applicable to View by 802.11n only.</i>
Tx Ch Width	Shows supported Tx channel width.
Rx Ch Width	Defines the channel width that may be used to transmit to the AP or STA.
PCO	Shows the PCO status which can be either of the following: <ul style="list-style-type: none"> • PCO active in the BSS • PCO inactive
Greenfield Supported	Indicates whether Greenfield transmission is supported, which can be either of the following: <ul style="list-style-type: none"> • Y = Yes • N = No
SGI	(Short Guard Interval) Shows the Short Guard Interval for 20-MHz and 40-MHz.
2nd Channel	(Secondary Channel Offset) Indicates the offset of the secondary channel relative to the primary channel.
Operating Mode	Indicates the operating mode of the BSS from which protection requirements of HT transmissions are determined.
Non-Greenfield STA Present	Indicates whether non-Greenfield stations are present, which can be either of the following: <ul style="list-style-type: none"> • N = All stations are greenfield-capable. • Y = One or more HT stations associated are not Greenfield-capable.
Non-HT OBSS	(OBSS Non-HT STAs Present) <ul style="list-style-type: none"> • Y = Use protection due to OBSS • N = No protection due to OBSS

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
40 GHz Intolerant	For APs, this indicates whether BSSs within the range are required to prohibit 40-MHz transmissions; for STAs, it indicates to its associated AP that it is required to prohibit all 40-MHz transmissions within the BSS.
RIFS Mode	Displays FIFS mode.
Tx STBC	(Tx STBC Supported) Indicates whether Tx STBC is supported, which can be either of the following: <ul style="list-style-type: none"> • Y = Supported • N = Not supported.
Rx STBC	(Rx STBC Supported) Indicates the state of Rx STBC support, which can be one of the following: <ul style="list-style-type: none"> • 0 = Not supported • 1 = 1 stream • 2 = 2 one and two streams • 3 = One, two, and three streams
LDPC	Shows LDPC Coding Capability which cab either of the following: <ul style="list-style-type: none"> • Y = Yes • N = No
SM Power Save	Displays SM Power Save.
Dual Beacon	Indicates whether Dual Beacon is used: <ul style="list-style-type: none"> • Y = Secondary beacon is transmitted by AP. • N = No secondary beacon is used.
Dual CTS Protection	Indicates wether Dual CTS Protection is required: <ul style="list-style-type: none"> • Y = Required. • N = Not required.
L-SIG TxOP Full Support	Indicates whether L-SIG TxOP is supported: <ul style="list-style-type: none"> • Y = All HT STAs support LSIG TxOP Protection. • N = One or more HT STAs do not support LSIG TxOP Protection.

Table 3-4: WLAN RF Data Summary Table Entries

Icon	Description
WAPI	WLAN authentication and Privacy Infrastructure is a Chinese National Standard for Wireless LANs (GB 15629.11-2003).

AP

The AP screen includes six statistical charts or tables. You can choose from a list of available charts/tables to add or remove in the current Dashboard List. (See WiFi Dashboard).

STA

The STA screen includes six statistical charts or tables. You can choose from a list of available charts/tables to add or remove in the current Dashboard List. (See WiFi Dashboard).

Ad-Hoc

The Ad-Hoc screen includes six statistical charts or tables. You can choose from a list of available charts/tables to add or remove in the current Dashboard List. (See WiFi Dashboard).

See Chapter.. on Multi-Adapters.

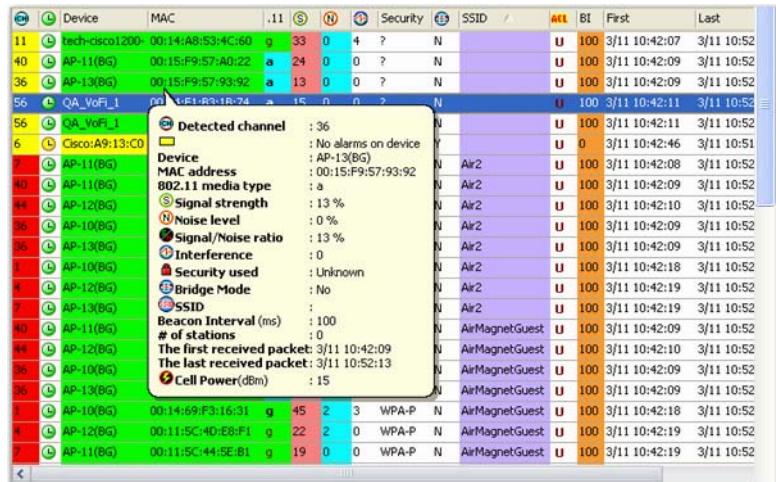
Locating a Wireless Device from the Start Screen

To quickly access the Find tool for a specific device from the Start Screen, right-click the device in question and select “Find” from the pop-up menu. This will bring up AirMagnet’s Find tool, which allows you to physically locate the device. For instructions on how to use the Find tool, see “Locating Rogue Devices” on page 304.

Using Bubble Help

The  (Show/Hide Bubble Help) button allows you to enable or disable the bubble help, which is a context-sensitive tip screen that is only available for the Signal Meter, 802.11 Information and AirWISE Advice, and Device Data sections of the Start screen. It provides helpful information these parts of the screen where text labeling is impossible to implement due to space constraints.

To use the bubble help, click  and then mouse over an object in any of the those sections. Refer to Figure 3-17.



	Device	MAC	.11	S	Security	SSID	ACL	Bl	First	Last		
11	tech-cisco1200-00:14:A8:53:4C:60	g	33	0	4	?	N	U	100	3/11 10:42:07		
40	AP-11(BG)	00:15:F9:57:A0:22	a	24	0	0	?	N	U	100	3/11 10:42:09	
36	AP-13(BG)	00:15:F9:57:93:92	a	13	0	0	?	N	U	100	3/11 10:42:09	
56	QA_VoFi_1	00:16:EF:03:18:74	a	15	n	n	?	N	U	100	3/11 10:42:11	
56	QA_VoFi_1	Cisco:A9:13:C0							U	100	3/11 10:42:11	
6	AP-11(BG)							U	0	3/11 10:42:46		
40	AP-11(BG)							U	100	3/11 10:42:09		
40	AP-12(BG)							U	100	3/11 10:42:09		
44	AP-12(BG)							U	100	3/11 10:42:10		
36	AP-10(BG)							U	100	3/11 10:42:09		
36	AP-13(BG)							U	100	3/11 10:42:09		
3	AP-10(BG)							U	100	3/11 10:42:09		
4	AP-12(BG)							U	100	3/11 10:42:19		
7	AP-13(BG)							U	100	3/11 10:42:19		
40	AP-10(BG)							U	100	3/11 10:42:09		
44	AP-12(BG)							U	100	3/11 10:42:10		
36	AP-10(BG)							U	100	3/11 10:42:09		
36	AP-13(BG)							U	100	3/11 10:42:09		
35	AP-13(BG)							U	100	3/11 10:42:09		
3	AP-10(BG)	00:14:69:F3:16:31	g	45	2	3	WPA-P	N	AirMagnetGuest	U	100	3/11 10:42:16
3	AP-12(BG)	00:11:5C:4D:E8:F1	g	22	2	0	WPA-P	N	AirMagnetGuest	U	100	3/11 10:42:19
3	AP-11(BG)	00:11:5C:44:5E:81	g	19	0	0	WPA-P	N	AirMagnetGuest	U	100	3/11 10:42:19

Figure 3-17: Using Bubble Help

AirWISE Details

Below the Device Data section is the AirWISE section, which shows alarms data in two major categories, i.e., Security IDS/IPS v.s. Performance Violation. See Figure 3-18 and Chapter 2 on Multi-Adapters.

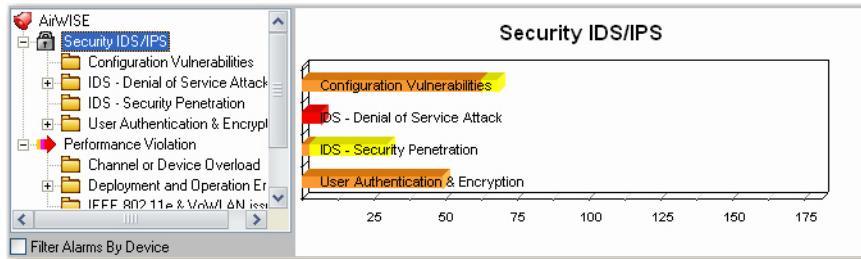


Figure 3-18: AirWise

On the left are various types of alarms in each category; on the right is a bar chart that displays the total number of alarms contained in each category that you have selected.

In the lower left-hand corner of this section is the Filter Alarms by Device check box. Normally, the Alarm Summary section displays the alarms that have been generated by all the devices (i.e., APs, STAs, or Ad Hoc). However, if this check box is checked, the Alarm Summary section will only display alarms about the device, whether it is an AP, station, or ad hoc station, you select from the Device Data section.

Changing Operating Frequency

Wireless devices can use different radio operating frequencies to transmit and receive packets on a wireless network, depending on the 802.11 wireless networking protocol being used. AirMagnet WiFi Analyzer supports all 802.11 protocols, i.e., 802.11a/b/g/n. Since wireless devices built on different 802.11 standards use different operating frequencies, selecting or changing the operating frequency on AirMagnet WiFi Analyzer forces the application to gather packets that are generated only by devices using a specific radio operating frequency. In so doing, it allows you to focus on network traffic involving wireless devices that are using a specific 802.11 protocol.

The Operating Frequency drop-down menu lists all the operating frequencies supported by the wireless network card currently used on AirMagnet WiFi Analyzer. Figure 3-17 shows the options that are available when an 802.11a/b/g/n wireless network card is used.



Figure 3-19: Operating Frequency Drop-Down Box

Changing operating frequency is just like physically changing the wireless network card. AirMagnet WiFi Analyzer will empty all the packets captured in the buffer and then start capturing data using the new operating frequency. Any change in operating frequency is reflected in other parts of the UI that are affected. If you are on a screen other than the Start screen, selecting another band will take you directly to the Start screen.

802.11 Protocols and Operating Frequencies

Table 3-5 briefly describes the operating frequencies used by different 802.11 wireless networking standards.

Table 3-5: 802.11 Protocols and Operating Frequencies

Protocol	Operating Frequency (GHz)	Typical Throughput (Mbps)	Maximum Data Rate (Mbps)	(Indoor) Range (Feet)	(Outdoor) Range (Feet)
802.11a	5.15~5.25 5.25~5.35 5.745~5.825	23	54	~90	~300
802.11b	2.4~2.5	4	11	~105	~330
802.11g	2.4~2.5	19	54	~105	~330
802.11n	2.4 and/or 5	74	248	~210	~480

FCC 4.9-GHz Mode

As a licensed band, the 4.9-GHz spectrum offers an interference-free operating environment for public safety broadband communications. It is best suited for fixed wireless applications for point-to-point (P2P) and point-to-multipoint (PMP) communications. There are a number of services that a public service agency or municipal authority can craft out of a 4.9-GHz radio transmission backbone. Typically these services and applications can replace costly leased services, thus leading to an ROI and long-term savings for the operating authority. AirMagnet currently provides the only WLAN analysis software that is capable of monitoring the 4.9-GHz band.

The 4.9-GHz feature only functions with the Ubiquiti SR4C 4.9-GHz and TRENDnet TEW-501PC ag adapters.

Changing RF Signal Unit of Measurement

By default, channel RF signal strength, noise level, and signal-to-noise ratio are displayed in percentage (%). However, you can change to dBm by clicking the %/dBm drop-down menu next to the media type button. See Figure 3-20.



Figure 3-20: dBm/% Drop-Down Box

Notice the changes in the Signal, noise, and signal-to-noise ratio fields in the Device Data section as you toggle between % and dBm.

Worldwide 802.11 a/b/g/n Radio Channel Allocation

Since regulatory rules dictate the radio frequencies (channels) and emission powers for 802.11 standards in various parts of the world, the number of channels available depends on the geographical location and the media band (2.4 GHz vs. 5 GHz) you select. Table 3-6 shows channel allocation for all both 2.4 GHz and 5 GHz media bands in major parts of the world.

Table 3-6: Worldwide Radio Channel Assignment

Region/Country	2.4 GHz	5 GHz
Americas	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 149, 153, 157, 161, 165
Most part of Europe and Australia	1 ~ 13	36, 40, 44, 48, 52, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
France	10 ~ 14	36, 40 44, 48, 52, 56, 60, 64
Spain	10 ~ 11	36, 40 44, 48, 52, 56, 60, 64
Japan	1 ~ 14	36, 40, 44, 48, 52, 56, 60, 64,
Pacific Rim (China, Taiwan, Hong Kong, Singapore, Korea, etc.)	1 ~11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

The Start screen displays the top-level information of your WLAN's RF environment. It is especially useful if you want to have a quick grasp of what is going on in or around your WLAN. However, keep in mind that the data on this screen are real-time and dynamic. Old data get erased as new data come in. It is for this reason that AirMagnet WiFi Analyzer comes with a live capture feature that allows you to record (save) data so that they can be replayed at a later time for analysis. The data can be exported as well. For more information, see “[Saving Captured Data](#)” on page 316.

Accessing Data Reports

The integrated AirMagnet Reporter automatically converts all on-screen data into reports. The content of the reports are screen-specific, making them easy to view, analyze, share, and archive. You can access the reports by clicking  **Reports** from the Navigation Bar or  **(Vi ew Reports)**. See chapter on multi-adapter when multiple adapters are used.

Detailed instructions on how to use the Reporter can be found in Chapter 8, “Managing WLAN Reports”.

Working on Channel Screen

You can drill down to the Channel screen by clicking any of the channel bars on the signal meter from the Start screen or by clicking  **Channel** from the Navigation Bar. The Channel screen lets you focus on a specific channel for detailed analysis. See Figure 3-21 See also chapter on multi-adapter when multiple WiFi adapters are used.



Figure 3-21: Channel screen

Channel Utilization and Throughput

The top part of the screen consists of two signal meters: one for channel utilization and the other channel throughput. As a rule of thumb, 60% of utilization or 6 Mbps of throughput is a realistic upper limit for an 802.11b network. Constant high channel utilization with most traffic in 11 Mbps and low packet error rates may indicate that the 802.11b network may not have enough capacity to meet the needs of all its users. One possible solution would be to reduce the cell size and to add access points at strategic locations.

Channel Selection Pane

The left-hand side of the screen contains the channel selection pane. Its contents vary depending on the media type you select. There are four columns in the channel selection pane: Channel , #AP, #STA, and #Ad-Hoc. These columns display the channel numbers and the number of APs, Stations, and Ad-Hoc devices on each channel.

Across the top of this part of the Channel screen are three radio buttons that represent the mode of the network. The buttons are:

- **Lower 40 MHz** – If selected, the 40-MHz lower channel is shown. Both the legacy and HT packets can be transmitted in lower 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.
- **20 MHz** – If selected, only shows 20-MHz channel. This mode focuses on the 20-MHz channel. According to the 802.11n Draft 2 standard, this mode is mandatory.
- **Upper 40 MHz** – If selected, the 40-MHz upper channel is shown. Both the legacy and HT packets can be transmitted in upper 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.

You can know whether any or all of these three modes are supported on a certain channel simply by clicking the channel number below. The mode will be automatically greyed out if it is not supported on that channel.

You can switch from one channel to another simply by selecting a from the list. Once a channel is selected, AirMagnet WiFi Analyzer will lock on that channel until another channel is selected. The selected channel is indicated by the number inside the circle in the middle of the upper part of the screen. See Figure 3-22.

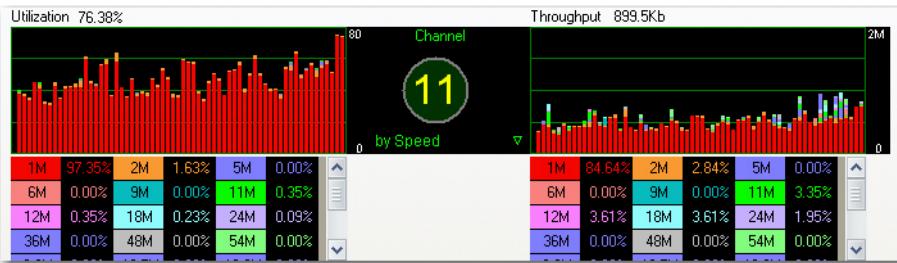


Figure 3-22: Focusing on one channel

The number “11” inside circle in Figure 3-22 indicates that the channel you are focusing on is a 20-MHz channel. However, a left arrow will appear below the channel number when a lower 40-MHz channel is selected and a right arrow will appear below the channel number when a upper 40-MHz channel is selected. Both arrows indicate that the channel you are focusing on is the primary channel in a 40-MHz channel. Furthermore, the left arrow indicates that the secondary channel is below the primary channel whereas the right arrow indicates that the secondary channel is above the primary channel.

The lower portion of the graph displays the speed at which packets are being transmitted on the selected channel. These fields are color-coded and correspond with the graphs above. If the entire graph is red (as shown in Figure 3-22), virtually all packets on your network are being transmitted at 1 Mbps.

Link Speed and Media Type

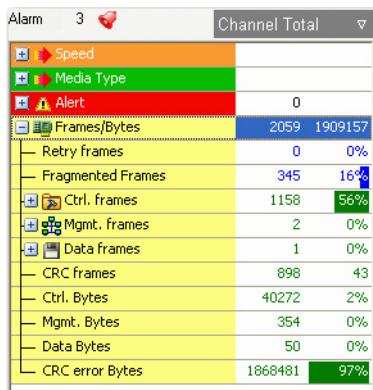
When you are using 802.11g, a/g, or a/b/g/n for your media type, a filter appears below the channel number, allowing you to toggle the data display between link speed and media type. Both link speed and media type are color-coded. Selecting by **Speed** will display the different rates at which data are being transmitted in the fields below the graphs; selecting by **Media** will display the media types that packets are being sent using.

Channel Data Summary

The middle-left part of the Channel screen summarizes various critical information about the selected channel.

On the top is a channel alarm summary. It shows the number of alarms triggered on the channel. Clicking  will take you to the AirWISE screen, where a detailed explanation about the alarm(s) and expert advice are available.

Below the alarm summary is a list of RF data summary for the selected channel. All the data are displayed in frames or bytes. Each type of data is represented by an icon. You can choose to view the details of any of these data or hide them by clicking the plus or a minus sign next to the corresponding icon. You can also filter the data display either by Channel Rate or by Channel Total using the options from the drop-down menu in the top-right corner of the summary pane. See Figure 3-23.

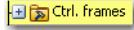


Alarm 3 		Channel Total
 Speed		
 Media Type		
 Alert		
 Frames/Bytes	0	
 Retry frames	0	0%
 Fragmented Frames	345	16%
 Ctrl. frames	1158	56%
 Mgmt. frames	2	0%
 Data frames	1	0%
 CRC frames	898	43
 Ctrl. Bytes	40272	2%
 Mgmt. Bytes	354	0%
 Data Bytes	50	0%
 CRC error Bytes	1868481	97%

Figure 3-23: Viewing channel data summary

Table 3-7 describes the screen information as shown in Figure 3-23.

Table 3-7: Channel Screen Control Buttons

Button	Description
 Speed	<ul style="list-style-type: none">Summarizes link speed of the channel.
 Media Type	<ul style="list-style-type: none">Summarizes the types of media discovered on the channel.
 Alert	<ul style="list-style-type: none">Lists frame error code information.
 Frames/Bytes	<ul style="list-style-type: none">Divides frame and byte counts into retry frames, fragmented frames, control frames, management frames, data frames, and CRC error frames, etc.
 Ctrl. frames	<ul style="list-style-type: none">Summarizes control frames/bytes.
 Mgmt. frames	<ul style="list-style-type: none">Summarizes management frames/bytes.
 Data frames	<ul style="list-style-type: none">Summarizes data frames/bytes.

The Channel screen makes it easy to detect low link speeds, excessive retries, and cyclic redundancy check (CRC) errors.

Device Data Graph

The part of the Channel screen displays the various types of network data in the form of line chart. Across the top this screen are two filters: the one on the left provides up to a dozen types of data for you to choose from for the graph and the one on the right allows you to choose the number of graphs (from 1 to 6) to display at one time. See Figure 3-24.

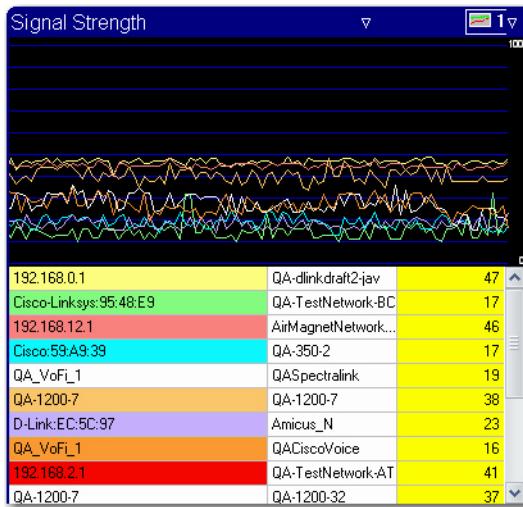


Figure 3-24: Device Data Graph for Selected Channel

Figure 3-24 shows the device data on the selected channel in the lower-right part of the Channel screen. Across the top are two filters: the Data Selector on the left allows you to select the type of data to display and the Graph Options on the right lets you choose to display the data in up to six individual mini screens.

The table below the graph contains information for the type of graph you have selected. The default graph (Signal Strength) displays all the devices detected on the channel. Each device is coded with a unique color which corresponds to the color of the line chart above. If any of the devices has a value of zero on the far right, then it will not show on the graph at all.

Analyzing Channel Occupancy

The Channel screen's Occupancy tab allows you to have a “bird’s eye view” of RF spectrum usage by 802.11 devices in the 2.4- or 5-GHz frequency band (depending on which channel is selected). It shows in real time the state of occupancy (or usage) of all available channels and provides a simple and straightforward way for the user to know which channels are in use and which channels they should choose in case they want to select a channel for better signal quality (with less interference).

For each 802.11 device, the Channel Occupancy screen displays the following information:

- The device name and media type.
- The device's "center" channel (frequency), as indicated by the position of the red-colored square.
- The device's signal strength, as indicated by the intensity of the red coloring of the "center channel cell": the darker the red, the stronger the signal strength.
- The device's channel, as indicated by the numeric value in the center channel cell; for 40 MHz channels, 1 and -1 are used to indicate 40-MHz Upper and 40-MHz Lower channels, respectively. The center frequency indicated by the red square could shift left by 10 MHz for the lower 40 MHz mode or right by the same amount for the upper 40 MHz mode.
- The device's modulated spectrum usage, as indicated by the yellow cells in its row; and the device's un-modulated spectrum usage, as indicated by the light yellow cells in its row.

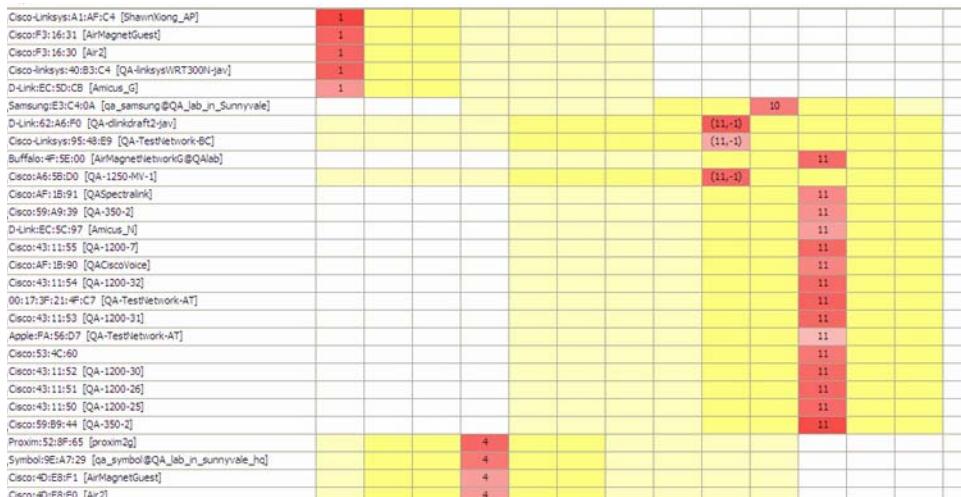


Figure 3-25: Channel screen showing channel occupancy

From Figure 3-25 above, we can make the following observations about the first 5 devices listed:

- 1) They are operating on 2.4-GHz Channel 1.
- 2) The 5th device has the weakest signal strength of the 5.
- 3) All 5 devices contribute modulated interference on Channels 2 and 3.
- 4) All 5 devices contribute (at least some) un-modulated interference on Channels 4 through 7.

We may also make the following observations about the 7th and 8th devices listed:

- 1) These devices are operating on 40 MHz (Lower), Channel 11.
- 2) The modulated interference extends two additional cells on either side of the center frequency, as compared to the 20 MHz devices discussed above.
- 3) However little, the un-modulated interference extends all the way to Channel 1.
- 4) We can see the 10-MHz shift in center frequency for the device (as indicated by the fact that the center channel is under Channel column 9, instead of 11).

It should be noted that the 2.4-GHz and 5-GHz channel occupancy differs from each other, in the fact that the 5-GHz channels are spaced 20 MHz apart, as compared to 5 MHz for the 2.4-GHz channels. Thus, devices will take up less cells in the 5-GHz view than the 2.4-GHz view.

Working on Interference Screen

The Interference screen allows you to view the amount of signal interference that currently exists on a given channel. The selected channel's interference score is displayed numerically as well as graphed on the right of the device listing. The interference score indicates the extent to which signal interference impacts your network's performance. The larger the value, the severe the impact. See Figure 3-26.

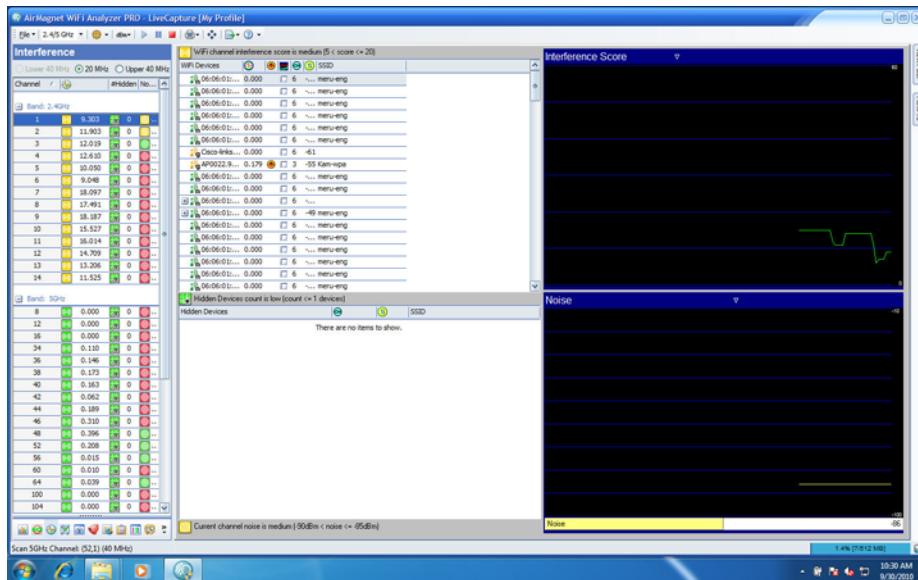


Figure 3-26: The RF Interference Page

A channel's interference score is calculated based entirely on standard WiFi devices. Each device operating on the selected channel or on adjacent channels will generate interference on the channel you are focusing on. The displayed interference score adds up the interference from these devices and shows how much interference the channel is experiencing as a result. Each separate channel may have widely varying interference scores due to different numbers of devices operating in the adjacent channels.

If you are using AirMagnet WiFi Analyzer by itself (without AirMagnet Spectrum Analyzer integrated), the displayed interference score represents the total of all standard interference generated on the selected channel by 802.11 devices, i.e., APs, wireless stations, etc. Any non-802.11 interference will simply show up as noise, which you can view by selecting the Noise option in the

graph below. To identify the objects or devices that are causing this noise, you may need to purchase AirMagnet Spectrum Analyzer and integrate it with AirMagnet WiFi Analyzer. See the [AirMagnet Spectrum Analyzer Integration](#) section below for more information.

Interference Score

A channel's interference score is calculated based entirely on standard WiFi devices. Each device operating on the selected channel or on adjacent channels will generate interference on the channel you are focusing on. The displayed interference score adds up the interference caused by all these devices and shows you how much interference the channel is experiencing as a result. The interference scores may vary widely among channels due to the difference in the number of devices operating on their adjacent channels.

If you are using AirMagnet WiFi Analyzer by itself (without AirMagnet Spectrum Analyzer integration), the displayed interference represents the total of all standard interference generated on the selected channel by 802.11 devices, i.e., APs, stations, etc. Any non-802.11 interference will simply show up as noise, which you can view by selecting the Noise graph option in the lower right-hand corner of the screen. To identify the sources of noise (i.e., objects or devices that are causing this noise), you may purchase AirMagnet Spectrum Analyzer and integrate it with AirMagnet WiFi Analyzer.

Channel Interference Calculation

802.11 defines RF transmit spectrum mask requirements for each of the modulation types supported by the standard. These requirements are used to limit the amount of interference an 802.11 device contributes to channels which are adjacent to the channel on which it is operating. As RF channels do not have exact edges, it is prudent that 802.11 devices employ filtering and/or other techniques to minimize the amount of RF energy they emit outside their operating channel when they transmit. While this "out-of-channel" interference is minimized, it can't be zero.

The following transmit spectrum masks are defined in the 802.11 standard (and/or its amendments):

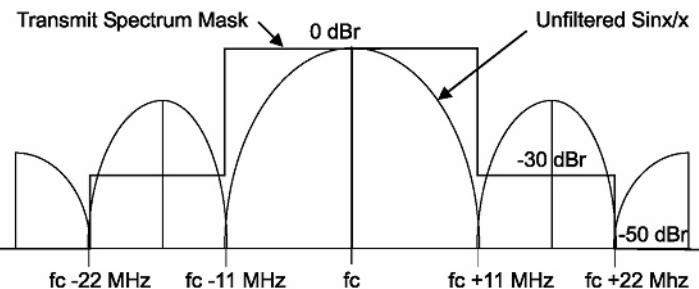


Figure 3-27: Transmit Spectrum Mask for 802.11b

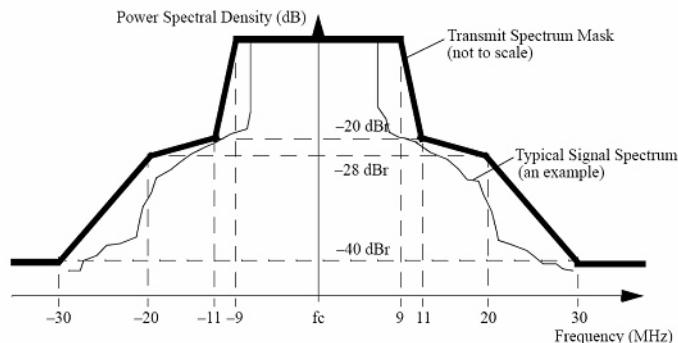


Figure 3-28: Transmit Spectrum Mask for 802.11a/g (20 MHz)

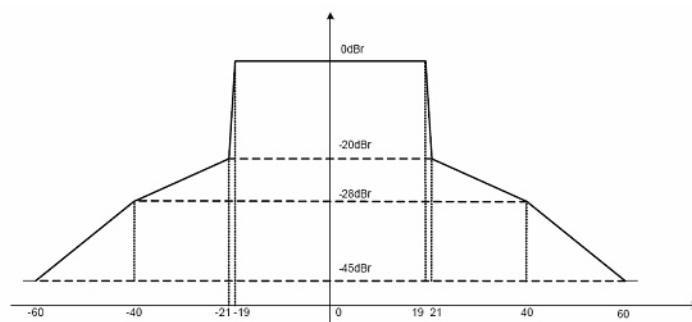


Figure 3-29: Transmit Spectrum Mask for 802.11n (40 MHz)

As illustrated in Figures 3-27 through 3-29, an 802.11 device is allowed to contribute as much as -28 to -50 dBr (decibels relative to peak) on adjacent channels when they transmit. For 40 MHz transmissions in the 2.4 GHz band, RF energy may be present as far away as 11 channels from the center frequency.

AirMagnet WiFi Analyzer uses these spectral properties of 802.11 devices to determine the amount of interference a particular device contributes to a particular (logical) channel.

In calculating an interference score, the following details are taken into consideration:

- 1) The “spectral distance” between the channel of interest and a device’s operating channel (including each of the channel’s widths).
- 2) Whether or not the interference from a device (to a channel) is caused by modulated spectrum (i.e., within the device’s operating channel width), or by the “bleed over” outside the modulated portion of the transmission(s).
- 3) The RSSI (signal strength) of the device.
- 4) The current “bandwidth utilization” of the device; that is, how often it is currently transmitting.

After performing calculations based upon the above, the interference score is normalized, scaled (and potentially capped) for each device in order to provide some consistency with previous versions of the product.

It should be noted that, in this way, a “busy” AP on Channel 6, with very strong signal strength, may contribute more interference to Channel 1, than a less busy AP on Channel 3, with a weaker signal strength (from the capture vantage point).

The list of interfering devices shown on the Interference screen distinguishes between modulated () and un-modulated () interference contributions.

Channel Interference Summary

The left-hand side of the Interference screen allows you to specify which channel you wish to view. The channel listings are divided by media type, with 802.11g channels listed first, and 802.11a channels below. You may collapse list by simply clicking the '+' sign next to the heading. See Figure 3-30.

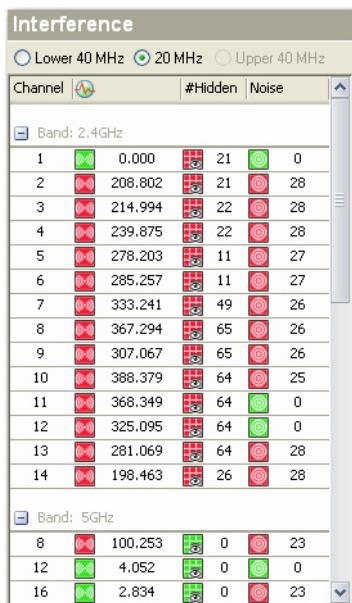


Figure 3-30: Channel Interference Summary

The channels you have available for selection vary depending on the media type you select and geographical location you reside. Different 802.11 media type and countries or regions of the world utilize different channels.

You can filter the content of the channel interference summary by using the radio buttons across the top of this section (Figure 3-30):

- **Lower 40 MHz** – Only the 40-MHz lower channel is shown. Both the legacy and HT packets can be transmitted in lower

40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.

- **20 MHz** –Only 20-MHz channel is shown. This mode is similar to 802.11a/g because the bandwidth required is 20 MHz and the devices present in this network are similar to the legacy devices. Per 802.11n Draft 2 standard, this mode is mandatory.
- **Upper 40 MHz** –Only the 40-MHz upper channel is shown. Both the legacy and HT packets can be transmitted in upper 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.

The channel interference summary contains four data columns which are intended to provide a brief overview of data on each channel. The columns (from left to right) are as follows:

- **The first column** - lists all available channels by 802.11 media band (2.4 GHz vs. 5 GHz). You may show or hide the media bands simply by clicking the '+' or “-” signs at the top of each section.

The channels you have available for selection will vary based on the media band you have selected and the country or region AirMagnet WiFi Analyzer is used; channel allocation may differ from country to country.

- **The second column** - displays the interference scores on the channels in real time.

The icons next to interference scores are color-coded: green for interference scores that aren't considered outside of normal levels (0-4.999); yellow for interference scores that are considered 'warning' signs (5-19.999); and red for severe interference (20 and above) that

requires immediate attention. Table 3-8 below provides a list of the color thresholds for each column.

Table 3-8: Channel Pane Color Codes

	Green	Yellow	Red
Interference	0-5	5.01-20	20.01 or greater
#Hidden	0-1	2-5	6 or greater
#Interferers	0-1	2-5	6 or greater

- **The third column** - displays the number of hidden devices detected on the corresponding channels. Hidden devices can cause interference and traffic collisions within your network, thereby slowing down general network operations (for more details regarding hidden devices, see Hidden Station Detected).
- **The fourth column** - displays the noise level detected on each of the listed devices. It can be in dBm or percentage, depending on the unit of measurement you use from the menu bar.

However, the four column will display the number of non-802.11 interfering devices detected on each of the channels if you have integrated AirMagnet Spectrum Analyzer and are using an AirMagnet Spectrum Analyzer card.

When a particular channel is selected, all areas in the right-hand side of the Interference screen will be updated to show interference- or noise-causing devices that are detected on that channel.

Interfering Devices

The interfering devices pane is made up of two parts. The left part is a table that shows all devices detected on the selected channel as well as the channel, interference score, modulated (SSID) / un-modulated (SSID), channel, signal strength, and SSID of each of the devices; the right part is that Interference Score graph that displays the interference scores of selected devices in the form of line charts. The message across the top of the table tells you about the overall state of RF interference on the channel. See Figure 3-31.

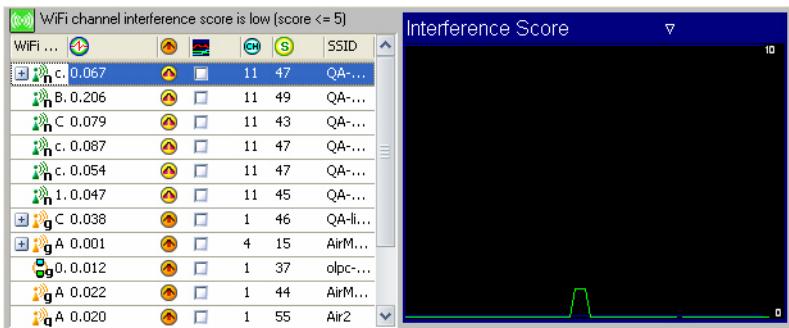


Figure 3-31: Devices and Interference Graph

You can use the check boxes in the middle column of the table to select the devices to be graphed on the Interference Score graph. You may select as many devices as you wish (each selected device is represented by a line chart of a unique color). You can also right-click anywhere in the table and select “Enable All” from the pop-up menu to all devices in the list. However, having too many devices selected at one time may result in a cluttered graph that could be difficult to read. For this reason, you may want to select only the devices of interest to you.

Even when you are focusing on a specific channel, devices from other channels will often appear on the RF Interference screen. This is because these devices are also causing interference on the selected channel. Devices on adjacent channels can cause cross-channel interference.

Hidden Devices

The hidden devices pane is located right below the interfering devices pane. It displays all hidden devices, if any, that are detected on your network. It provides information such as device name, channel, signal strength, and SSID of each hidden devices being detected. The message across the top of this section tells about the total number of hidden devices detected on the channel. See Figure 3-32.

Hidden Devices count is medium (1 < count <= 5 devices)			
Hidden Devices	CH	SN	SSID
GemTek:BD:FC:7F	1	43	Air2
GemTek:BD:FC:7F	1	0	Air2
Senao:22:78:AB	1	41	ShawnXiong_AP, p...
Intel:63:8B:0A	1	8	
Intel:63:9A:C0	1	15	<No current ssid>,...

Figure 3-32: Hidden devices on a channel

Hidden devices represent a problem where two different devices (stations, for example) cannot see each other directly (often due to distance between them). Since the two devices are unaware of each other, they may try to access an AP between them at the same time, causing network collisions. This would result in both stations needing to re-transmit their packets, thus creating a delay in your network traffic. For more information on hidden devices, refer to the “Hidden Station Detected” alarm in the AirMagnet WiFi Analyzer Policy Reference Guide.

Graph Pane

As shown in the preceding screen shots, the interference score graph charts the interference score of the selected channel and devices over time. The bottom portion of the graph pane, however, is more flexible. It graphs data involving the specific device you have selected in the interfering devices pane. See Figure 3-33.

Note that the lower graph does not chart the devices you have **checked**, but rather the one you have **selected** at any given time. Selecting a new device will cause the graph to refresh.

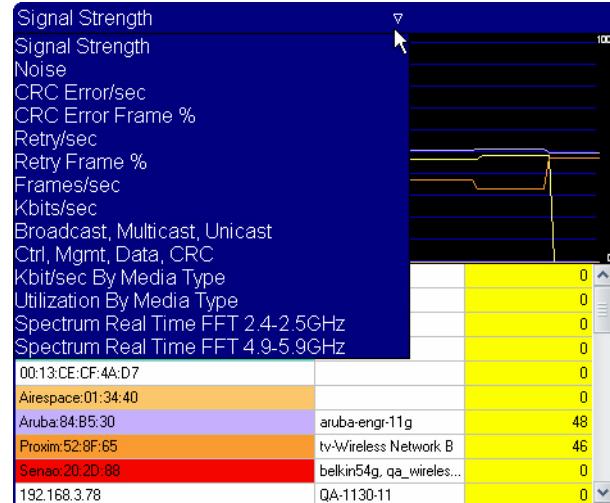


Figure 3-33: Lower graph field

Figure 3-33 displays the graph with no device selected. It charts statistics based on all the devices in the channel. The graph options change, however, when you actually select a device to view. Since this graph is based on the selected device (as opposed to a range of devices you have checked), it provides a wider variety of graph types to view.

AirMagnet Spectrum Analyzer Integration

When you are using AirMagnet WiFi Analyzer integrated with AirMagnet Spectrum Analyzer, the Interference screen can also display a third field below the devices list. It shows any non-802.11 devices that have been detected causing interference. Such devices can include microwaves, cordless phones, Bluetooth devices, wireless

cameras, etc. When such devices are detected, AirMagnet WiFi Analyzer will send out the “Non-802.11 Interfering Source Detected” alarm. The integration also makes available the spectrum graph selection in the graph pane. See Figure 3-34

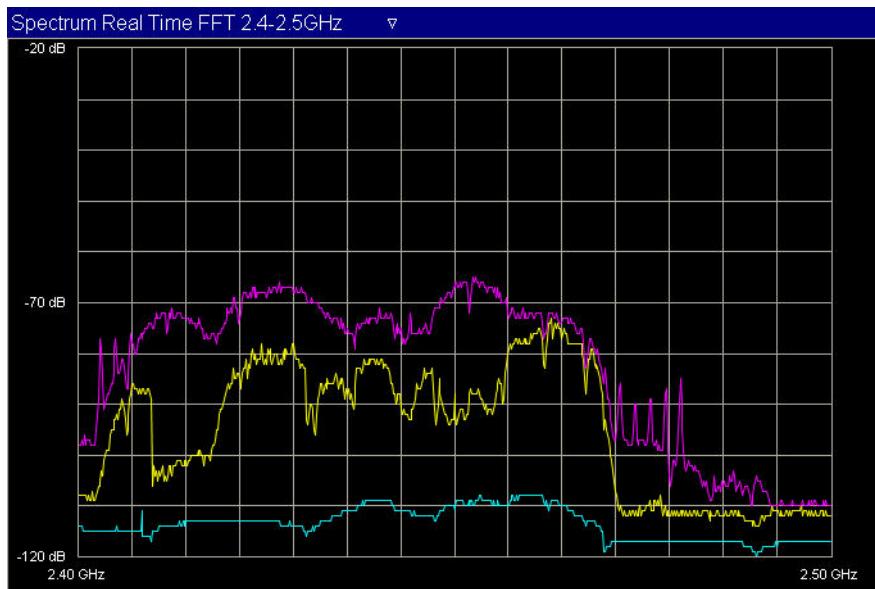


Figure 3-34: AirMagnet Spectrum Analyzer Graph

To enable AirMagnet Spectrum Analyzer:

- 1) Click (Configure) and select the General tab.
- 2) Check Enable Spectrum Analyzer. See Figure 3-35.



Figure 3-35: Enabling AirMagnet Spectrum Analyzer

- 3) Click OK to finish.

Upon enabling the AirMagnet Spectrum Analyzer option, you must restart AirMagnet WiFi Analyzer in order for AirMagnet Spectrum Analyzer to activate. Make sure that you have also inserted your AirMagnet Spectrum Analyzer adapter in the card slot on your laptop computer. After AirMagnet WiFi Analyzer is reloaded, the Interference screen will show a new pane at the bottom, with the AirMagnet Spectrum Analyzer graph option enabled.

RF Spectrum Interferers

The RF Spectrum Interferer pane displays all non-802.11 devices that are interfering with your network's performance as they are detected. See Figure 3-36.

RF Spectrum Interferer	Duty Cycle	Center Freq	Bandwidth	Power	Channel
Generic Wideband	6.20%	2450MHz	18MHz	-70.93dBm	6-10
Generic Wideband	24.14%	2453MHz	10MHz	-72.99dBm	8-10
Generic Wideband	22.24%	2454MHz	9MHz	-74.40dBm	8-10
Generic Wideband	26.57%	2454MHz	8MHz	-75.50dBm	8-10
Generic Wideband	36.97%	2453MHz	11MHz	-76.41dBm	8-10
Generic Wideband	37.07%	2452MHz	10MHz	-75.31dBm	8-10
Generic Wideband	39.34%	2452MHz	10MHz	-74.98dBm	8-10
Generic Wideband	39.02%	2453MHz	10MHz	-74.20dBm	8-10
Generic Wideband	39.14%	2453MHz	9MHz	-74.91dBm	8-10

Figure 3-36: Non-802.11 Interferers

The section below this pane displays information regarding the interferers detected thus far. It gives you an idea of how the interferers are impacting your wireless network's performance.

AirMagnet Spectrum Analyzer Graph

Enabling AirMagnet Spectrum Analyzer allows you to view a graph of the entire 802.11 spectrum, ranging from 2.4-2.5 GHz (for 802.11b/g devices) to 4.9-5.0 GHz (for 802.11a devices). Refer to Figure 3-32.

The AirMagnet Spectrum Analyzer graph displays the FFT (Fast Fourier Transform) plot, which contains three types of data represented by the line charts in distinctive colors. Table 3-9 briefly describes each of these data. If you wish to have more information on AirMagnet Spectrum Analyzer, refer to the *AirMagnet Spectrum Analyzer User Guide* or online Help within the stand-alone AirMagnet Spectrum Analyzer software application.

Table 3-9: AirMagnet Spectrum Analyzer FFT Plot Data

Chart Color	Data Type	Description
Purple	Max Hold	The maximum power value detected at any time since the plot was initiated. <i>Max Hold</i> means that the plot holds onto the maximum power value up to the present.
Yellow	Max	The maximum power value detected during the most recent measurement interval.
Cyan	Average	The average power value detected during the most recent measurement interval.

Working on Infrastructure Screen

You can drill down directly to the Infrastructure screen by clicking a node (e.g., an SSID, Ad-Hoc, AP, or STA) from the Start screen. (See also chapter on Multiple Adapters when multiple WiFi adapters are used.) You may also access the Infrastructure screen by tapping



on the Navigation Bar. See Figure 3-37.

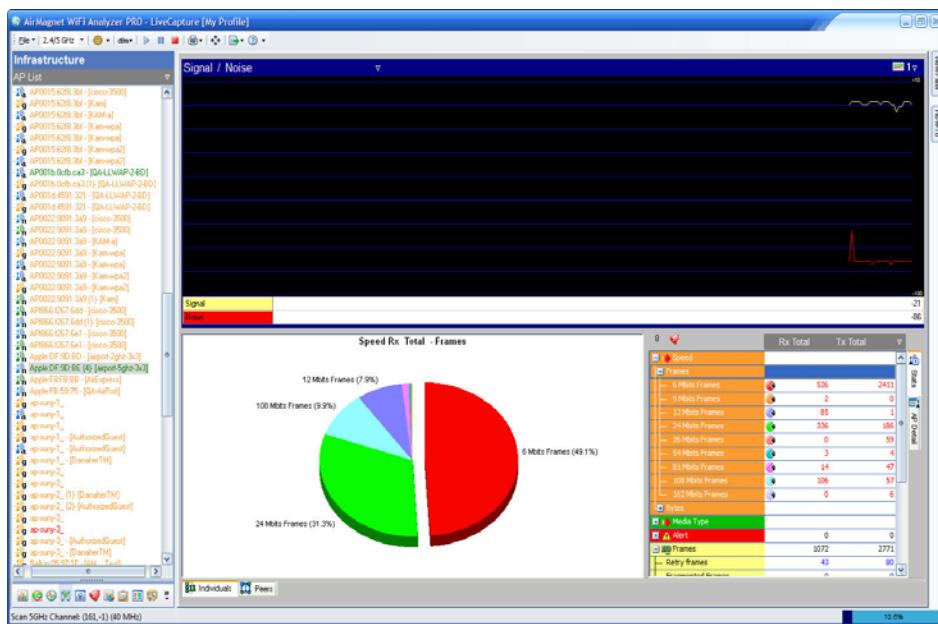


Figure 3-37: Infrastructure screen

Network Tree Structure

The left part of the Infrastructure screen displays in an organized form all nodes detected on your WLAN. You can use the filter at the top of this field to display the network infrastructure by SSID, channel, access point, station, ad-hoc network, 802.1x user, or media type. Selecting an access point will have all associated stations shown under the access point, identified by MAC or IP address. See Figure 3-38.

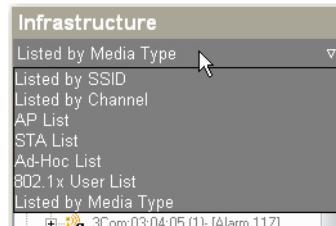


Figure 3-38: Infrastructure screen filters

Network Infrastructure Color Codes

As seen from Figure 3-35, SSIDs, APs, and stations on the network tree structure are color-coded. Each color represents a specific RF signal status as described in Table 3-10.

Table 3-10: Infrastructure RF Signal Color Codes

Color	Description
Green	The device has been active for the last 5 seconds.
Orange	The device has been inactive for the last 5 to 60 seconds.
Red	The device has been inactive for the last 60 to 300 seconds.
Grey	The device has been inactive for more than 300 seconds.

Analyzing Data of Individual Devices

The right-hand side of the Infrastructure screen displays the data for the selected node on the network tree structure. Selecting an AP or station from the network infrastructure allows you to display various detailed information about the selected device.

The Infrastructure Data Graphs

The top of the right-hand side of the Infrastructure screen is a graphical display of data for the selected node on the network tree. You can use the Data Selector at the top left of this pane to choose the data to display and the Graph Options at the top right to select a viewing option. This allows you to view up to six graphs simultaneously. The default graph displays the selected device's signal and noise levels, but you may choose from a variety of graphs similar to the options in the RF Interference page. See Figures 3-39 and 3-40.

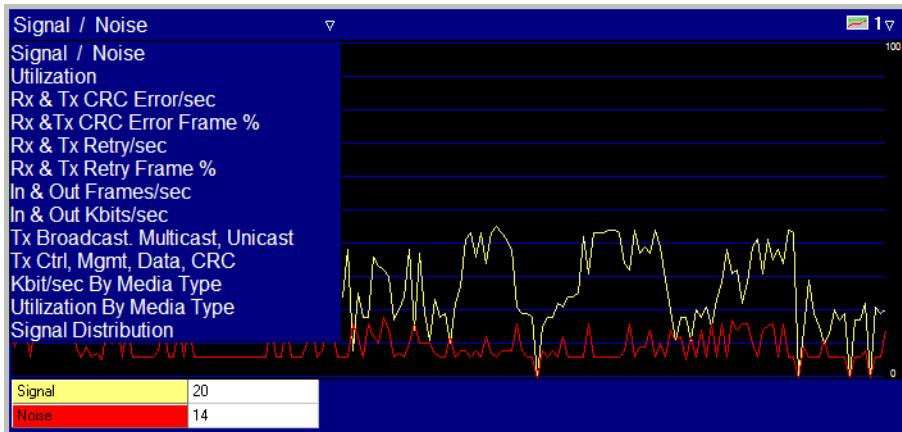


Figure 3-39: Viewing a single data graph

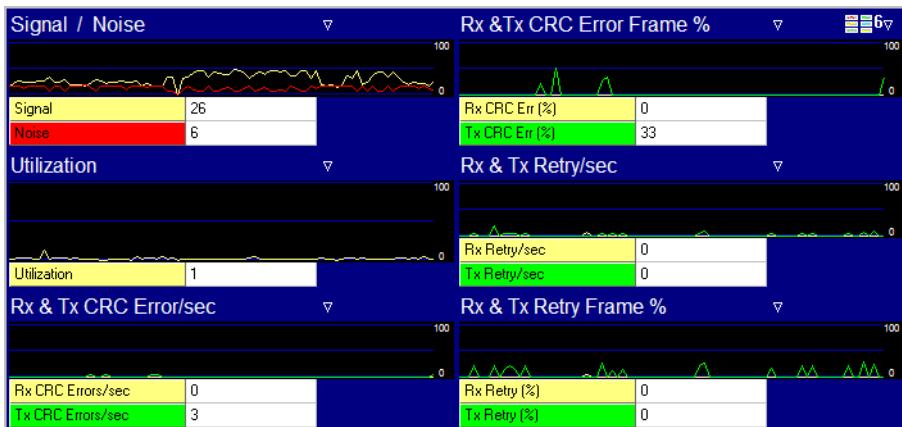


Figure 3-40: Viewing multiple data graphs

Infrastructure Data Summary

The lower part of the screen looks almost the same as what is shown on the Channel screen, but the Infrastructure screen focuses more on the WLAN structural components (i.e., SSIDs, access points, stations, etc.). Therefore, the section at the far right could be AP Detail or Station Detail, depending on the selection made on the network infrastructure.

The AP/Station Detail section shows the authentication mechanisms enabled on the selected device. If a particular device utilizes multiple SSIDs, this section will be repeated for each SSID used.

You can click a plus sign to show detailed data in that category. The selected data are also graphed in the pie chart. You can also customize the data display using the filter in the upper-right corner of the pane. See Figure 3-41.



Figure 3-41: Infrastructure data summary

Figure 3-41 shows the AP Detail field on the far right of the screen, but your view may vary depending on your computer's resolution. A laptop PC with a screen resolution below 1600 x 1200 dpi may show the AP/ Station Detail field listed below the other ones to the immediate right of the pie chart.

Infrastructure Data Pie Chart

The pie chart displays data for the selected AP or station from the network tree. You can display the data by Speed, Alert, Frames, Control Frames, Management Frames, or Data Frames by clicking the corresponding icon on the right. The chart is color-coded and each slice is labeled with its data type and percentage of the overall chart.

Alarm Status

The alarm status above the data summary field shows the number of alarms that have been logged involving the selected network nodes (i.e., SSID, AP, or station). Clicking  will take you to the AirWISE screen where you can view detailed information about the alarm(s).

802.11d/h Information

Two additional fields that aren't found in the Channel screen provide information regarding any 802.11d or 11h packets detected. The 802.11d specification is much like 802.11b except that 802.11d allows its configuration to be modified at the MAC layer in order to ensure that a network complies with any local rules or regulations. Systems that utilize 802.11d may adjust frequency settings, power levels, and a number of other specifications; this ensures that 802.11d is ideal for systems that will be used in multiple different areas across the world because it can be adapted to suit almost any standard. AirMagnet WiFi Analyzer will allow you to view the settings of any device utilizing 802.11d so that you may ensure that all of your devices use the same settings.

802.11h addresses restrictions placed on the 5-GHz frequency currently used by 802.11a devices. The International Telecommunication Union created this set of standards in order to prevent potential interference between 802.11a devices and satellite communications systems. AirMagnet WiFi Analyzer provides an easy view of all the information contained in any 802.11h packets detected on your network.

Viewing Connections between Devices

Clicking the Peers tab at the bottom of the Infrastructure screen changes the Infrastructure screen display to peer-to-peer mapping. It allows the user to visualize the relationship between wireless stations at Layers 2 and 3 when they are associating with each other. There are two scenarios as indicated by the drop-down menu in the upper-left corner of the graph screen: Peer-to-Peer and Peer-AP-Peer.

Peer-to-Peer Connections

The Peer-to-Peer graph shows two wireless stations directly associating with each other, without the aid of an AP. All stations are marked in white; the lines joining the stations are of different colors which are assigned randomly for the sole purpose of easy differentiation. See Figure 3-42.

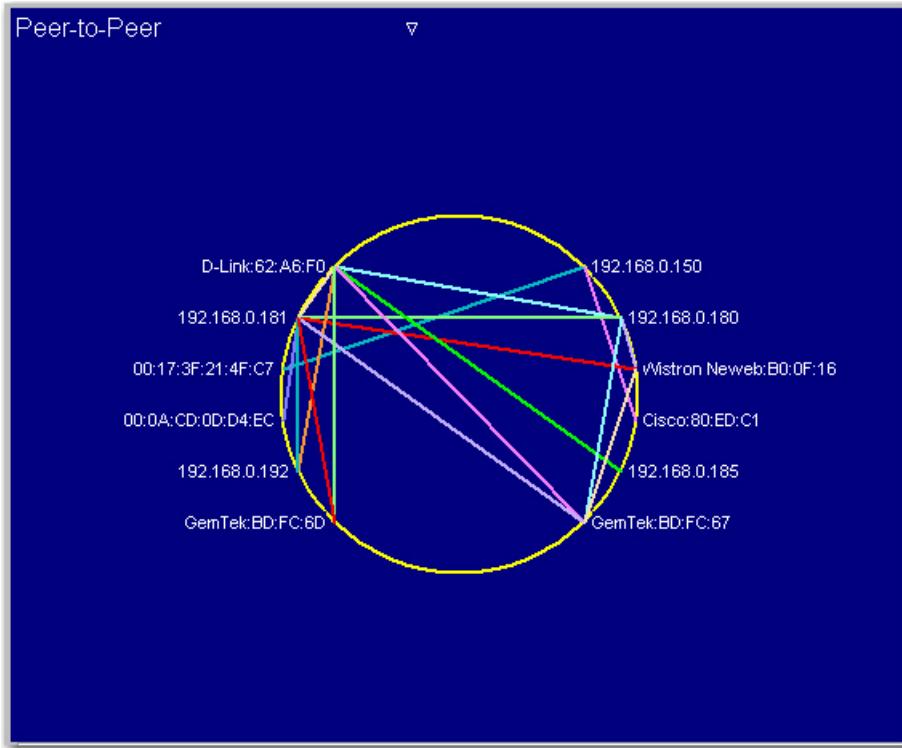


Figure 3-42: Peer-to-Peer connections

Peer-AP-Peer Connections

The Peer-AP-Peer view shows that stations are associating with each other through an AP. See Figure 3-43.

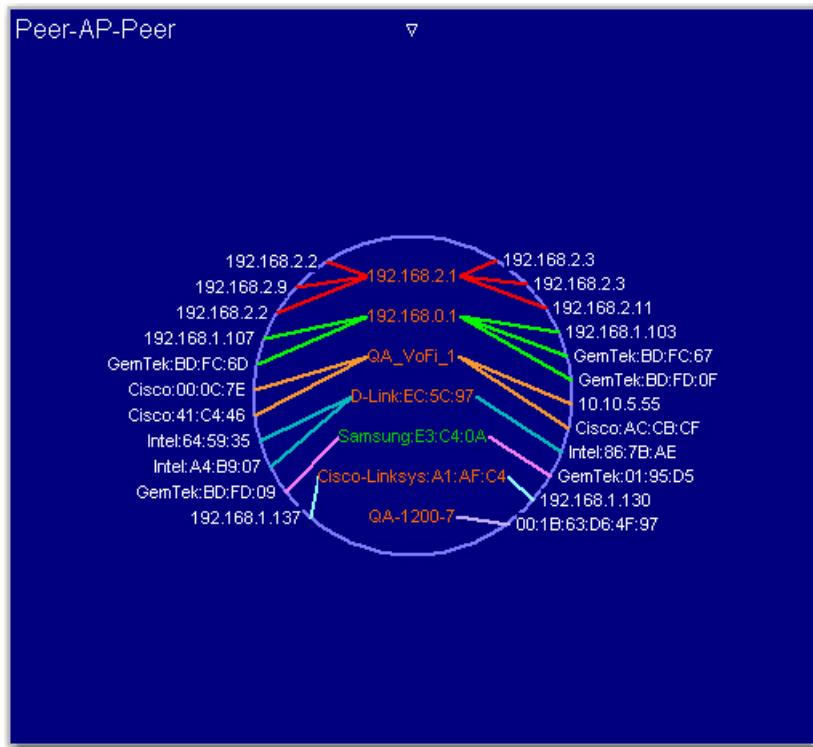


Figure 3-43: Viewing connections between devices

As shown in Figure 3-42, the APs and stations shown in the Peer-AP-Peer connection map are identified by device name, MAC address, vendor name, or a combination of vendor name and MAC address, etc. The entries inside the circle are APs while those outside the circle are stations. The APs are color-coded, reflecting the 802.11 protocols that are used on them:

- Blue – 802.11a
- Green – 802.11b
- Orange – 802.11g
- Green (for 2.4 GHz) and Blue (for 5 GHz) – 802.11n

The lines between APs and stations are also of different colors. However, unlike the color scheme used for APs, the colors for the lines are randomly assigned and merely indicate the order in which the connections are established.

Working on AirWISE Screen

AirMagnet's alarm feature is driven by AirMagnet AirWISE—AirMagnet's patent-pending intelligence analytical engine that helps network professionals monitoring network security and performance status, pinpoint problems, and assist in problem resolution.

You can drill down directly to the AirWISE screen by double-clicking **Security or Performance** under AirWISE Advice from the Start screen, by clicking  on any of the screens, or selecting

 on the Navigation Bar. See Figure 3-44 and Chapter 9 on Multi-Adapters.

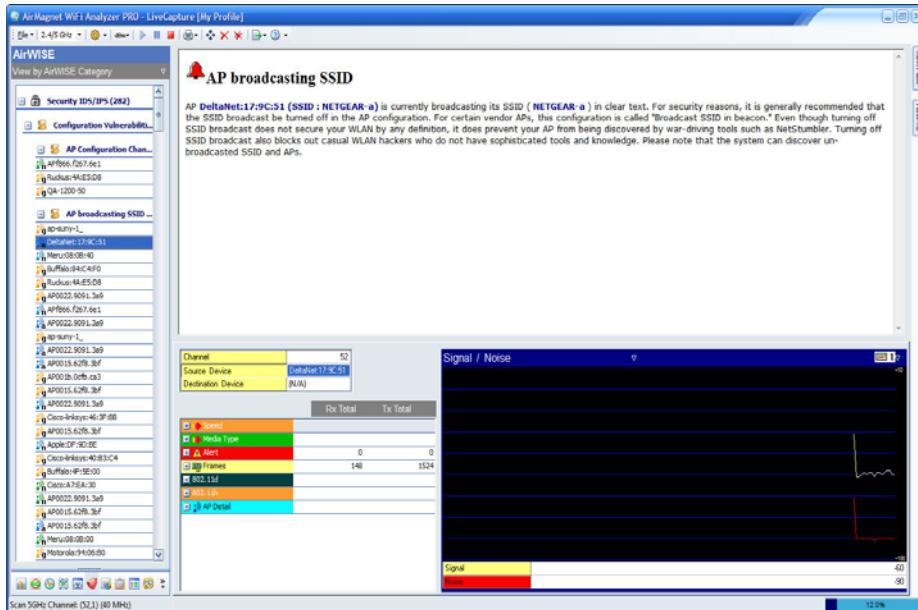


Figure 3-44: AirWISE screen

AirWISE Screen Viewing Options

The left-hand side of the AirWISE screen displays network alarms that have been captured by AirMagnet WiFi Analyzer since the beginning of the session. The alarms are listed according to the viewing option the user selects. You can select an option using the filter across the top of the screen. Simply click the down arrow and select an option from the drop down list. See [Figure 3-45](#).

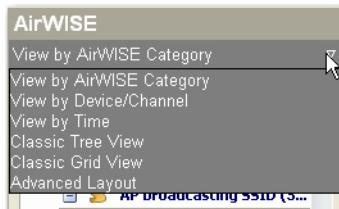


Figure 3-45: AirWISE screen viewing options

As shown in [Figure 3-45](#), the AirWISE screen offers the following viewing options:

- **View by AirWISE Category** - This option displays alarms by the structure of the AirMagnet AirWISE network policy.
- **View by Device/Channel** - This option displays alarms by channel or by device.
- **View by Time** - This option displays alarms by the time they are captured: alarms that are captured within a certain time frame are grouped together; alarms in the same time frame are then further divided by the structure of the AirMagnet AirWISE network policy.
- **Classic Tree View** - This option displays alarms using the classic AirMagnet tree structure which is based on the structure of the AirMagnet AirWISE network policy. All alarms belong to the same policy category are grouped together. It also shows the level of severity of each alarm. In this view, the severity of an alarm is indicated by the icon in front of it, as explained in Table 3-11:

Table 3-11: Alarm Icon and Alarm Severity

Icon	Severity
	Critical
	Urgent
	Warning
	Informational

Managing Alarm List

AirMagnet displays all alarms as they occur. Normally, the alarms are listed in the order they were generated, with the oldest one appearing on top of the list.

The alarms, especially those that have been taken care of, can be removed from the Alarm List using the following options:

- Delete the selected alarm or the one on top of the list.
- Delete all alarms at once.

You may also right-click any alarm and select “Delete Alarm” from the resulting menu.

Analyzing Network Policy Alarms

The right hand-side of the AirWISE screen is the Expert Advice screen. It provides event-driven explanations and detailed analysis of the policy or policy violation selected from the Alarm Tree.

Tip: The policy hierarchy on the left-hand side of the AirWISE screen governs the way data are displayed on the Expert Advice screen. As you drill down deeper into the policy

structure, the information becomes more specific. See [Figure 3-46](#).

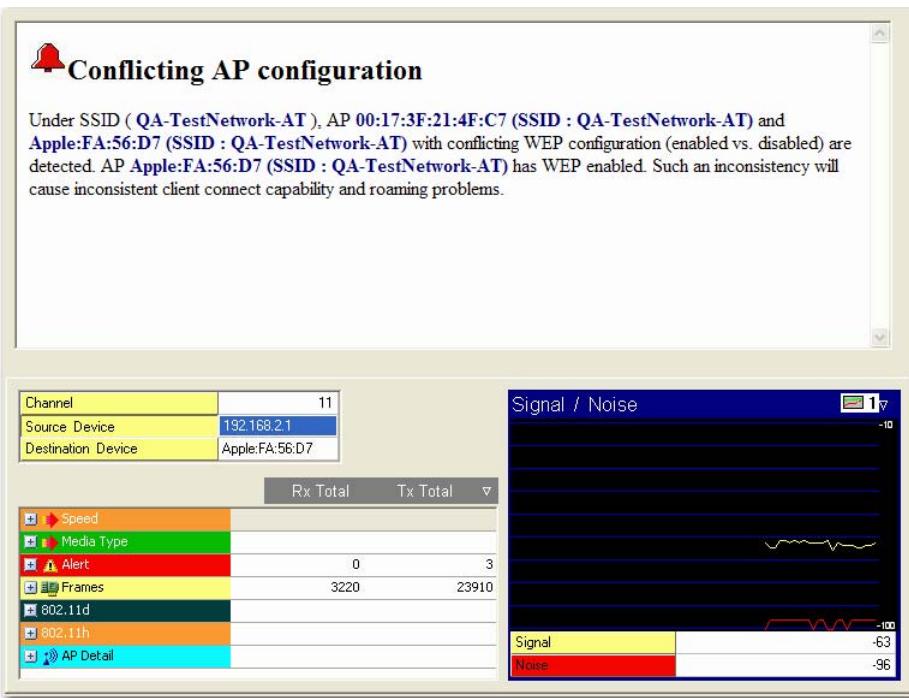


Figure 3-46: AirWISE alarm selected

As shown above, when you have a specific alarm selected, the top pane will display exactly which device caused the alarm and how it did so. The lower pane contains a summary of packet information from the device in question, much like the summary panes in the Infrastructure screen. To find advice regarding how to resolve the alarm, select the alarm subcategory in the AirWISE tree pane on the left.

Expert Advice

The Expert Advice provides detailed explanation of the selected policy, event, or alarm. It warns of the potential risk of the policy breach and offers solutions for the identified issues or problems. The user may need to use the scroll bar or arrow along the right edge of the screen to access the complete advice.

Data Analysis

The Data Analysis section shows the channel where the alarm has occurred, as well as the source and destination node of the link. It allows you to conduct detailed analysis of the selected alarm. The screen provides two display options: Details and Graph. The former is a tabulated summary of data in terms of Speed, Alert, Frames, Control frames, Management Frames, Data Frames, and AP Details or Station Detail; the latter provide a graphical display of data in six different viewing options. You can toggle between the two options using the tabs along the right edge of the screen. [Figure 3-47](#) shows the Data Analysis screen when the Graph tab is selected. If the screen resolution is high enough or if the screen itself is wide enough, the contents for each tab will be displayed in a separate screen.

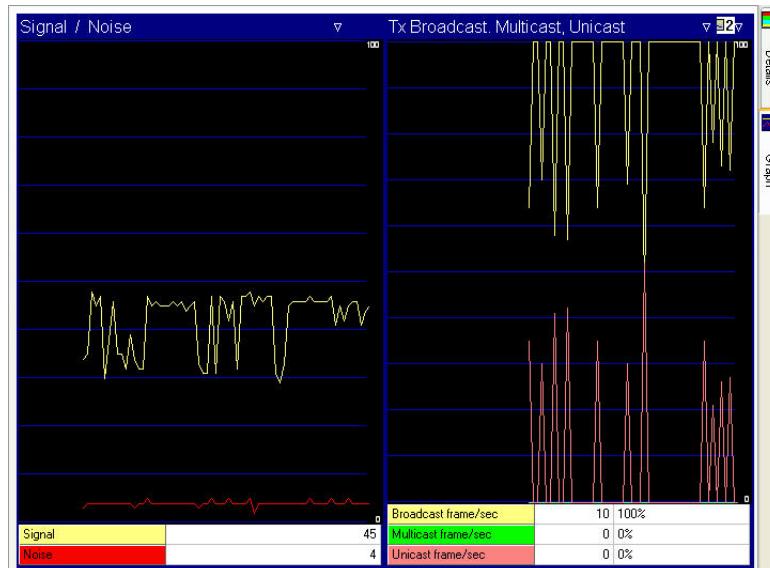


Figure 3-47: Infrastructure screen data graphs

Notice that the data tabulation and graphs are the same as those shown on the Infrastructure screen.

Viewing All Alarms Generated by a Specific Device

This feature allows you to view all alarms generated by a specific device on the same screen. It provides a way for you to organize and view alarms by device, making alarm analysis device-centric.

To display all alarms triggered by a specific device:

- 1) From the Network Policy Hierarchy section, select a policy category and expand it to the alarm level.
- 2) Right-click an alarm, and select **View Device Alarms** from the pop-up menu. See [Figure 3-48](#).



Figure 3-48: The right-click menu

Once you click **View Device Alarms**, the AirWISE screen will refresh and it will focus on all alarms generated by the same device. See [Figure 3-49](#).

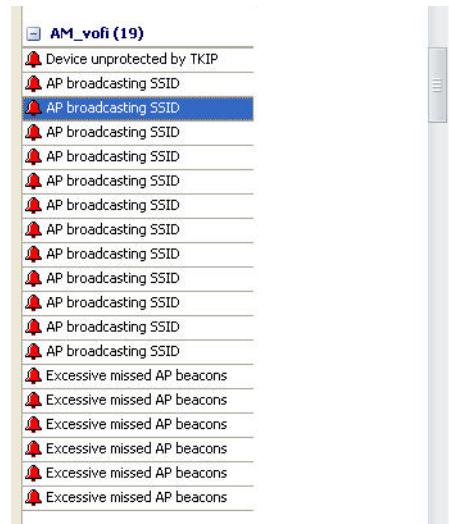


Figure 3-49: Viewing device-specific alarms

- 3) Click each alarm to view the information about the device and alarm description.
- 4) To return to the general AirWISE screen, click the filter down arrow above the Network Policy Hierarchy and select **View by AirWISE Category** from the drop-down list. Refer to [Figure 3-45](#).

Working on Top Traffic Analysis Screen

The Top Traffic Analysis screen allows you to view and analyze data in the form of charts. There are several options for the screen: most show data about the wireless devices (including 802.11n devices) detected on your WLAN, but the compliance section presents data about your network's compliance with government and industry regulations regarding information security.

To access the **Top Traffic Analysis** screen, click  on the **Navigation Bar**. By default, the screen displays device data when it opens. See [Figure 3-50](#) and Chapter 2 on Multi-Adapters.

Users running at 800x600 resolution will see a drop-down menu that allows them to zoom in on the charts displayed. It is recommended that the Refresh box be unchecked when using the zoom feature.

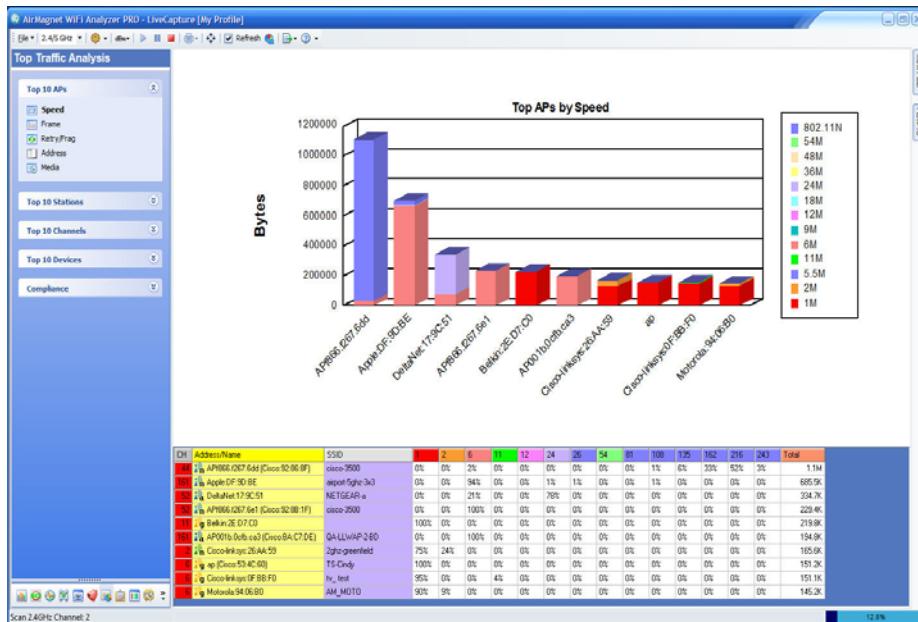


Figure 3-50: Top Traffic Analysis screen

The Top Traffic Analysis Screen refreshes frequently, which may cause a flickering effect on your screen. You may uncheck the refresh box in the tool bar to prevent this.

Top Traffic Analysis Screen UI Components

As shown in Figure 3-50, the Top Traffic Analysis screen has three different panes:

- The charts navigation pane on the left allows you to select the type of data you wish to view a chart regarding.
- The main display pane in the top right displays the currently selected chart.
- The devices pane on the bottom right displays specific statistics regarding the devices shown in the chart above.

Viewing Device Charts

By default, all the channels and SSIDs are selected when the Top Traffic Analysis screen opens. And the screen can provide graphical display of the top 10 devices in the following categories as indicated in [Figure 3-51](#). The Compliance section below displays the various compliance charts, giving you a detailed summary of how well your network complies with regulatory security standards.



Figure 3-51: Selecting a top 10

Each top 10 category can then be further divided by data type as shown in the Data Type drop-down list displayed under each section heading.

Normally, you can view a device chart by selecting a top 10 category and then choosing a data type. The screen will then display the top 10 most active devices in the selected category. However, if you want to view the most active devices in certain SSIDs or on certain channels, you can do so by using the View Filter tab to select only the SSIDs or channels in which you are interested. In this case, the device chart may still be capable of displaying data of up to 10 devices, but the actual number of devices displayed depends on the number of devices that are active in the SSIDs or on the channels. [Figure 3-52](#) shows a device chart for only 6 devices on a single SSID.

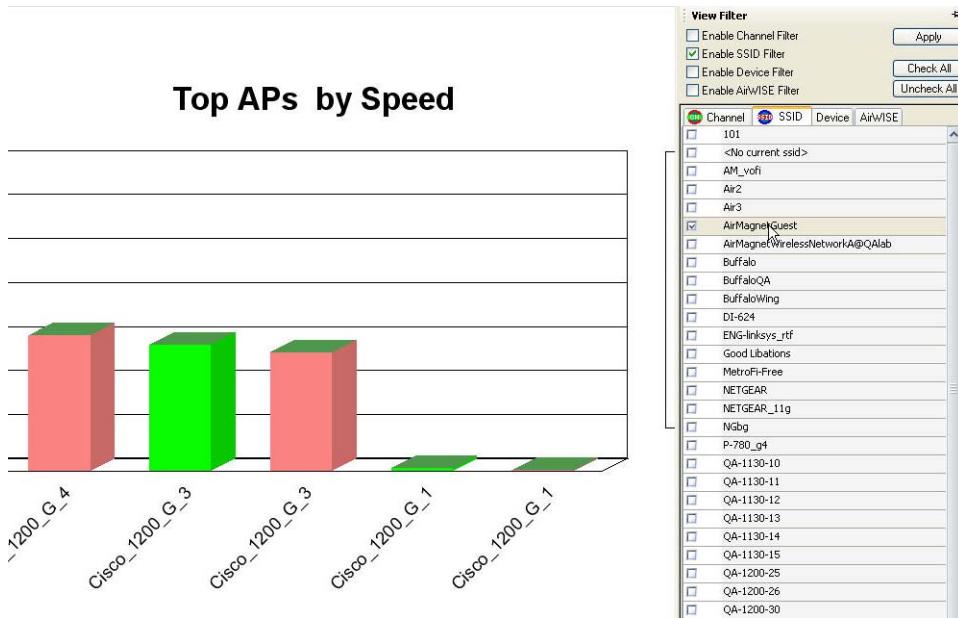


Figure 3-52: Filtering device chart by SSID

Exporting Chart Data

You can export the data contained in the current chart by clicking (Export Data) at the top of the Charts screen and selecting “Export Top Traffic Analysis”. A confirmation message will pop up on the screen, indicating that the export is successful. See Figure 3-53.



Figure 3-53: Export confirmation

Choosing a Graph Option

AirMagnet allows the user to configure their chart settings using the **Graph Options** button on the Charts screen.

To configure chart settings:

- 1) Click  at the top of the screen. The Graph Options dialog box appears. See [Figure 3-54](#).

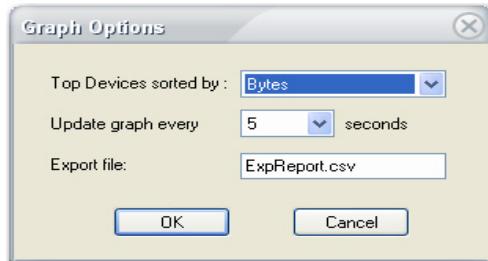


Figure 3-54: Configuring graph settings

- 2) Make the desired selections, and click OK.

Chart Data Tabulation

Below the graph is a table that offers a breakdown of the selected data type for the top 10 devices. See [Figure 3-55](#).

CH	Address/Name	SSID	1	6	9	12	18	24	36	48	54
11	warlord (Cisco:A7:EA:30)	QA-1250-roam	0%	6%	0%	8%	0%	0%	15%	9%	5%
4	3Com:03:04:05	Alarm 54:DoS EAPStart, A...	0%	100%	0%	0%	0%	0%	0%	0%	0%
7	Cisco:44:5E:B1		0%	39%	41%	2%	1%	2%	3%	2%	4%
7	Cisco:4D:E8:F1		0%	6%	10%	10%	18%	35%	17%	0%	0%
13	QA-Euro-Cisco (Cisco:A7:FC:F0)	QA-EURO-CISCO	27%	71%	0%	0%	1%	0%	0%	0%	0%
11	Buffalo:4F:5E:00	AirMagnetNetworkG@QAL...	18%	56%	12%	9%	3%	0%	0%	0%	0%
9	AMS-1200-5 (Cisco:44:13:20)	AMS-1200-5	100%	0%	0%	0%	0%	0%	0%	0%	0%
7	Cisco:4D:E9:11		0%	8%	39%	14%	8%	20%	0%	8%	0%
1	Cisco-linksys:40:B3:C4	XXX-ENG-NGbg	100%	0%	0%	0%	0%	0%	0%	0%	0%

Figure 3-55: Data tabulation

This table complements the information displayed in the chart and helps the user to better understand the chart.

The grid in [Figure 3-55](#) expands dynamically. More columns are dynamically added to each speed grid as data at that particular speed are observed. Also, once a column is added, it is retained in the grid for as long as the capture continues even though data at that speed might not be seen anymore.

Tip: If the top 10 channels are graphed, clicking in the table will open the Channel screen.

Viewing Compliance Charts

Compliance charts and reports are available in AirMagnet WiFi Analyzer PRO only.

The Top Traffic Analysis screen also allows you to view charts that reflect your network's compliance status with government and industry regulations on information security. The compliance charts give you a general idea of your network's health; for more detailed information regarding a specific compliance regulation, you may generate a comprehensive report for your network and view it using the Reports page. [Figure 3-56](#) shows all options for regulatory compliance.



Figure 3-56: Compliance data options

The compliance charts provide you with an easy-to-view summary of your network's compliance with various industry standards. The following sections briefly describe some of the compliance reports provided by AirMagnet.

Basel II

The Basel II Accord promotes greater consistency in the way banks and banking regulators approach risk management. It is designed to establish minimum levels of capital for internationally active banks. In specific regard to AirMagnet, Basel II incorporates an explicit capital charge for operational risk. Operational risk includes the security risks in operating a wireless network. Basel II succeeds the Basel I Accord. Both were developed by the Basel Committee on Banking Supervision (hereinafter, the Committee). The Committee is made up of bank supervisors and central bankers from the Group of Ten (G10) countries. The G10 countries include: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States. International banks can use AirMagnet products and Compliance Reports™ to identify and mitigate the operational risks of maintaining a wireless network.

DOD 8100.2

The Department of Defense (DoD) Directive Number 8100.2 (the Directive hereafter) stipulates the key policy sections regarding the use of commercial wireless devices, services, and technologies in the DoD. Its purpose is to safeguard the DoD networks from the security vulnerabilities inherent with wireless networks, making security a prerequisite for the deployment and use of commercial wireless technologies in the DoD.

EU-CRD

The European Union (EU) Capital Requirements Directive, popularly known as CAD3 (Capital Adequacy Directive), implements the Basel II Accord and introduces new capital requirements for internationally active banks, credit institutions, and investment firms in the EU. It succeeds earlier directives that implemented the capital requirements found in the Basel I Accord. AirMagnet System- and Device-level Compliance Reports™ will identify the operational risks in wireless networks that may lead to system disruptions or failures and external fraud.

FISMA

The Federal Information Security Management Act (FISMA) mandates that Federal agencies like the Department of Health and Human Services, the FCC (Federal Communication Commission), and the FTC (Federal Trade Commission) develop, document, and implement an information security program to provide security for the information and information systems that support the operations and assets of the agencies. This includes the information and information systems provided to the agency from another agency or from a contractor.

FISMA applies to the following:

- All information in the Federal government except information marked as classified.
- All information systems except those operating as national security systems.
- Any organization that is a government agency, sells hardware and/or software to a government agency, or supports the information or information systems of a government agency.

GLBA

The Gramm-Leach Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, mandates that financial institutions protect the security and confidentiality of their customers' personally identifiable financial information.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed to improve the efficiency and effectiveness of the nation's health care system and promote the use of EDI (Electronic Data Interchange) in health care. To accomplish its purpose, regulations were issued by HHS (Department of Health and Human Services) to safeguard the privacy and security of the PHI (Protected Health Information). PHI is any health information that identifies an individual and relates to his or her physical or mental health.

ISO 27001

ISO/IEC 27001:2005 (hereinafter ISO 27001) is an International Standard designed for all sizes and types of organizations (government and non-government). At base, the International Standard should be used as a model to build an Information Security Management System (ISMS). An ISMS is part of an organization's system that manages networks and systems. It is premised on business risks and aims to "establish, implement, operate, monitor, review, maintain, and improve information security." Going beyond the model, organizations can attain an ISO 27001 certification from independent auditors. A certification can show an organization's commitment to security and instill trust with partners and customers. It can also be used as evidence in compliance with legal requirements, but it will not, in itself, satisfy legal requirements. Independent auditors like ISOQAR and Lloyd's Registered Quality Assurance (LRQA) certify an organization's compliance with ISO 27001. Note that the American National Accreditation Body (ANAB) in the United States and the United Kingdom Accreditation Service in the United Kingdom regulate ISO 27001 auditors. AirMagnet Enterprise can satisfy ISO 27001 and 17799 requirements for wireless networks and devices with System Level, Policy Level, and Device-Specific Compliance Reports. Using the ISO 27001 Plan-Do-Check-Act model, AirMagnet solutions can help an organization PLAN, CHECK, and ACT to improve an ISMS.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed by Visa and MasterCard to prevent identity theft and credit card fraud. It is a standard required of Visa and MasterCard Members, service providers, and merchants and one voluntarily adopted by other card associations like American Express and Discover Card as a condition for participation. Participating businesses must comply with 12 "best practice" requirements for wireline and wireless networks and validate their compliance periodically.

SOX

The Sarbanes-Oxley (SOX) Act, also known as the Public Company Accounting Reform and Investor Protection Act, was passed by the US Congress in 2002 as a comprehensive legislation to reform the accounting practices, financial disclosures, and corporate governance of public companies.

Viewing Compliance Charts

To display a Compliance chart:

- 1) Select the compliance chart you wish to display from the Compliance section in the left-hand pane. See Figure 3-57.

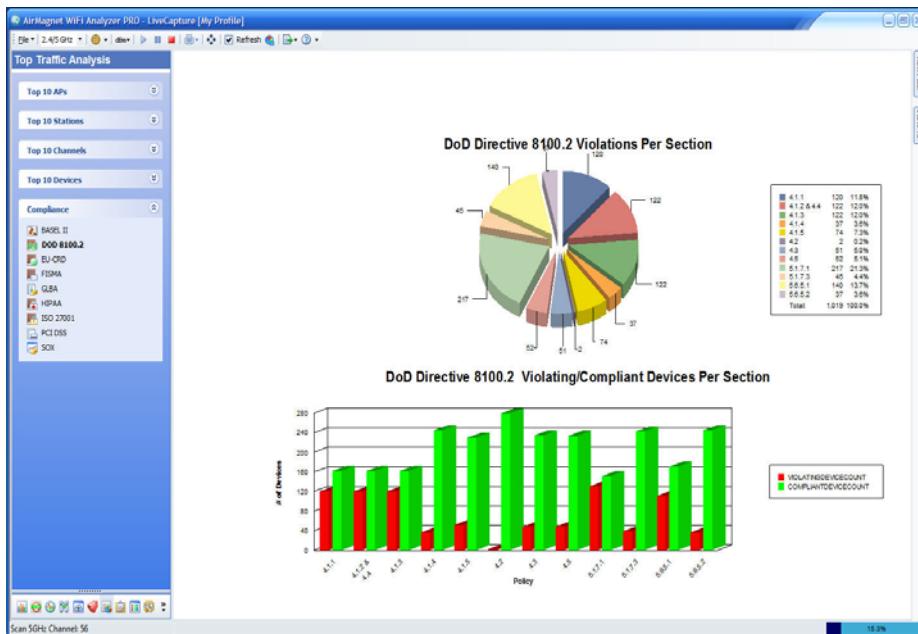


Figure 3-57: A compliance chart

Viewing Compliance Reports

Compliance data are also available in compliance reports. You can access the reports screen by clicking  from the navigation bar and selecting the type of report you wish to generate. See Chapter 9 and 10 for more information.

Compliance Reports Disclaimer

AirMagnet DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley, and Payment Card Industry Data Security Standard (PCI DSS)

Compliance Reports provide a security framework to comply with regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on wireless network security and aim to guide network administrators in documenting their security policies and responding to security threats and incidents in compliance with industry best practice and government regulations.

AirMagnet Policy Compliance Reports provide information about the law and are designed to help users satisfy government regulations. This information, however, is not legal advice. AirMagnet has gone to great lengths to ensure the information contained in the Policy Compliance Reports is accurate and useful. AirMagnet recommends you consult legal counsel if you want legal advice on whether our information and software is interpreted and implemented to fully comply with industry regulations.

The information contained in the Policy Compliance Reports is furnished under and subject to the terms of the Software License Agreement ("License"). The Policy Compliance Reports do not create a binding business, legal, or professional services relationship between you and AirMagnet. Because business practice, technology, and governing laws and regulations vary by location, full compliance with regulations will depend on your particular circumstances.

Working on Decodes Screen

You can access the Decodes screen by clicking  on the Navigation Bar. See [Figure 3-58](#). See also chapter on Multi-adapter when multiple WiFi adapters are used.

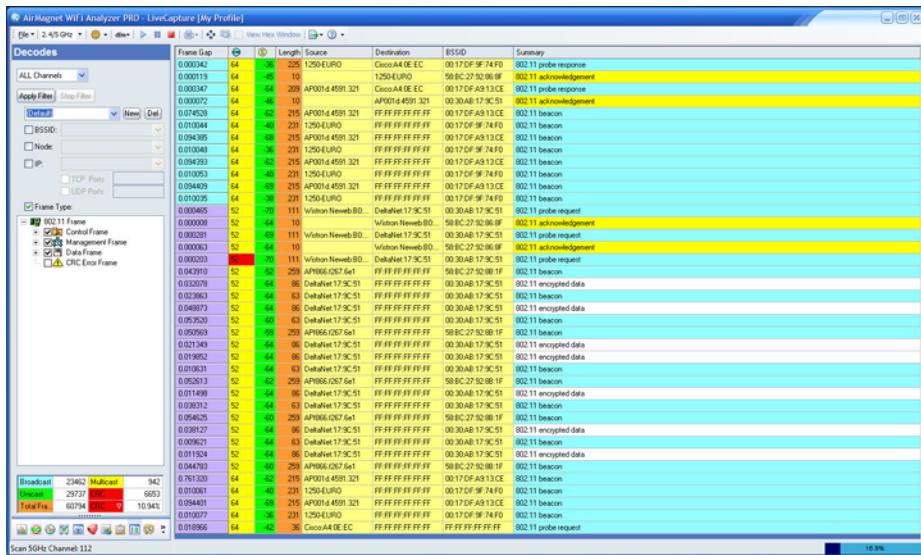


Figure 3-58: Decodes screen

The Decodes screen lets you view a scrolling list of packet frames as they are captured. Table 3-12 briefly describes the information on the Decodes screen.

Table 3-12: Decode Screen Parameters

Field	Description
No	The sequence of the captured packets. Shown only when packet capture is stopped.
M	Check the box in this field to start the frame count from the selected packet. The Delta column will then start with that packet at 0, and number accordingly for future packets. Shown only when packet capture is stopped.
Time	Time the packet was received. Shown only when capture is stopped.

Table 3-12: Decode Screen Parameters

Field	Description
Frame Gap	The time gap between two frames.
Delta	The time elapsed between each packet. Shown only when capture is stopped.
CH	Channel.
S	Signal strength.
Length	Frame length.
Speed	The speed at which the packet was transmitted.
Source	Source node.
Destination	Destination node.
BSSID	The source BSSID.
Summary	Data packet summary.

The bottom portion of the Decodes page provides a meter that gives the user information regarding the current status of the capture buffer. As the buffer fills, the meter will gradually approach 100%. After the first fill, the meter will restart using a different color, thus allowing the user to monitor how many cycles the buffer has been through since the last status check.

Add/Remove Columns

You may adjust which columns to display in the Decodes table by using the Add/Remove Columns dialog.

To Add or Remove Columns in the Decodes table:

- 1) Right-click a column heading in the Decodes table to display the Set Display Columns pop-up. Select Set Display Columns. See Figure 3-59.

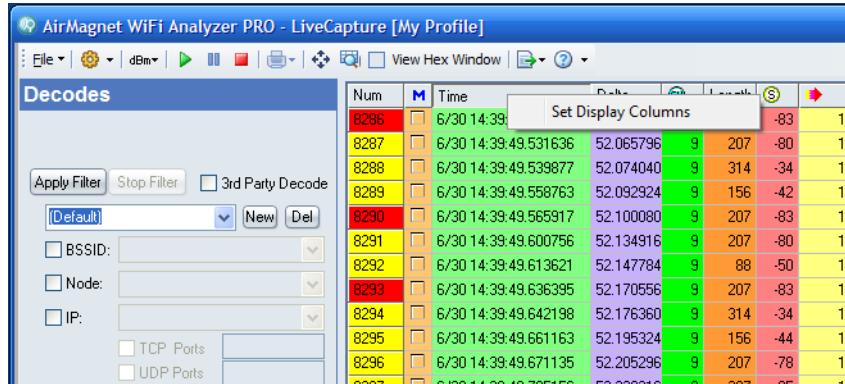


Figure 3-59: Set Display Columns

- 2) Use the check box controls to set the columns to display. Click OK. See Figure 3-60.

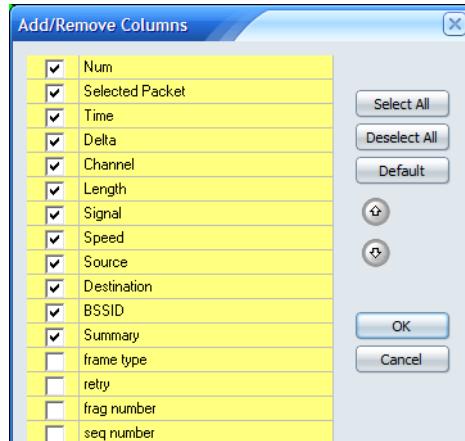


Figure 3-60: Add/Remove Columns

Filtering Packet Captures

The left side of the Decodes screen is a filter pane. Filters are used to define the data displayed on the screen. The application comes with a default filter. You can also create filters of your own using a number of parameters, such as SSID, node, IP address, frame type, etc. To use a filter to screen the data shown on the screen, you must select a filter and click the “**Appl y Filter**” button.

All filters are optional. They are intended to help users focus their analysis on a specific channel, SSID, node, IP address, or types of frames if they want to. Also, the filters can be used individually or in any combination that the application allows.

To stop the use of a filter, click the **Stop Filter** button.

Creating a New Filter

AirMagnet WiFi Analyzer allows users to create filters using filter settings of their choice. These filters, once created, will be automatically saved in the application for future use until they are deleted.

To create a new filter:

- 1) Click the **New** button and rename the [**New Filter**] with a unique name.
- 2) If you want to focus on a specific SSID, check **SSID** check box and select it from the list menu.
- 3) If you want to focus on a specific node on the network, check the **Node** check box and select the MAC address of that node from the list menu.
- 4) If you want to focus on a specific IP address, check the **IP** check box and select the IP address from the list menu. You may also want to specify the TCP and/or UDP port if you have that information available.
- 5) Select the frame or frames of interest.

Applying a Filter

Filters, once created, can remain available each time you launch the application. They make it easy for viewing traffic by channel, SSID, node, IP address, frame type, or a combination of some or all these parameters.

To use a filter:

- 1) Decide which channel you want to focus on. If you want to focus on a specific channel, then click the down arrow across the top and select the channel of interest. Otherwise, do nothing so that the screen can show frames captured on all available channels
- 2) Click the down arrow and select the filter of interest. See Figure 3-61.

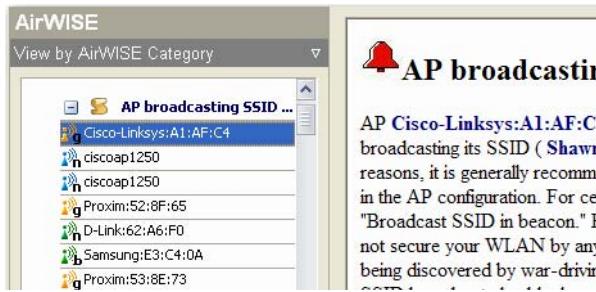


Figure 3-61: Choosing a custom filter

- 3) Click **Apply Filter**.

*Once a filter is activated, it will filter the data displayed on the screen using the parameters of the filter. You can deactivate a filter by clicking **Stop Filter**.*

Deleting a Filter

Filters, including the Default filter, can be deleted from the filter list menu at any time.

To delete a filter:

- 1) From the filter list menu, select the filter of interest. See Figure 3-61.
- 2) Click the Del button.

Conducting Packet Decoding

By default, the Decodes screen shows the data packets as they are captured live in a first-in first-out scrolling order. To conduct detailed packet analysis, you have to stop the screen from scrolling so that you can take a closer look at any packet of interest.

Note: If the upper-layer decode support feature (3rd party decodes engine) was installed during product installation, you may switch between the default decode engine and the 3rd party decodes engine while viewing the captured data. If you did not choose to install this feature during application installation, you may choose to install it at any time from the Configuration dialog>Filter tab.

Figure 3-62 shows the view using the 3rd party decodes engine. Figure 3-63 show the normal view.

Using the 3rd party decodes engine, unencrypted data will also provide upper layer decoding.

N.	M	Time	Delta	Length	S	Source	Destination	BSSID	Summary
1	<input checked="" type="checkbox"/>	6/20/17:13:51.722500	0.000000	6	82	-63	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1
2	<input type="checkbox"/>	6/20/17:13:51.824818	0.102318	6	82	-63	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1
3	<input type="checkbox"/>	6/20/17:13:51.850925	0.128425	6	76	-62	1 00:14:A5:31:F2:E4	Proxim:CA:53:8A	00:14:A5:31:F2:E4 IEEE 802.1
4	<input type="checkbox"/>	6/20/17:13:51.851391	0.128691	6	10	-55	1	00:14:A5:31:F2:E4	IEEE 802.1
5	<input type="checkbox"/>	6/20/17:13:51.877611	0.155111	6	70	-63	11 00:14:A5:31:F2:E4	01:80:C2:00:00:00	00:14:A5:31:F2:E4 STP Conf.
6	<input type="checkbox"/>	6/20/17:14:06:289948	14.567448	6	76	-62	1 00:14:A5:31:F2:E4	02:C0:1A:04:05:4B	00:14:A5:31:F2:E4 IEEE 802.1
7	<input type="checkbox"/>	6/20/17:14:06:317043	14.594543	6	76	-62	1 00:14:A5:31:F2:E4	Proxim:C0:C1:D0	00:14:A5:31:F2:E4 IEEE 802.1
8	<input type="checkbox"/>	6/20/17:14:06:317939	14.595439	6	76	-62	1 00:14:A5:31:F2:E4	Proxim:C0:C1:D0	00:14:A5:31:F2:E4 IEEE 802.1
9	<input type="checkbox"/>	6/20/17:14:06:476387	14.753887	6	76	-63	1 00:14:A5:31:F2:E4	Fluke:50:56:E4	00:14:A5:31:F2:E4 IEEE 802.1
10	<input type="checkbox"/>	6/20/17:14:06:476698	14.754198	6	10	-61	1	00:14:A5:31:F2:E4	IEEE 802.1
11	<input type="checkbox"/>	6/20/17:14:06:485226	14.762726	6	76	-62	1 00:14:A5:31:F2:E4	Fluke:50:56:E4	00:14:A5:31:F2:E4 IEEE 802.1
12	<input type="checkbox"/>	6/20/17:14:06:485511	14.763011	6	10	-60	1	00:14:A5:31:F2:E4	IEEE 802.1
13	<input type="checkbox"/>	6/20/17:14:06:494463	14.771953	6	76	-61	1 00:14:A5:31:F2:E4	Fluke:50:56:E4	00:14:A5:31:F2:E4 IEEE 802.1
14	<input type="checkbox"/>	6/20/17:14:06:494775	14.772275	6	10	-58	1	00:14:A5:31:F2:E4	IEEE 802.1
15	<input type="checkbox"/>	6/20/17:14:20:865600	29.143100	6	76	-62	1 00:14:A5:31:F2:E4	Intel:1A:13:B2	00:14:A5:31:F2:E4 IEEE 802.1
16	<input type="checkbox"/>	6/20/17:14:20:866560	29.144060	6	76	-62	1 00:14:A5:31:F2:E4	Intel:1A:13:B2	00:14:A5:31:F2:E4 IEEE 802.1
17	<input type="checkbox"/>	6/20/17:14:20:866885	29.144304	6	10	-59	1	00:14:A5:31:F2:E4	IEEE 802.1
18	<input type="checkbox"/>	6/20/17:14:20:915550	29.193050	6	82	-63	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1
19	<input type="checkbox"/>	6/20/17:14:21:018306	29.295806	6	82	-62	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1
20	<input type="checkbox"/>	6/20/17:14:21:120567	29.398068	6	82	-62	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1
21	<input type="checkbox"/>	6/20/17:14:35:940296	44.217795	6	76	-63	1 00:14:A5:31:F2:E4	GemTek:BD:FC:3A	00:14:A5:31:F2:E4 IEEE 802.1
22	<input type="checkbox"/>	6/20/17:14:35:940301	44.217800	6	10	-53	1	00:14:A5:31:F2:E4	IEEE 802.1
23	<input type="checkbox"/>	6/20/17:14:36:075564	44.353064	6	82	-62	1 00:14:A5:31:F2:E4	FF:FF:FF:FF:FF:FF	00:14:A5:31:F2:E4 IEEE 802.1

Figure 3-62: 3rd Party Decodes Engine view

To conduct packet decoding:

- From the Toolbar, click (Stop Live Capture). The Decodes screen gradually comes to a standstill. See [Figure 3-63](#).

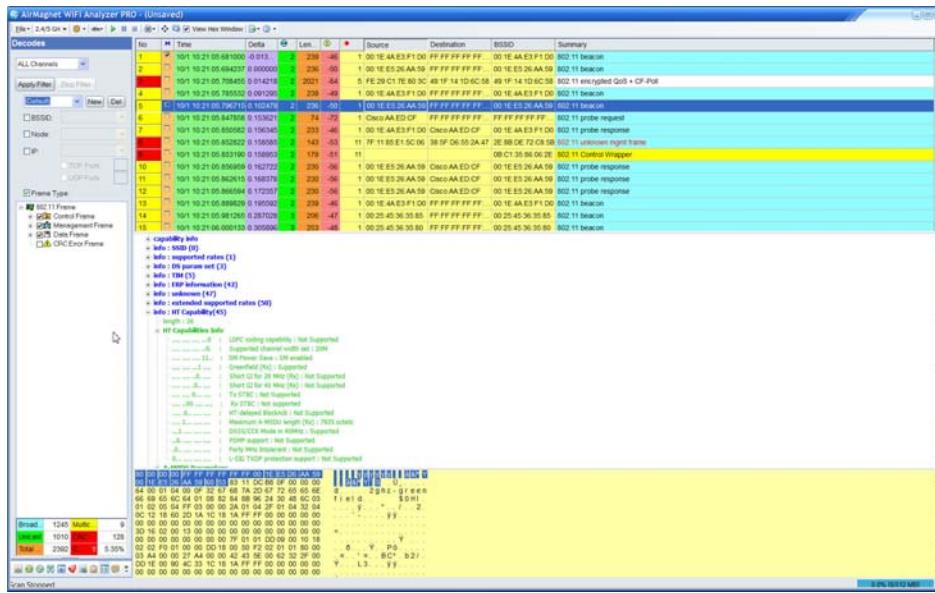


Figure 3-63: Decoding a captured packet

- On the toolbar, check the View Hex Window check box.
- From the screen, select a packet and review all the information about it.
- Start decoding the packet by expanding all entries in the lower part of the screen.

Note: Right-click on the packet tree to select rapid tree expansion and collapse options: Expand Subtrees, Expand All, Collapse All.

- Repeat Steps 3 and 4 to analyze all packets of interest.
- To resume live packet capture, click (Start Live Capture).

The Pause Decodes button applies to AirMagnet WiFi Analyzer PRO only; it does not apply to AirMagnet WiFi Analyzer Express.

Finding Packets on Decodes Screen

When decoding packets, you can quickly locate a particular packet on the screen using (Find in This View) if you know some basic information about the packet you are trying to find.

To find a particular packet:

- 1) From the Decodes screen, click (Stop Live Capture).
- 2) From the menubar, click . The Find dialog box appears. See Figure 3-64.

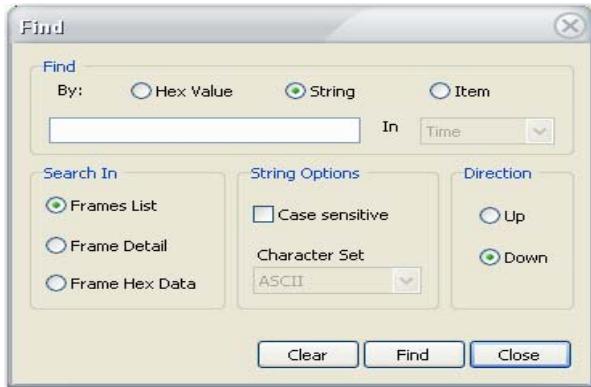


Figure 3-64: Finding a packet

- 3) Make the desired entries and selections and click Find.

Working on Roaming Analysis Screen

Viewing Wireless Roaming

Users can access the Roaming Detail screen by clicking the **Roaming Analysis** button located in the Navigation Bar.

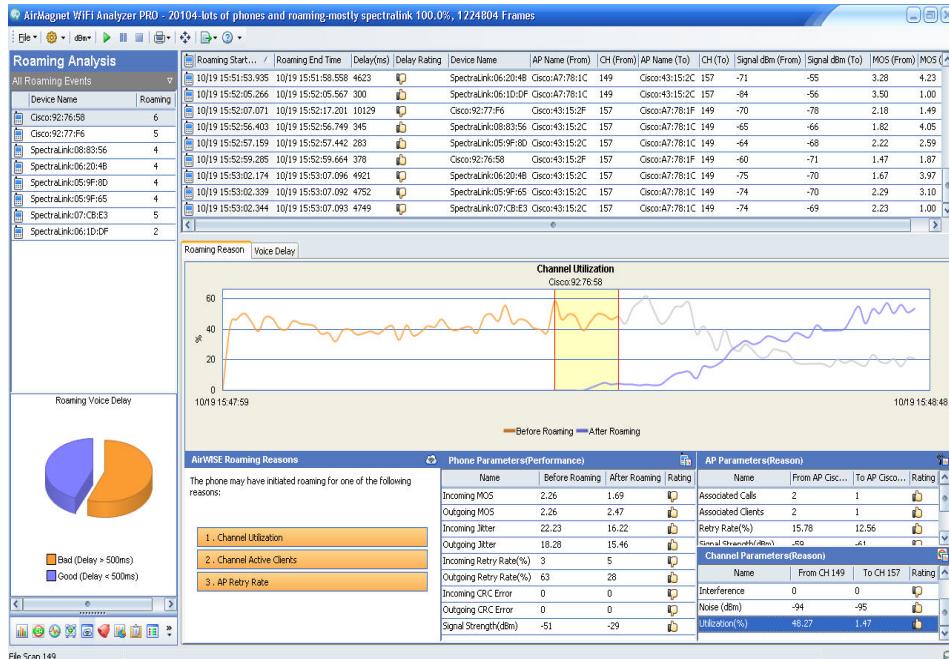


Figure 3-65: Roaming Details

As seen in Figure 3-65, the Roaming Analysis screen is divided into two major panes: the Device Listing (on the left) and the Roaming Details section (on the right). These regions are described in more detail in the following sections.

Device Listing

By default, the Device Listing pane displays all devices that experienced roaming instances while the application was actively scanning. This listing can include standard wireless stations as well as VoFi phones, depending on the devices present in the environment. See Figure 3-66.

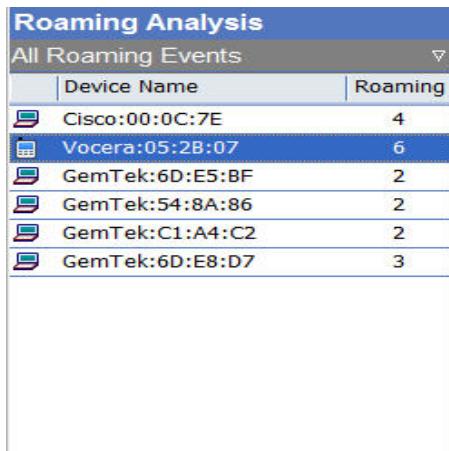


Figure 3-66: Device Listing Pane

As shown above, the information is laid out in a table that provides additional details about each device, as described in Table 3-13.

Table 3-13: Device Listing Data

Column	Description
(Icon)	The first column simply displays an icon that corresponds to the type of device detected.
Device Name / Channel	By default, this column displays the specified name of the device. If no name has been entered, the name is generated using a combination of the device vendor name and the last six digits of its MAC address. Note that when viewing roaming by channel, this column simply indicates the channel number.
Roaming	This field allows the user to quickly assess the number of instances a given device or channel experienced roaming. Larger numbers could indicate that a device is experiencing connection issues and may require additional analysis, as described in “Analyzing Roaming Details” on page 142.

Table 3-13: Device Listing Data

Column	Description
Roaming In/Out	These columns are only present when viewing the Device Listing by AP or Channel. The number provided for Roaming In indicates the total number of times that devices were found to roam to the AP or Channel indicated, whereas the Out column represents the number of times devices roamed away. Channels or APs that have a large number of devices roaming away from them may be indicative of insufficient signal coverage in that area.

The columns present in the table may vary depending on the view option selected in the Roaming Event Filter, described below.

Roaming Event Filter

In order to easily assess the data of interest, users can adjust the information displayed in the Device Listing by using the drop-down filter provided at the top of the pane. See [Figure 3-67](#).



Figure 3-67: Filter Options

Note that since the columns provided vary depending on the selection made, the user can tailor the display to provide exactly the data required:

- **All Roaming Events** – The default option, this selection provides a broad overview of all devices experiencing

roaming and the number of instances detected. This listing can include both standard wireless stations as well as VoFi phones.

- **List by Station**—This option displays only wireless stations, thereby filtering out phones. This can be useful for environments where voice traffic is already considered sufficient for the needs of the users present but data traffic appears to be suffering.
- **List by Phone**—The opposite of List by Station, this filter ignores instances of data roaming and allows the user to focus entirely on VoFi phone roaming.
- **List by AP**—This selection lists all APs that experienced devices roaming either to or away from them as well as the number of instances detected for each. APs that have a large number of roams could be overloaded, indicating that additional infrastructure may be needed in the region.
- **List by Channel**—The final filter allows the user to view the roaming instances divided up into the individual channels detected. As with the List by AP selection, the user can view the number of roams both to and away from each channel; large numbers of roams away from a channel could indicate that there is too much interference present at that particular frequency range.

Roaming Pie Chart

The lower portion of the Device Listing provides a pie chart display of the Voice Delay present in the VoFi roaming instances detected. This value measures the time that passes between the last packet transmitted via the initial AP and the first packet transmitted via the new AP (i.e., the AP to which the phone roamed). Voice Delay is a major indicator of the quality of a VoFi conversation; higher delay can cause lags in the communication between the two phones, and ultimately may result in dropped calls.

Analyzing Roaming Details

The majority of the Roaming Analysis screen is occupied by the Roaming Details pane, which provides detailed data based on the user's selections in the Device Listing. After the user has made a selection from the left-hand pane (by clicking a device or channel of interest), the information in the Roaming Details section refreshes to reflect data specific to the selection made. See Figure 3-68.

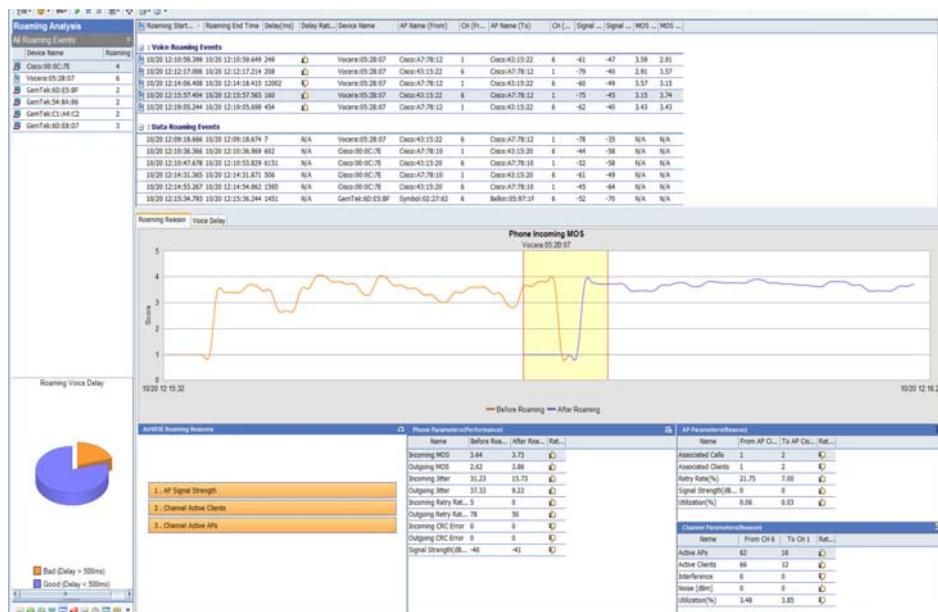


Figure 3-68: Detailed Roaming Data

Due to the amount of information available, the Roaming Details pane is divided up into three major sections: the Roaming Instance Table (across the top), Roaming Reasons (the first tab selected from the bottom), and Voice Delay Information (the second tab). Each of these is described in greater detail in the following sections.

Roaming Instance Table

The top portion of the pane contains a table that displays all instances of roaming detected for the device selected. Depending on the device, these instances could be either Data or Voice Roaming Events. To view roaming data for a specific event, simply click the desired selection in the table and the other portions of the screen will refresh accordingly. See Figure 3-69.

	Roaming Start T...	/	Roaming End Time	Delay(ms)	Delay Rating	Device Name	AP Name (From)	CH (Fro...	AP Name (To)	C...
: Data Roaming Events										
09/09 13:15:08.962	09/09 13:15:13.071	4109	N/A	Cisco:AC:CB:CF	Cisco:A7:78:10	1	Cisco:43:15:20	6		
09/09 13:20:50.839	09/09 13:20:55.029	4190	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1		
09/09 13:34:38.398	09/09 13:34:43.929	5531	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1		
09/09 13:34:52.348	09/09 13:34:55.256	3008	N/A	Cisco:AC:CB:CF	Cisco:A7:78:10	1	Cisco:43:15:20	6		
09/09 13:36:00.391	09/09 13:36:03.713	3322	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1		
09/09 13:45:14.979	09/09 13:45:19.568	4589	N/A	GemTek:5F:AD:97	Cisco:F3:16:32	1	Belkin:05:97:1F	6		
09/09 13:45:18.496	09/09 13:45:20.917	2420	N/A	Sensor:21:29:07	GemTek:31:F2:E4	6	Belkin:05:97:1F	6		
09/09 13:46:44.432	09/09 13:46:46.816	13183	N/A	Cisco:AC:CB:CE	Cisco:43:15:20	6	Cisco:A7:78:10	1		

Figure 3-69: Roaming Table Selection

The columns in the table contain a variety of various data for both VoFi and data roaming instances, as described in Table 3-14.

Table 3-14: Roaming Instance Table Columns

Column	Description
(Icon)	The icons in the first column indicate the type of device associated with each event; data roams are indicated by a computer icon, whereas VoFi roams display a phone.
Roaming Start/End Time	The times at which the device started and finished the roaming process.
Delay (ms)	The delay measured from the time at which the last packet was transmitted to the original AP to the time at which the first packet was transmitted to the new AP.

Table 3-14: Roaming Instance Table Columns

Column	Description
Rating	The icons provided in the Rating column indicate whether the device's wireless service improved as a result of the roam. This is calculated based on the delay value; by default, a delay longer than 500ms indicates a bad roam, as the device took too long to establish a new connection and could have interrupted any calls or data transactions that were processing at the time of the roam. To configure roaming delay threshold, go to File>Configure>General tab. <i>Note: The Rating column only applies to VoFi calls; data roams will simply display "N/A".</i>
Device Name	The name of the roaming device.
AP Name (From/To)	These columns indicate the names of the APs involved in the roam (i.e., both the original AP and the one to which the device roamed).
CH (From/To)	These columns display the original channel (before roaming) and the final one (after roaming).
Signal (From/To)	Signal strengths of from/to APs at the end of roaming.
MOS (From/To)	These fields provide the MOS score for the call both prior to and after roaming. <i>Note: The MOS columns pertain only to VoFi calls and will display "N/A" for data instances.</i>

Determining the Roaming Cause

By default, when the user first navigates to the Roaming Analysis screen, the Roaming Reason tab is displayed. This selection provides a variety of different sub-panes that help the user identify the reason for the selected roam.

Roaming Reasons

Selecting the Roaming Reason tab in the bottom-left portion of the screen allows the user to identify the potential reasons for the selected roaming instance. This changes the Roaming Chart, Delay, and Decodes portions of the screen. See Figure 3-70.

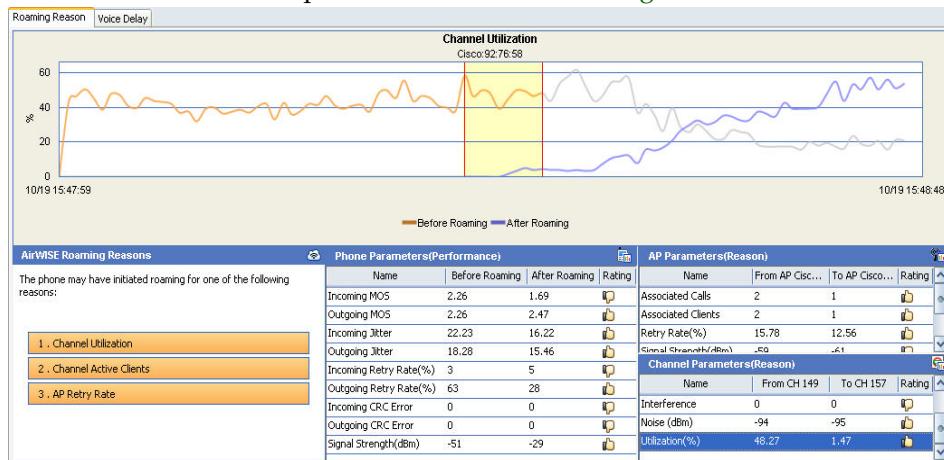


Figure 3-70: Roaming Reason Display

The Roaming Reasons pane in the lower-left lists possible reasons behind the instance of roaming. Clicking these reasons will adjust the chart display to highlight data that can help diagnose the roam.

The type of chart displayed will vary depending on the selection made in the panes across the bottom of the screen. As shown above, when the user clicks one of the links in the Roaming Reasons pane, the chart refreshes accordingly. However, the chart will also update depending on the selection made in the Phone Parameters, AP Parameters, or Channel Parameters panes.

The vertical, shaded band highlights the time period around which roaming occurred, and this region captures representative conditions (see AP/Channel Parameters) at the time of roaming.

When a selection is made in either of the parameter panes, the chart displays an arrow indicating the call performance before and after the roam.

Each of the parameter panes display data in three basic columns:

- **Before Roam**—The data displayed in the first column corresponds to the call experience prior to the roaming instance.
- **After Roam**—The second column displays data as detected after the roam has completed.
- **Rating**—The final column displays a thumbs-up icon if the category (e.g., MOS, Retry Rate, Jitter, etc.) improved after the roam finished; a thumbs-down will appear if the category suffered as a result of the roam.

This data can help the user identify problems with the user experience during the call process. For example, the roam shown in [Figure 3-70](#) experiences improvements in Retry Rate and CRC Errors (as displayed in the Phone Parameters), but Jitter appears to have increased significantly as a result of the roam. This could indicate that the user would consequently experience added difficulty in maintaining a conversation.

Device Parameters

Immediately to the right of the Roaming Reasons pane, the Device Parameters field will vary depending on the type of roaming instance selected; instances of data roaming will simply display the signal level both before and after the roam. For a VoFi roam, these details will be supplemented by retry rates, CRC errors, MOS, and Jitter information. See [Figure 3-71](#).

Name	Before R...	After R...	R...
Incoming MOS	1.38	1.87	
Outgoing MOS	1.73	1.87	
Incoming Jitter	15.06	8.09	
Outgoing Jitter	10.46	7.47	
Incoming Retry...	17	21	
Outgoing Retry...	58	0	
Incoming CRC ...	3	0	
Outgoing CRC ...	0	0	
Signal Strength...	-40	-26	

Figure 3-71: Station/Phone Parameters

AP Parameters

When troubleshooting repeated instances of wireless roaming, it can be helpful to identify just how much traffic the APs in the region are handling. The AP Parameters field provides this information, identifying the number of calls and clients serviced by both APs involved in the instance of roaming selected (e.g., the original and final APs). See [Figure 3-72](#). Note: Values shown are calculated by averaging over time within the vertical, shaded area.

AP Parameters(Reason)		
Name	From AP Cis...	To AP Cis...
Associated Clients	1	0
Retry Rate(%)	12.75	19.75
Signal Strength(dBm)	-40.50	-68.13

Figure 3-72: AP Parameters

As shown above, users can also view the retry rate, signal strength, and utilization before and after the roam. This information can be helpful in identifying whether the roam was justified or not; if the original AP had a low signal level just before the roam, it may be that the station or phone was simply moving away from that region and needed to locate a closer source of wireless connectivity.

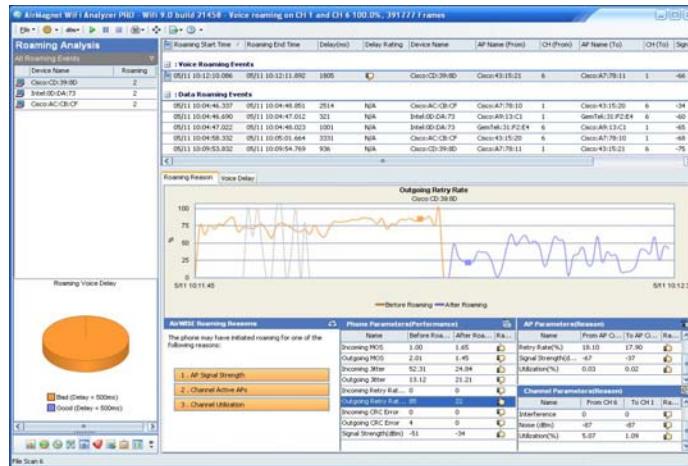


Figure 3-73: Retry rates

The orange square on the graph identifies the condition of the ‘from’ AP approximately one second before roaming is detected to have started. The blue square identifies the condition of the ‘to’ AP after roaming is detected to have completed. This second data point is determined by finding the most stable value in the time period right after roaming has completed.

Channel Parameters

The Channel Parameters field provides a quick overview of the channels involved in the roam, allowing the user to identify whether a crowded or blocked channel is the root cause. See [Figure 3-74](#). Note: Values shown are calculated by averaging over time within the vertical, shaded area.

Channel Parameters(Reason)		
Name	From CH1	To CH6
Active APs	24	69
Active Clients	4	4
Interference	0	0

Figure 3-74: Channel Parameters

By identifying the number of APs and clients present on the selected channel, users can see whether there were simply too many active devices in the environment at the time of the roam. A large number of wireless clients can cause interference, which could result in poor connection quality. In a similar manner, high levels of noise and utilization could result in reduced bandwidth available for the client's connection.

Voice Delay

The Voice Delay tab will only be available if an instance of VoFi roaming is selected, as its information does not apply to standard data roaming.

The Voice Delay tab provides users with an overview of all data pertaining to VoFi roaming, making it perfect for troubleshooting localized instances of excessive roams. The following sections detail each section of information provided on this tab.

Packet Chart

After the desired selection has been made in the Roaming Table, the Packet Chart will update to display a detailed chart of the frames transmitted and received during the conversation both before and after the instance of roaming. See Figure 3-75.



Figure 3-75: Packet Chart

The chart highlights the selected roaming instance in red, with the color-coded packet displays on either side of the gap. Users can check or uncheck options as desired in the color legend in order to view the frames detected during the call.

The Frame Flow Chart display is divided into two sections; frames collected before roaming was initiated are displayed along the upper portion of the chart, whereas the frames gathered after the roam are displayed in the lower portion.

Delay Analysis

The Delay Analysis section displays the duration of the delays detected during roaming, including the time taken to select a new AP, associate, and resume the conversation. See Figure 3-76.

Delay Analysis		
Roaming Gap	Delay(ms)	
Voice Delay	99	627
AP Selection Delay	4	614
802.11 Association Delay	44	615
802.1X Auth Delay	3	629
Key Exchange Delay	82	630
Session Resume Delay	3	632

Figure 3-76: Voice Delay Details

The Voice Delay Analysis (upper) portion of the pane breaks the total delay during the roam into (up to) 5 components, as described below:

- **AP Selection Delay**—The time taken to select an AP that will provide a better call experience.
- **802.11 Association Delay**—The time that elapsed during the association process to the new AP.
- **802.1x Authentication Delay**—The time required for authentication to 802.1x-enabled networks.
- **Key Exchange Delay**—The delay experienced during 802.1x key exchanges.
- **Session Resume Delay**—The time between the successful authentication and the subsequent transmitted voice frame.

Selecting a specific delay option from the Delay Analysis table adjusts the Packet Chart to display frames specific to the selection made.

The lower portion of the window displays advanced details about the delay selected. Users can scroll through this information for specific data regarding how the delay is identified or click **More Info...** for additional details. See [Figure 3-77](#).

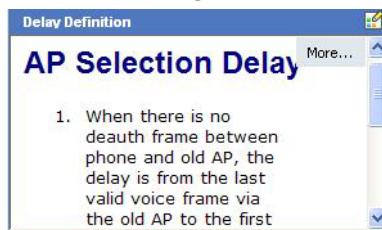


Figure 3-77: Additional Information on Selected Roaming Instance

Packet Decodes

The Decode Table and Tree can be used to help identify the packets transmitted before and after the roaming process. Selecting a specific packet will display its summary in the Decode Tree. See [Figure 3-78](#).

#	From AP	To AP	Time
1	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
2	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
3	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
4	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
5	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
6	802.11 encrypted...	802.11 encrypted...	12:11:16:06:57.988
7	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.008
8	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.008
9		802.11 probe request	12:11:16:06:58.013
10		802.11 probe resp.	12:11:16:06:58.013
11	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.038
12	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
13	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
14	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
15	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.049
16	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
17	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
18	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.048
19	802.11 encrypted...	802.11 encrypted...	12:11:16:06:58.108

Figure 3-78: Roaming Decodes

Table 3-15 describes the columns found in the Decode Table.

Table 3-15: Decode Table Columns

Field	Description
#	The frame's number in the roaming transaction.
AP (From)	The AP from which the phone roamed.
[Arrows]	The arrows detail the direction in which each frame is moving, e.g., the arrow pointing right indicates that the frame was sent from the phone to the destination AP. An arrow pointing left indicates that the frame was transmitted from the destination AP to the phone.
AP (To)	The AP to which the phone roamed.
Time	The time at which the frame was sent.

Multiple Adapters

The multi-adapter function is a capability whereby more than one WiFi adapter can be used concurrently to capture traffic. Each adapter is ‘locked’ on a single channel full-time. This means all traffic is captured for those channels that the adapters are locked on, making it possible for post-capture forensic analysis. Another major benefit is simultaneous multi-channel monitoring.

1] The Roaming Analysis page requires the use of multi-adapter.

2] Packets captured from multiple adapters get saved as a single trace file.

To take advantage of the multi-adapter capability different pages use different display modes to render data (see Table 3-16)

For Adapter-Specific screens, a new menu appears in the toolbar that allows the user to specify the adapter to be used. [Figure 3-79](#). For more information, see Chapter 2, Utilizing Multiple Adapters and Launch.



Figure 3-79: Multi-Adapter Menu

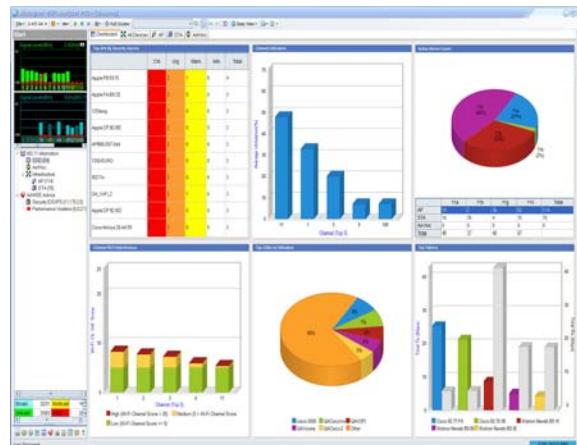
Table 3-16: Multi-Adapter Capability

View	Page
Consolidated Captured data from all adapters is analyzed and presented in a single 'virtual' view.	Start Roaming Analysis
Split Data and analysis for each adapter is presented in its own window within a page.	Channel Decodes

Table 3-16: Multi-Adapter Capability

View	Page
Adapter Specific Data and analysis for an adapter are shown singly. User selects which adapter view to use.	Infrastructure AirWISE Top Traffic Analysis Reports WiFi Tools
Not Available	Interference

Refer to Figure 3-80 to Figure 3-88.

**Figure 3-80: Start Page**

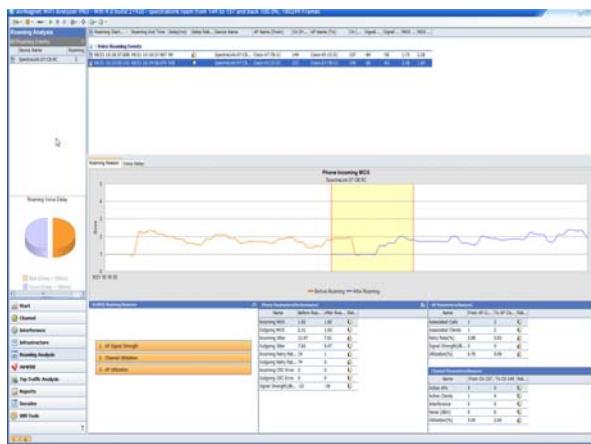


Figure 3-81: Roaming Analysis Page

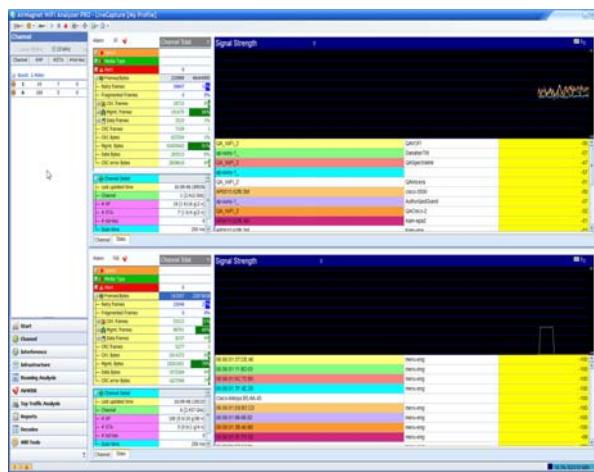


Figure 3-82: Channel Page

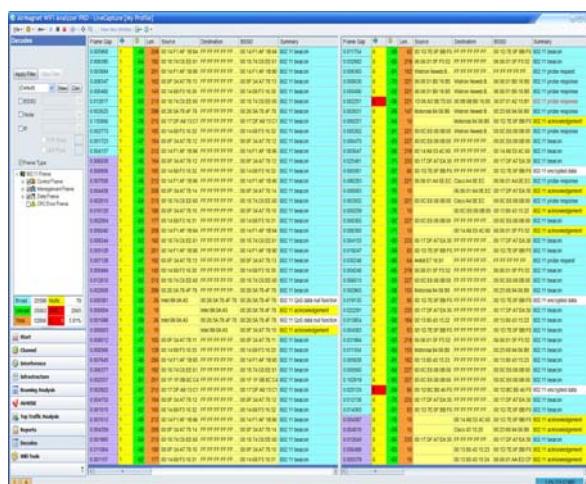


Figure 3-83: Decodes Page

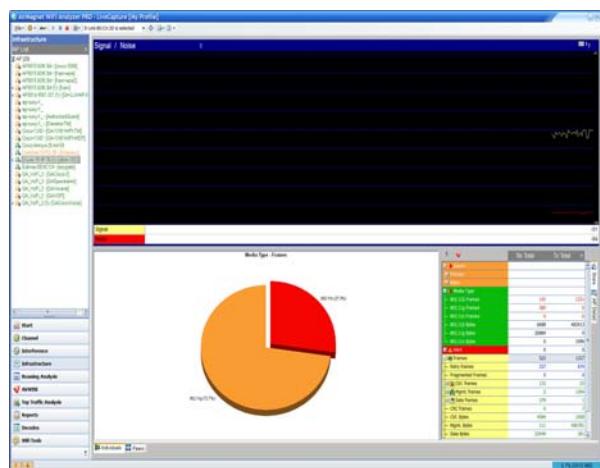


Figure 3-84: Infrastructure Page

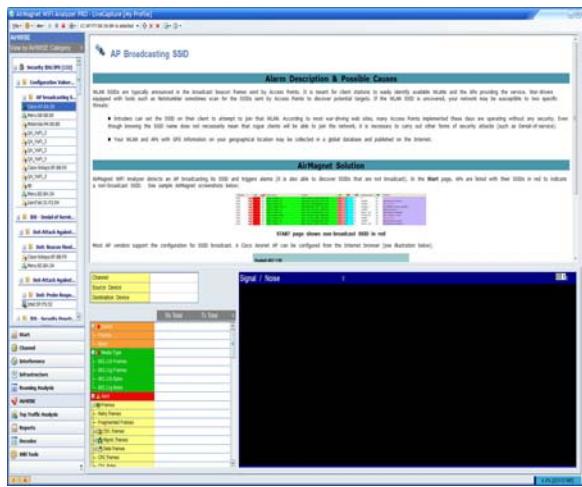


Figure 3-85: AirWISE Page

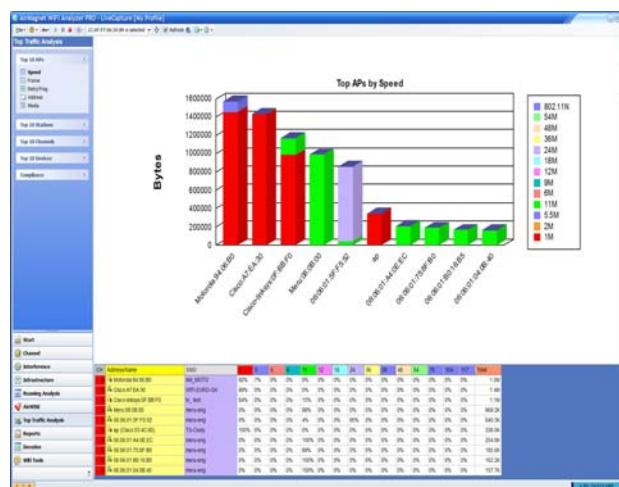


Figure 3-86: Top Traffic Analysis Page

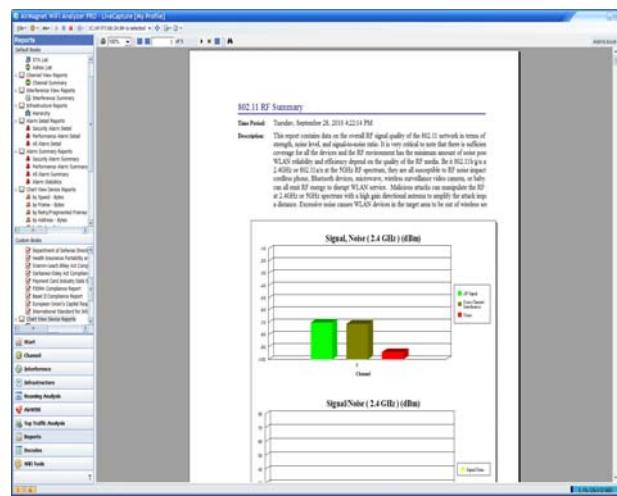


Figure 3-87: Reports Page

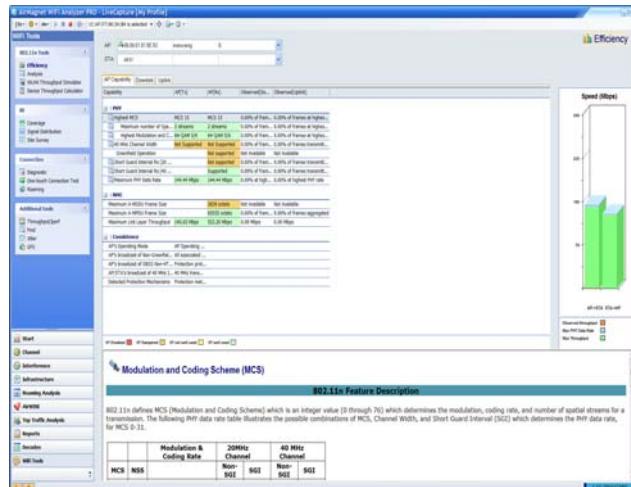


Figure 3-88: WiFi Tools Page

Chapter 4: System Configuration

Chapter Summary

All AirMagnet WiFi Analyzer system configuration settings such as capture filters, policies, channel scan list, export file names, address books, access control list, etc., are saved in a default profile named My Profile. This can facilitate the recall of the configuration settings for each site survey. You can save the configuration settings for any given location or site for wireless LAN administration. You can also export configuration settings as templates that can be imported for use in other surveys later on.

If your wireless LAN administration responsibility covers more than one site, or if you are servicing more than one customer, you will find the AirMagnet configuration profile utility very helpful for managing various configuration settings.

This chapter covers the following topics:

- Creating a system profile
- Configuring general system settings
- Configuring 802.11 settings
- Configuring filter settings
- Customizing channel scan settings
- Managing WLAN policies
- Creating an address book.
- Setting up an access control list (ACL)
- Specifying site information
- Generating AP groups
- Applying custom and pre-defined skins

Configuring a System Profile

This section discusses how to create an AirMagnet WiFi Analyzer system profile. Once a profile is established, it will be used as a boilerplate under which all system parameters will be organized, making it easy to archive, retrieve or share these data.

Note: Once configured, the name of the profile will appear in the title bars of all the configuration screens under the **Configure . . .** command. See the screen captures in this chapter.

Creating a New Profile

To create a new AirMagnet profile:

- 1) Click (Configure). The AirMagnet Config screen appears. See Figure 4-1.

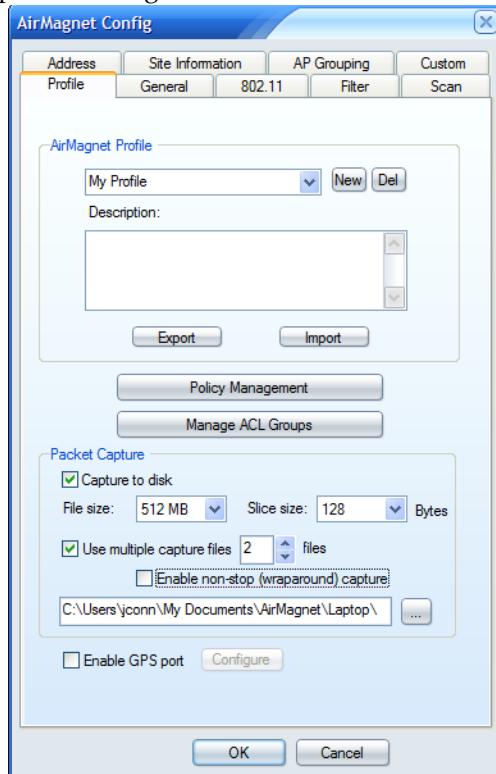


Figure 4-1: Configuring a system profile

- 2) Select New, and overwrite [NewProfile] with a unique a name.
- 3) Click in the Description field, and enter a description for the profile.
- 4) If applicable, click Import and find and import an existing profile.

Use the Import option only if you have a profile saved on your PC or network.

- 5) Click Policy Management to set the policy of the profile. See “Managing Network Policy Profiles” on page 221 for information on how to manage network policies.
- 6) Click Manage ACL Groups to configure the ACL groups of the profile. See “Assigning Policies to ACL Groups” on page 235 for information on how to configure ACL groups.
- 7) Optionally, check Enable GPS port if you want to use this feature. The GPS Configuration screen appears. See Figure 4-2.

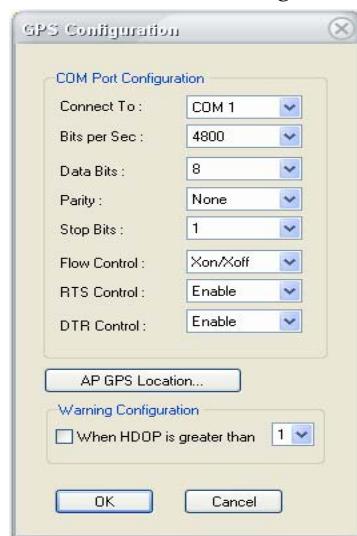


Figure 4-2: Configuring GPS settings

- 8) Specify the parameters you want to use, and click OK.
- 9) Then click OK to finish setting up the profile.

Optionally, you can export the profile for record-keeping or to share it with others using the Export button.

Exporting a System Profile

You can also export a profile so that you can save it for later use.

To export a profile:

- 1) From the AirMagnet Config>Profile screen (Figure 4-1), click Export. The Save As screen appears. See Figure 4-3.

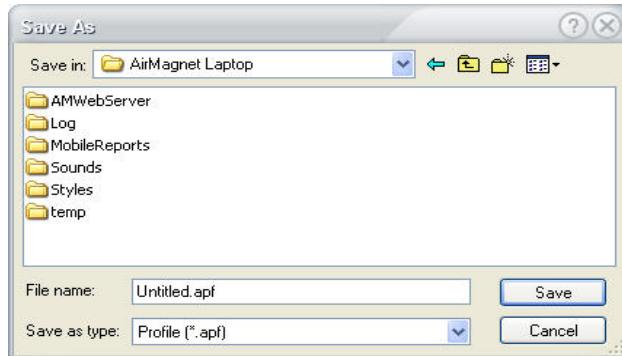


Figure 4-3: Exporting a profile

- 2) Specify a name for the profile to export.
- 3) Select a folder where the profile is to be saved.
- 4) Select a file type (i.e.,.apf).
- 5) Click Save.

AirMagnet WiFi Analyzer profile files use the .apf file extension.

If you have saved a system profile, you may use it as a template for a new site survey by importing the profile.

Importing a System Profile

If you have an AirMagnet profile (.apf) file saved on your system or network, you may import it using the Import button.

To import a profile:

- 1) From the AirMagnet Config>Profile screen (Figure 4-1), click Import. The Open screen appears. See Figure 4-4.

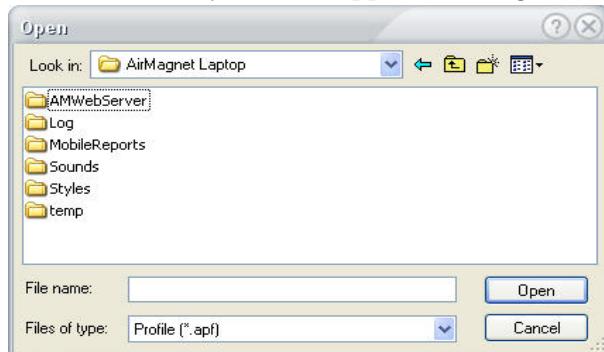


Figure 4-4: Importing a profile

- 2) Select the folder in which the profile file is stored.
- 3) Select a file type, i.e., .apf in this case.
- 4) Locate and select the file in the file list.
- 5) Click Open.

Packet Capture

As shown in Figure 4-5, you may choose to capture packet data to disk by three methods: Capture to disk, Use multiple capture files and Enable non-stop capture.

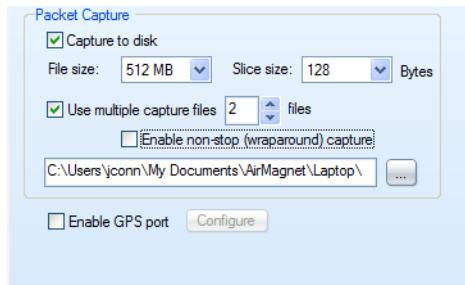


Figure 4-5: Packet capture portion of Profile tab

Capture to disk: Check this option to capture and save packet data to a maximum file size based on the selection from the **File size** dropdown. You may also choose a Byte Slice size from the **Slice size** dropdown. Capturing is stopped once the buffer size is reached.

When the specified buffer size is reached, a dialog is displayed that provides a browse option to save the file to disk.

Use multiple capture files: By also checking this option, you may choose to set the number of multiple consecutive files that will be captured of the file size specified in "Capture to disk." Each file will receive an end-of-capture time stamp file name (e.g. July 12, 2011-1410.amm). The file will be saved to the location set in the browse box. As you can see in Figure 4-5, the default save location is "airmagnet/laptop."

Enable non-stop (wraparound) capture: By also checking this option, a continuous capture mode is enabled. This means that when the set number of "multiple capture files" is reached, the oldest file will be automatically deleted in order to save a new file. Using this method, packet data will be continuously captured while the total number of files is limited to the number set in "Use multiple capture files."

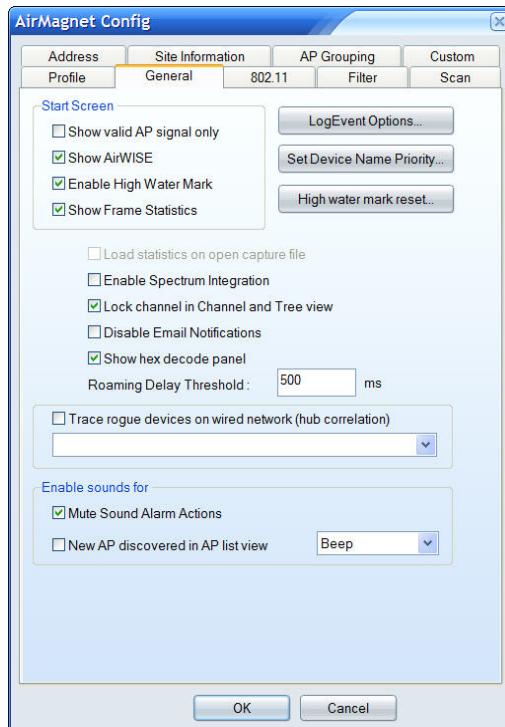
Continuous capture will continue until this check box is unchecked.

Configuring General System Settings

The General settings configuration provides various options for screen display and packet capture.

To change the General configuration settings:

- 1) From the AirMagnet Config screen, select the General tab. The AirMagnet Config>General screen appears. See [Figure 4-6](#).

**Figure 4-6: Configuring general settings**

- 2) Make the desired selections as described in Table 4-1.

Table 4-1: Configuring General Settings

Parameters	Description
Show valid AP signal only	If checked, the system will not display brown bars representing Cross Channel Interference in the signal graph. (Start screen)

Table 4-1: Configuring General Settings

Parameters	Description
Show AirWISE	If selected, AirWISE will appear in the lower-left part of the Start screen.
Show Frame Statistics	If selected, the Start page will display a small box containing frame summary information below the pie chart. (Start Screen)
Enable High Water Mark	If checked, the graphs in the top left corner of the start screen will store a high point during a user-specified interval. This allows you to see the highest point your network traffic has reached within a given time. To specify this time, click the Start screen high water mark reset button.
Load statistics on open capture file	If checked, a loaded capture file will display all the information that was captured during the saved session. A normal playback will only display devices detected until the capture buffer has been filled; this option allows you to view devices that were logged previously but then overwritten as the buffer became full.
Enable Spectrum Analyzer	If checked, AirMagnet Spectrum Analyzer integration will be enabled. See “ AirMagnet Spectrum Analyzer Integration ” on page 100 for more information.
Lock channel in Channel and Tree view	If checked, the system will stop scanning other channels when you are viewing a selected channel in detail on the Channel screen.
Disable Email Notification	If selected, no email notification will be sent.
Show hex decode panel	If selected, the hexadecimal panel will be displayed on the Decodes screen.

Table 4-1: Configuring General Settings

Parameters	Description
Roaming Delay Threshold	Used to calculate the delay threshold which is calculated based on the delay value; by default, a delay longer than 500ms indicates a bad roam, as the device took too long to establish a new connection and could have interrupted any calls or data transactions that were processing at the time of the roam.
Trace rogue devices on wired network	If checked, the system will trace rogue devices on the wired side of the network. Note that your laptop must be connected via an ethernet connection to use this option. When tracing is active, AirMagnet WiFi Analyzer will attempt to trace all rogue devices that are connected to the same hub as the WiFi machine.
Enable sound for	<ul style="list-style-type: none"> • Mute Sound Alarm Actions If checked, the system will not beep when a new alarm is generated. • New AP discovered in AP list view If checked, the system will beep when a new AP is detected. Click the down arrow to select a sound option.

- 3) Click OK when completed.

Customizing Event Log Options

This option allows you to specify exactly which actions recorded/ performed by AirMagnet WiFi Analyzer will be recorded to the Windows event log. While having all of these options enabled allows you to have a solid historical record of the data you've received, it can also consume disk space rapidly.

To access event log options:

- 1) From the AirMagnet Config screen, select the General tab.
- 2) Click the LogEvent Options... button. See [Figure 4-7](#).

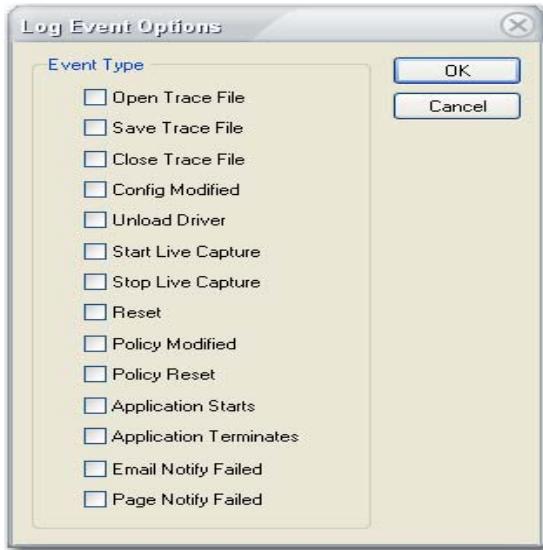


Figure 4-7: Log Event Options

- 3) Select the options you wish to record, and click OK.

Integration with Windows Wireless Configuration

This feature allows AirMagnet WiFi Analyzer PRO users to take advantage of the Windows wireless profiles they have created in Windows and use them directly with AirMagnet WiFi Analyzer PRO's active tools (e.g. Site Survey, Performance, Connect, Roaming, etc.). This feature applies to Microsoft Windows XP, Windows Vista and Windows 7 operating systems. The configuration and modification of the wireless profiles must be and can only be done inside Windows operating systems.

Creating Wireless Configuration on Windows XP

If you want to use AirMagnet WiFi Analyzer's auto configuration feature on a laptop PC running on Microsoft Windows XP operating system with an 802.11n wireless network card, you must do the following: 1) Download and install the Microsoft Core XML Services (MSXML 6.0) from <http://www.microsoft.com/downloads/>

details.aspx?FamilyId=993c0bcf-3bcf-4009-be2127e85e1857b1\$displaylang=en. 2) Download and install the Microsoft Wireless LAN API (KB918997) from [http://www.microsoft.com/doanloads/details.aspx?familyId=52A43BAB-DC4E-413F-AC71-158EFD1ADA50\\$displaylang=en](http://www.microsoft.com/doanloads/details.aspx?familyId=52A43BAB-DC4E-413F-AC71-158EFD1ADA50$displaylang=en). (The API is not needed if you are running AirMagnet WiFi Analyzer on Windows XP operating system with service Pack 3.)

Integration of AirMagnet WiFi Analyzer with Windows Wireless Configuration on Windows XP operating system requires an 802.11n wireless network adapter and the Microsoft Core XML Services (MSXML 6.0) and Microsoft Wireless LAN API (KB918997) installed on the system on which AirMagnet WiFi Analyzer is used.

Any addition, modification, and/or deletion of wireless network names (SSIDs) used for integration with Windows XP must and can only be done in Windows XP.

When configuring network names (SSIDs) in Windows, make sure that AirMagnet WiFi Analyzer is closed (stopped).

To create a wireless configuration on Windows XP:

- 1) Make sure that AirMagnet WiFi Analyzer is closed.
- 2) Make sure that an 802.11n wireless network adapter is inserted in the laptop's card slot.
- 3) From your desktop, click Start>Control Panel >Network Connections.
- 4) Right-click an 802.11n wireless network and select Properties from the drop-down menu.
- 5) From the Wireless Networks Connection Properties dialog box, click Wireless Networks.
- 6) Click Add. . . . The Wireless network properties dialog box appears. See [Figure 4-8](#).

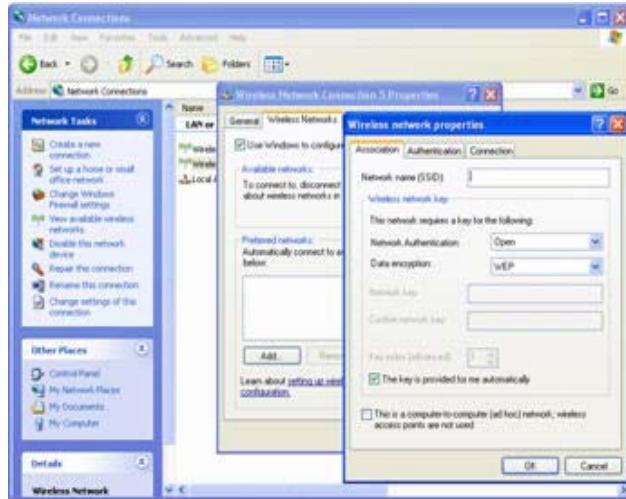


Figure 4-8: Configuring nework settings on Windows XP

- 7) Make the required entries and/or selections and click Ok. See Figure 4-9.



Figure 4-9: A New Network Connection on XP

- 8) Repeat Step 6 through 7 to add all wireless network connections as applicable.
- 9) When all wireless connections are added, make sure that Use Windows to configure my wireless network settings is checked and click Ok.
- 10) Close the Network Connections dialog box.
- 11) Launch AirMagnet WiFi Analyzer.
- 12) Select File>Configure>802. 11. See [Figure 4-10](#).



Figure 4-10: XP network name (SSID) shown

All wireless network connections (SSIDs) you have added on Windows XP are available in AirMagnet Config dialog box under the 802.11 tab. You can choose to use any of them by clicking the down arrow and selecting the one of your choice. See [Figure 4-11](#).



Figure 4-11: Selecting a Windows wireless connection

- 13)** Select the wireless network of your choice and click Ok.

Once a Windows wireless network connection (SSID) is selected, the security attributes (i.e., authentication, encryption, etc.) are shown in the dialog box. If you want to change any of these attributes, you must do it in the Wireless Network Connections Properties dialog box on Windows. See the section below.

Modifying Network Security Attributes on XP

- 1)** Make sure that AirMagnet WiFi Analyzer is closed.
- 2)** From your desktop, click Start>Control Panel >Network Connections.
- 3)** Right-click the 802.11n wireless network and select Properties from the drop-down menu.
- 4)** From the Wireless Networks Connection Properties dialog box, click Wireless Networks.

- 5) Highlight the wireless network of interest and click Properties. The dialog box showing the properties of the wireless network appears.
- 6) Make the desired changes and click OK.
- 7) Click OK to close the Wireless Network Connection Properties dialog box.

If you want to remove a wireless network connection (SSID), simply highlight it in the Wireless Network Connection Properties dialog box and click Remove. Then click OK on the Wireless Network Connection Properties dialog box to implement the change.

Creating Wireless Configuration on Windows Vista

This feature applies to all wireless network adapters based on the Atheros chipset.

To use wireless configuration on Windows Vista operating system:

- 1) Make sure a wireless network adapter is inserted in the card slot of the laptop PC.
- 2) From your desktop, click Start>Control Panel >Network and Sharing Center. The Manage Wireless Networks dialog box appears. See Figure 4-12.

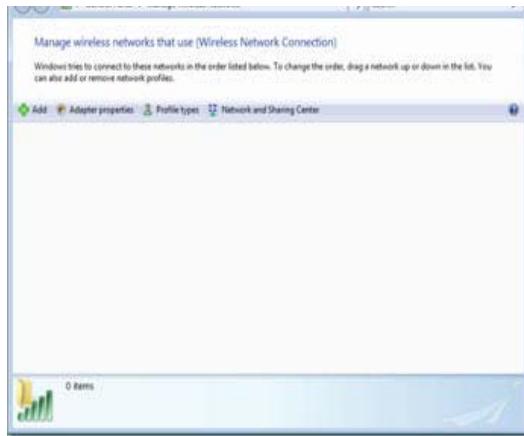


Figure 4-12: Adding wireless connection on Windows Vista

- 3) Click Add. The 'Manually Create a Wireless Network' Dialog Box appears. See Figure 4-13.



Figure 4-13: Manually create a network profile

- 4) Click Manually create a network profile. The 'Manually connect to a wireless network' dialog box refreshes. See Figure 4-14.

You can also Add a network that is in range of this computer.



Figure 4-14: Creating a network profile

- 5) Make the required entries and/or selections and click Next.
- 6) Repeat Steps 2 through 5 to create as many wireless network profiles as applicable.

All wireless network profiles you have create appear in the Manage Wireless Networks dialog box and can also show up in the AirMagnet Config dialog box under the 802.11 tab, as described below.

- 7) From AirMagnet WiFi Analyzer, click File>Configure...>802.11. See Figure 4-15.



Figure 4-15: Selecting a Windows network profile

- 8) Click the down arrow, select a wireless network form the drop-down list menu, and click OK.

Creating Network Connections in AirMagnet WiFi Analyzer:

Unlike the integration with the Windows XP operating system, the integration with the Windows Vista operating system allows users to create network connections directly from inside AirMagnet WiFi Analyzer.

To create network connection from AirMagnet WiFi Analyzer:

- 1) From AirMagnet WiFi Analyzer, select File>Configure>802. 11.
- 2) Click New. The Create Wireless Network dialog box appears. See [Figure 4-16](#).



Figure 4-16: Creating network connection in AirMagnet WiFi Analyzer

- 3) Enter a name for the wireless network and click OK.

Once you have clicked OK, the manage Wireless Network dialog box in Windows Vista appears showing the new network conenction you have just named on top of the list of available network connections. See Figure 4-17.

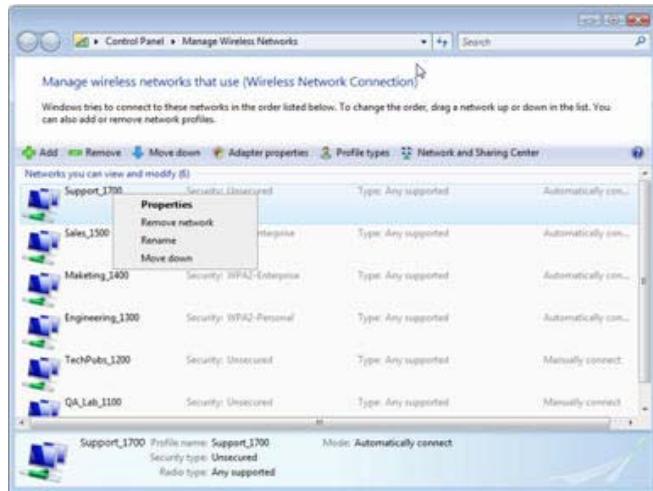


Figure 4-17: Configuring network connection in Windows Vista

- 4) Right-click the new connection you have created and click **Properties** from the pop-up menu.

A dialog box with the name of the connection on its title bar appears. Since the connection has not been configured yet, it does not have any security attributes. Therefore, you need to add the desired security attributes to it. See Figure 4-18.

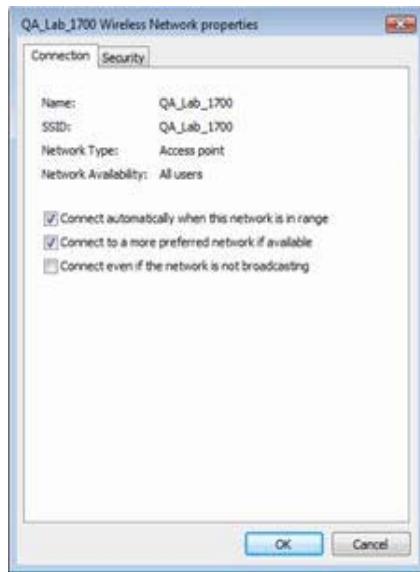


Figure 4-18: Configuring network connection in Windows Vista

- 5) Click the Security tab, make the required selections and/or entries, and click OK.

Now the new network connection is configured and can be used the same way as you do with the connections you create in Windows Vista.

Modifying Network Security Attributes in Windows Vista

Just as you can initiate the creation of network connections directly from inside AirMagnet WiFi Analyzer, you can start making changes to an existing network connection from inside AirMagnet WiFi Analyzer as well.

To modify a network connection from AirMagnet WiFi Analyzer

- 1) From the AirMagnet Config dialog box, select the 802.11 tab, select a network connection of interest, and click Edit.... The Wireless Network Properties dialog box appears. See Figure 4-19.

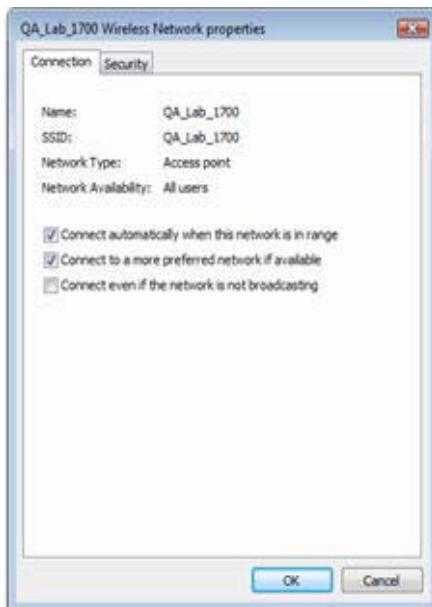


Figure 4-19: Editing Network Security Attributes

- 2) Click the Security tab. See [Figure 4-20](#).

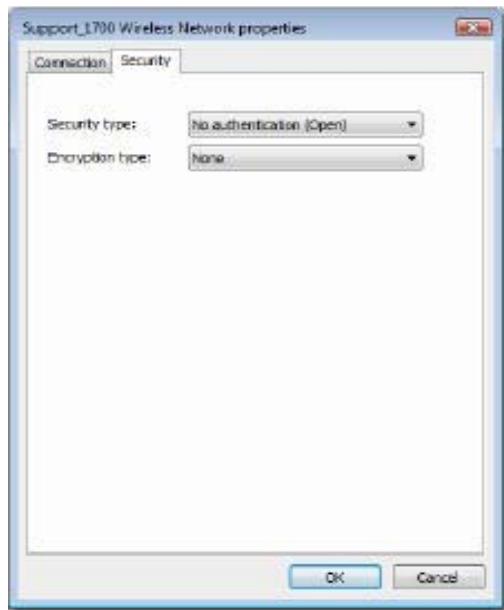


Figure 4-20: Editing network security attributes

- 3) Make the desired changes and click OK.

If you want to remove a network connection created on Windows Vista operating system, simply highlight the connection from the Manage Wireless Networks dialog box and click Remove.

Configuring 802.11 Settings

The 802.11 configuration screen allows you to set the parameters to allow AirMagnet to function as an active 802.11 node on the network. It is important that you set up these parameters properly before using any of the active tools.

Important For each SSID entered (or selected from the list), there is a whole set of 802.11 parameters associated with it, including Authentication and Advanced configurations.

To configure 802.11 settings:

From the AirMagnet Config screen, select the 802.11 tab. The AirMagnet Config>802.11 screen appears. See [Figure 4-21](#).

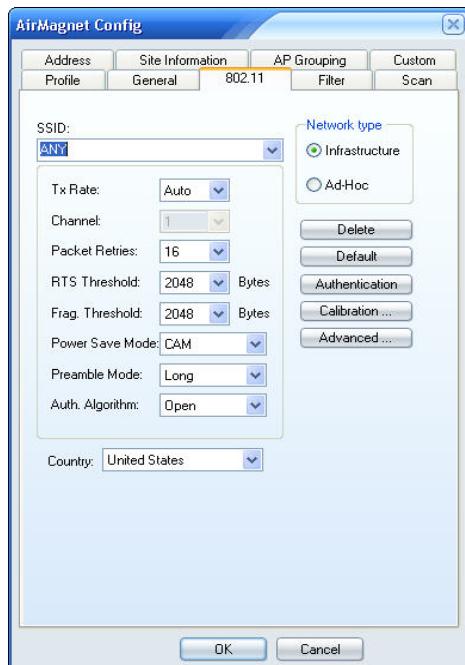


Figure 4-21: Configuring 802.11 parameters

Figure 4-21 applies if you do not have Windows Wireless Configuration (profiles) created ahead of time either on Windows XP or Vista. If you already have Window Wireless Configuration done on your PC, the screen will look different from this in either situation. Refer to “Creating Wireless Configuration on Windows XP” on page 30 and “Creating Wireless Configuration on Windows Vista and Windows 7” on page 35.

- 4) Make any of the following selections as described in Table 4-2.

Table 4-2: Configuring 802.11 Settings

Parameters	Description
SSID	Choose ANY or a specific SSID to associate. When AirMagnet active tools such as Ping or DHCP try to associate within a given SSID or with a given AP, all the configured parameters in this dialog box will be applied to the WLAN card.
Network type – Infrastructure	The infrastructure mode bridges a WLAN with a wired Ethernet LAN.
Network Type – Ad-Hoc	The Ad-Hoc mode is a method for wireless devices to directly communicate with each other, all wireless devices within range of each other being able to discover and communicate in a peer-to-peer fashion without involving access points.
Tx Rate	Select a transmission speed at which your AirMagnet is to be operated. Keep in mind that the higher the speed, the more bandwidth you will consume. The default setting is Auto, which allows the system to select whatever speed that is appropriate.
Channel	Specify a channel when Ad-Hoc mode is selected. See Network type above.



Table 4-2: Configuring 802.11 Settings

Parameters	Description
Packet Retries	Specify the maximum number of transmission retries at the 802.11 protocol level.
RTS Threshold	Specify the threshold of packet length to trigger the use of the 802.11 RTS/CTS mechanism.
Frag. Threshold	Specify an 802.11 frame fragmentation threshold.
Power Save Mode	Choose Active (CAM) or Power Save mode. The former keeps the system active all the time whereas the latter switches the system to a energy-saving mode when it is left idle for some time.
Preamble Mode	Select Long or Short (for 802.11 preamble).
Auth. Algorithm	Select Open or Shared Key authentication.
Country	Select the country where AirMagnet is used.
Delete	Click this button to delete the selected SSID.
Default	Click this button to restore the 802.11 configuration to the settings configured by the manufacturer.
Authentication...	<p>Opens the authentication dialog box, where you can choose (to configure) any of the following authentication settings:</p> <ul style="list-style-type: none"> • WEP • LEAP • EAP-Fast • Host-Based EAP • Pre-Shared Key
Advanced...	Allows you to configure advanced driver settings.

Table 4-2: Configuring 802.11 Settings

Parameters	Description
Calibration...	Allows you to adjust RF signal strength (of a selected wireless LAN card) in 5 dBm increments as well as the noise floor.

- 5) Click OK when completed.

If you have Windows (XP and Vista only) Wireless Configurations created on the laptop PC, then you will see a different 802.11 dialog box than the one shown in Figure 4-21. In that case, the procedures used for configuring 802.11 will be different than those discussed here. See “Creating Wireless Configuration on Windows XP” on page 30 and “Creating Wireless Configuration on Windows Vista and Windows 7” on page 35.

Configuring Authentication Mechanisms

Security is a big concern for wireless LAN administrators. AirMagnet supports the latest wireless network security technologies to ensure your network security. Currently, AirMagnet supports the following authentication mechanisms:

- WEP
- LEAP
- EAP-FAST
- Host-Based EAP
- WPA Pre-Shared Key
- WPA2

By default, your AirMagnet WiFi Analyzer comes without any authentication mechanism pre-configured. You can select and configure any of the four security mechanisms based on the needs of your wireless network.

Each option is described in its section below.

Before attempting to use any authentication mechanisms within AirMagnet WiFi Analyzer, make sure that the computer is able to associate to the AP without AirMagnet WiFi Analyzer loaded. If it cannot, the mechanisms may be misconfigured within Windows or the wireless client utility, thus leaving AirMagnet WiFi Analyzer unable to associate as well.

Some of the following authentication types are only supported by specific cards, and may have additional restrictions. For additional information regarding authentications supported by specific cards, refer to AirMagnet's Knowledge Base: http://www.airmagnet.com/faq/index.php?page=index_v2&id=48&c=8.

WEP

Wired Equivalent Privacy (WEP) protocol is an IEEE 802.11 security protocol that provides WLAN with a minimum level of security and privacy comparable to that of a typical wired LAN. If this option is selected, users will be required to enter a WEP key to use active tools.

LEAP

Also known as Cisco-Wireless EAP, LEAP (Lightweight Extensible Authentication Protocol), provides username/password-based authentication between a wireless client and a RADIUS server like Cisco ACS or Interlink AAA. It is one of several protocols used with the IEEE 802.1X standard for LAN port access control. Users must enter a user name and password for AirMagnet WiFi Analyzer to use to authenticate to the RADIUS server in order to use active tools. Check the WiFi Protected Access (WPA) box if your network uses WPA encryption.

Host-Based EAP

Similar to LEAP authentication, Host-Based EAP (Extended Authenticating Protocol) differs in that the user name and password must be configured in the computer's settings, rather than those within AirMagnet WiFi Analyzer. In other words, Windows must authenticate with the RADIUS server in order to use active tools. Note that this configuration must take place outside of AirMagnet WiFi Analyzer.

WPA Pre-Shared Key

The WiFi Protect Access Pre-Shared Key mechanism requires the user to configure Windows' network settings (or those of the client utility) to match the encryption protocols specified by the enterprise network. Note that this configuration must take place outside of AirMagnet WiFi Analyzer.

Configuring WEP settings

To configure WEP settings:

- 1) From the AirMagnet config>802.11 screen, click Authentication. . . . The Wireless Authentication screen appears. See [Figure 4-22](#).



Figure 4-22: Selecting an authentication mechanism

Only the authentications that are supported by your wireless card will show in the Wireless Authentication dialog box.

- 2) Click the down arrow and select WEP from the drop-down list. The Wireless Authentication>WEP screen appears. See Figure 4-23.



Figure 4-23: Configuring WEP

- 3) Make the desired selections and click Apply.

Configuring LEAP

To configure LEAP settings:

- 1) From the AirMagnet Config>802.11>Wireless Authentication screen, click the down arrow and select LEAP. See Figure 4-24.



Figure 4-24: Configuring LEAP

- 2) Check the WiFi Protected Access (WPA), if applicable.

- 3) Make the desired entries and click Apply.

You can configure EAP-FAST, Host-Based EAP, and Pre-shared Key in the same way. For more information on WPA configuration and support, visit <http://www.airmagnet.com/faq/index.php>.

Configuring Advanced Driver Settings

The Advanced... button on the 802.11 screen allows you to tailor the power of your wireless LAN card driver according to your wireless LAN needs.

To configure advanced driver settings:

- 1) From the AirMagnet Config>802.11 screen, click Advanced. . . .
The Advanced Driver Settings screen appears. See Figure 4-25.

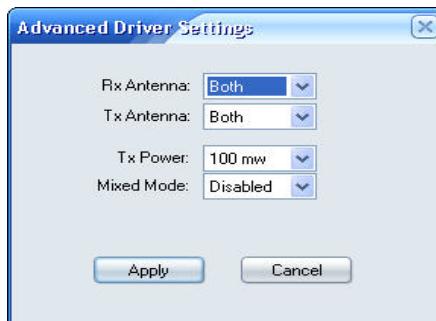


Figure 4-25: Configuring driver settings

- 2) Make the desired selections as described in Table 4-3.

Table 4-3: Parameters for Advanced Driver Settings

Parameter	Description
Rx Antenna	Receiving antenna. Select Left, Right, or Both.
Tx Antenna	Transmission antenna. Select Left, Right, or Both.
Tx Power	Transmission power. Click the down arrow and select one from the list.

Table 4-3: Parameters for Advanced Driver Settings

Parameter	Description
Mixed Mode	Choose Enabled or Disabled.

- 3) Click Apply when completed.

Wireless LAN Card RF Calibration

Numerous 802.11 wireless network adapters are available on the market. Since they are designed and manufactured by different vendors, their performance will differ from manufacturer to manufacturer. Such being the case, problems may arise as to the accuracy and/or consistency in radio signal strength among the wireless network adapters that are being used, which in turn often cast shadow upon the reliability of WiFi data collected through them. AirMagnet WiFi Analyzer solves this issue.

As the leader in WiFi network analysis and troubleshooting, AirMagnet has completed an exhaustive calibration and testing program for most of our “preferred” list of WiFi adapters as listed on the AirMagnet website (http://www.airmagnet.com/support/supported_adapters/). The program covers multiple card manufacturers and involves extensive testing across all WiFi channels, different operating systems, and different power/attenuation levels. To our knowledge, this represents the most extensive testing of its kind in the industry and ensures the accuracy of your AirMagnet measurements, while continuing to provide the flexibility and cost advantages of using off-the-shelf wireless adapters. AirMagnet has updated its products to account for these findings to ensure the highest levels of accuracy for our products and to provide our customers with the most accurate and reliable measurements on the market.

RF Calibration in AirMagnet WiFi Analyzer

AirMagnet WiFi Analyzer comes with a RF Calibration dialog box to make wireless network adapter calibration fast and easy. You can bring up the dialog box (see the figure below) by clicking:

- **File>Configure...>802.11>Calibration...** or

- **Configure>802.11>Calibration....**

How to Use RF Calibration Options in AirMagnet WiFi Analyzer

Once you have brought up the RF Calibration dialog box, you should click the down arrow in the upper-left corner and select one of the following options (Figure 4-26):

- **No Calibration**
- **Pre-Defined Calibration** (This is the second entry, i.e., **Air-Magnet 802.11 a/b/g/n Wireless PC card**.)
- **Custom Calibration**

The following paragraphs describe each of the options and the ways to use them.

No Calibration

“No Calibration” means no adjustment offsets are applied by AirMagnet to the wireless network adapter. This option should be used when the user prefers to utilize the adapter manufacturer’s raw RF signal strength readings.

To use a wireless network adapter’s default settings without calibration:

- 1) From the upper-left corner of the RF Calibration dialog box, click the down arrow and select **No Calibration** from the list menu. See Figure 4-26.

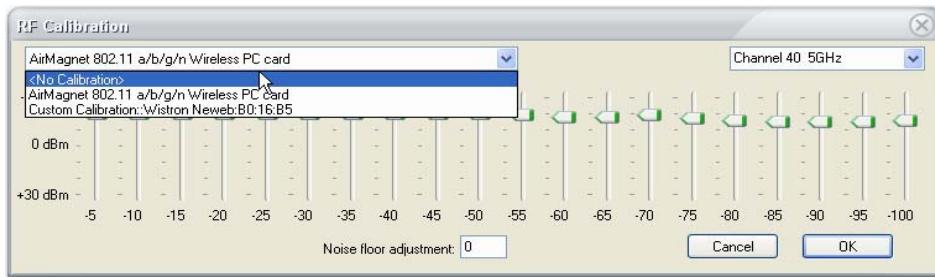


Figure 4-26: Using a wireless network adapter without calibration

When “No Calibration” is selected, all other controls in the RF Calibration dialog box will be grayed out (unavailable). This is because the user do not need to do anything when using this option.

- 2) Click the OK button to implement the selection.

Pre-Defined Calibration

If the wireless network adapter you are using happens to be on the pre-calibrated list, then the AirMagnet application automatically recognizes the adapter and displays the pre-defined calibration option. In other words, if your wireless network adapter is displayed as a “Pre-Defined Calibration” entry in the list menu, it means that you have the option to select and utilize the AirMagnet calibrated values. In this case, you do not have to do anything other than select this entry. You still have the option to make changes to the settings of a pre-calibrated wireless network adapter. In this case, you are customizing a pre-calibrated wireless network adapter, which will also be discussed below.

All tests for defining the calibrated values for the wireless adapter were performed using calibrated spectrum analyzers in a professionally shielded isolation chamber to ensure the best possible accuracy. The calibration first uses the spectrum analyzer to measure the down-link (from AP to station) radio signal strength from the Access Point at various attenuation points, with an attenuating placed in between the two. The attenuation is achieved by tuning down the radio signal power the attenuating receives from the AP. For example, if the attenuating receives the signal strength of -20 dBm from the AP, it will tune it down to -30 dBm. As a result, the AP signal strength will be -30 dBm when received by the spectrum analyzers. The measurements are carried out at on all channels applicable to the 802.11 protocol used on the wireless network adapter being calibrated. Once the benchmark values are established using the spectrum analyzer, we then perform the same measurement procedures with an 802.11 wireless network adapter (for example, AirMagnet 802.11 a/b/g/n Wireless PC Card) and adjust the values in reference to the benchmark values.

Let us consider an example. If at Attenuation Point A, the spectrum analyzer displays a radio signal power value of -20 dBm and the adapter being calibrated displays -30 dBm, AirMagnet adds 10 dBm to bring it to line up with the benchmark values. The pre-defined offsets are relative to the spectrum analyzer. In other words, the pre-defined calibration patterns will make the target WiFi adapter to report signal strength readings similar to those reported by professional grade spectrum analyzers. For the same wireless network adapter, this same procedure is repeated on every applicable channel/frequency. This is how the pre-defined calibration values are derived. All calibration data involving those pre-calibrated wireless network adapters are included in the application.

To use pre-defined calibration:

- 1) Click the down arrow and verify if your wireless network adapter appears as a pre-defined Calibrated adapter. See Figure 4-27.

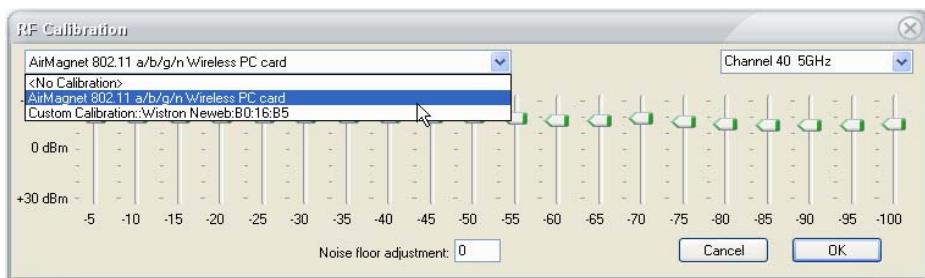


Figure 4-27: Using a pre-calibrated wireless network adapter

- 2) Select it if the name of your wireless network adapter appears (for example, AirMagnet 802.11 a/b/g/n/ Wireless PC Card as shown in the figure) in the list.
- 3) Click OK.

The above three steps are all the user needs to do if the wireless network adapter has been identified as Pre-Defined Calibration (by AirMagnet). No other action is needed. However, this does not mean that the user cannot make any change to a pre-calibrated wireless network adapter. On the contrary, AirMagnet does allow the user to make changes to a

pre-calibrated wireless network adapter. In this case, you are actually making custom calibrations on the basis of a predefined calibration. Any custom calibration made in this way will not change any of the signals values that are dependent on the pre-calibration setting. Instead, it updates the custom calibration option with the new settings. The following paragraph discusses how to make changes to settings of a pre-calibrated wireless network adapter.

To make changes to a pre-defined calibration:

- 1) Repeat Steps 1 through 2 in the previous paragraph.
 - 2) From the upper-right corner, click the down arrow and select a channel of interest.
 - 3) Use the sliders to turn up or down the RF signal strength as desired.
 - 4) When the “**Create a custom RF calibration based on current settings?**” message appears, click **Yes**.
 - 5) Continue to adjust the signal strengths with the sliders.
 - 6) Adjust the noise floor by entering a desire value in the **noise floor adjustment** box.
 - 7) Click **OK** to implement the change.
-

Custom RF calibration on a pre-calibrated wireless network adapter must be done channel by channel, one at a time. This is because changes made to a particular channel apply to that channel only. If you want to change the pre-calibration on another channel, you have to repeat the same steps above.

Custom Calibration

Custom Calibration can be used when you want to create your own calibration table for your wireless network adapter from the RF Calibration dialog box.

Custom calibration patterns can be created to equalize the signal strength readings between any combination of WiFi adapters. Begin by measuring (similar to the process defined in the pre-calibration section) two different radios with zero offsets at varying distances, comparing the received signal strengths at each distance, then calculating the differences between WiFi adapters and using the differences to set the offset of one radio in an effort to match the signal strength reading of the other WiFi adapter. In doing this, you establish a series of reference signal values which can be used while custom-calibrating a wireless network adapter in AirMagnet WiFi Analyzer.

This feature allows you to calibrate the RF signal strength and noise floor of the wireless network card in 5-dBm increments. This way you can normalize different WiFi adapters to exhibit similar signal level readings. Without using this feature, the signal level readings may vary significantly between WiFi adapter from different vendors, or even between different models from the same vendor.

The horizontal numbers (-5 to -100) represent the signal strength levels received by a WiFi adapter. At each signal strength level, an offset can be set (from -30dB to +30dB) by adjusting the sliders up or down.

To custom-calibrate a wireless network adapter's RF signal power:

- 1) From the drop-down list menu, select **Custom Calibration** (The name of your wireless network adapter should be appended here, if it has not been pre-calibrated). See Figure 4-28.

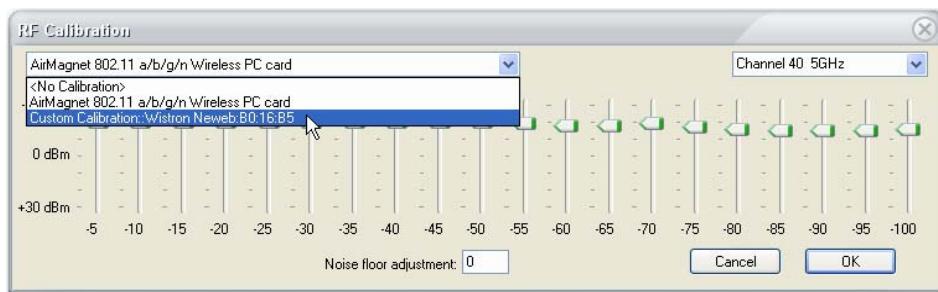


Figure 4-28: Calibrating an uncalibrated wireless network adapter

- 2) From the upper-right corner, click the down arrow and select a channel of interest.

Normally, RF calibration is performed on a per-channel basis unless you want to apply the same calibration to all channels. In this case, you should select **All Channels** from channel list menu.

- 3) Use the sliders to offset the differences in signal strength between the reference values and those of the wireless network adapter you are calibrating.
- 4) If you wish, highlight the number for noise floor adjustment box and type a new value over it.
- 5) Click OK when complete.

Configuring Packet Capture Filters

AirMagnet uses various sampling techniques to scan all available channels for 802.11 frames for statistical analysis. In order to find and solve complex protocol problems quickly, you must first narrow the scan down to a specific SSID or AP and the associated channel. Then you should use various filter options in AirMagnet to discard those unwanted 802.11 packets. These basic troubleshooting techniques will help detect and pinpoint any problem that may exist.

Setting Up a New Filter

To configure filter settings:

- 1) From the AirMagnet Config screen, click the Filter tab. The Filter configuration screen appears. See 4-15.

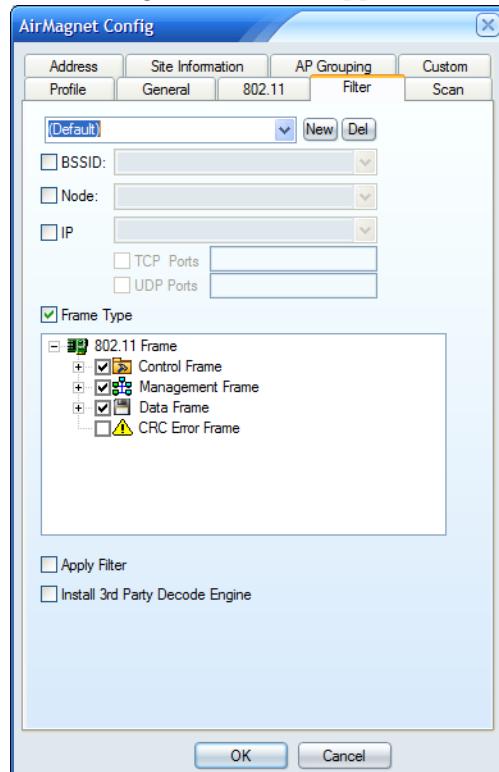


Figure 4-29: Configuring packet filters

- 2) Click New, and enter a name for the filter.

You can select one filter option from the remaining fields; check the check box next to the filter type you wish to implement (BSSID, Node, IP, or Frame Type) and make the selections as described below.

- 3) To use BSSID, click the BSSID radio button, and select a BSSID from the drop-down list.

- 4) To use Node, click the Node radio button, and select a node from the drop-down list.
- 5) To use IP, click the IP radio button and select an IP address; then check the TCP Ports and/or UDP Ports check box and enter the port number(s).
- 6) To use Frame Type, click the Frame Type radio button.
- 7) Expand the frame options one by one.
- 8) Uncheck all frame types, and then select only those you want to include in the filter. See Figure 4-30.



Figure 4-30: Setting Data Frame filters

- 9) Optionally, check the Enable Filter check box. This box must be checked if you wish to use your filter.
- 10) Click OK when completed.

*When **Enable Filter** is selected, the **Filter** check box on the Decodes screen will be automatically checked, meaning that only the frames that match the parameters of the filter will pass through the filter.*

Removing an Existing Filter

You can remove a filter that is no longer in use.

To delete a filter:

- 1) From the AirMagnet Config>Filter screen, highlight the filter from the filter drop-down list.
- 2) Click Del .
- 3) Click OK when completed.

Install 3rd Party Decodes Engine

If you did not choose to install 3rd Party Decodes during product installation, you may choose to do it here.

The upper-layer decode support feature will decode the upper layers of your capture files.

To install the 3rd Party Decodes Engine:

- 1) Check 3rd Party Decodes Engine. Doing this will begin running its installation.
- 2) Agree to the GNU license terms. See [Appendix D, “Upper-layer decode support license”](#)
- 3) You may also choose to permit everyone who uses the computer to access this feature.

Configuring Channel Scan Settings

Configuring channel scan settings allows you to decide which channels are to be scanned and the frequency at which they are scanned.

Regulatory rules dictate the radio frequencies (channels) and emission powers for the 802.11 standards. To comply with these regulatory domains, WLAN devices are pre-configured to operate on various channels in different countries worldwide. Table 4-4 summarizes the channel allocation in major parts of the world.

Table 4-4: Worldwide Radio Channel Assignment

Region/Country	802.11b/g	802.11a
America	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 149, 153, 157, 161
Most parts of Europe and Australia	1 ~ 13	36, 40, 44, 48, 52, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
France	10 ~ 14	36, 40 44, 48, 52, 56, 60, 64
Spain	10 ~ 11	36, 40 44, 48, 52, 56, 60, 64

Table 4-4: Worldwide Radio Channel Assignment

Region/Country	802.11b/g	802.11a
Japan	1 ~ 14	36, 40, 44, 48, 52, 56, 60, 64
Pacific Rim (China, Taiwan, Hong Kong, Singapore, Korea)	1 ~11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

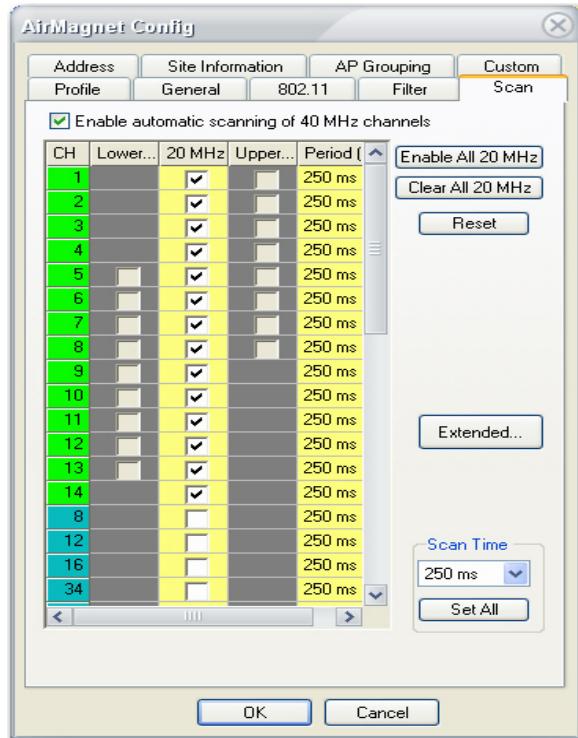
Despite these regulatory requirements, there are occasions where the prohibited channels do contain 802.11 devices due to misconfiguration or the presence of a malicious rogue AP. Since AirMagnet scanning does not emit any radio waves, it is completely compliant to all the regulatory rules.

The benefits of using the world-mode operation are threefold:

- 1) For WLAN administrators and consultants who travel around the globe, AirMagnet's world-mode feature allows easy selection among the regulated channels.
- 2) Since rogue APs may operate in any channel regardless of regulatory requirements, the ability to scan all channels for rogue APs is essential.
- 3) Being able to spot misconfigured WLAN devices operating in violation of regulatory rules is also an added benefit.

To configure channel scan settings:

- 1) From the AirMagnet Config, select the Scan tab. The AirMagnet Config>Scan screen appears. See [Figure 4-31](#).

**Figure 4-31: Selecting channels to be scanned**

As shown above, the channels are color-coded; those highlighted in green are 802.11b/g/n channels, and those in blue are 802.11a/n channels. By default, the *Enable Automatic Configuration of 40 MHz Channels* check box is checked, which allows the application to automatically detect 40-MHz transmissions. If you uncheck this option, then you have to manually select the channels in either or both the Lower 40 MHz or Upper 40 MHz columns. Lower 40 MHz means the lower 40 MHz channels to the left of the center

frequency while the upper 40 MHz channels refer to channel to the right of the center frequency.

- 2) Click Clear All to remove the default scan settings, and then check only the channel(s) you want to focus on.
- 3) Click in the Period (ms) field for each channel and specify a scan time interval from the drop-down list. See [Figure 4-32](#).



Figure 4-32: Changing scan frequency

- 4) Optionally, click the down arrow below Scan time (at the bottom right of the window) to select a time, and then click Set All to change the scan time of all channels to the selected value.
- 5) If necessary, click Reset to restore the default scan settings.
- 6) Click OK when completed.

Configuring Channel Scanning for Multiple Adapters

In order to allow users to specify custom channel scan options for each individual adapter in use, the Scan tab of AirMagnet WiFi Analyzer's configuration menu has been modified slightly, as shown in [Figure 4-33](#).

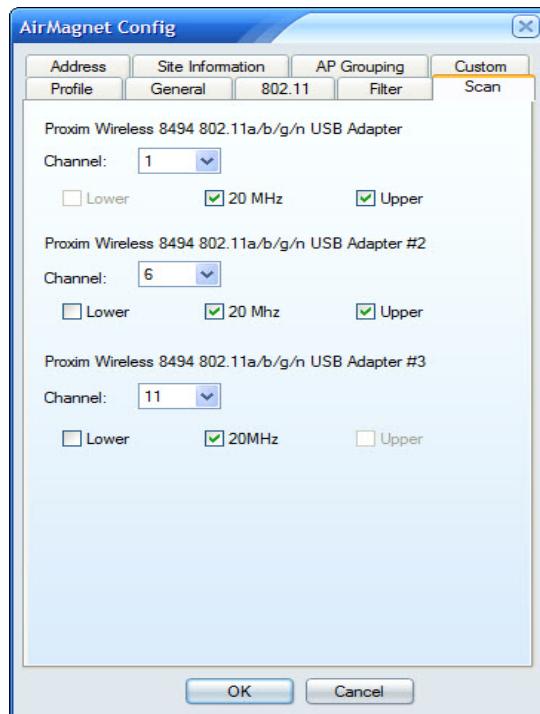


Figure 4-33: Channel Scan Options

As shown above, individual channel selection drop-down menus are implemented for each adapter actively capturing within the application. Simply specify the channel desired for each adapter and click OK to adjust scan settings.

Scanning Extended 802.11a Channels

Extended channels refer to the 802.11a channels not normally used by most businesses or countries. You can scan only the standard country channels by clicking the “Select Country Code Channels” button. However, since attacks from hackers and outside sources may not always choose to attack from the usual channels, you may scan the extended ones that are normally unused by clicking the “Extended...” button. Some devices also use extended channels by default (or are

deliberately configured to do so); setting AirMagnet WiFi Analyzer to scan these channels will help ensure that all the devices in your network are configured properly according to your company's policies. See [Figure 4-34](#).

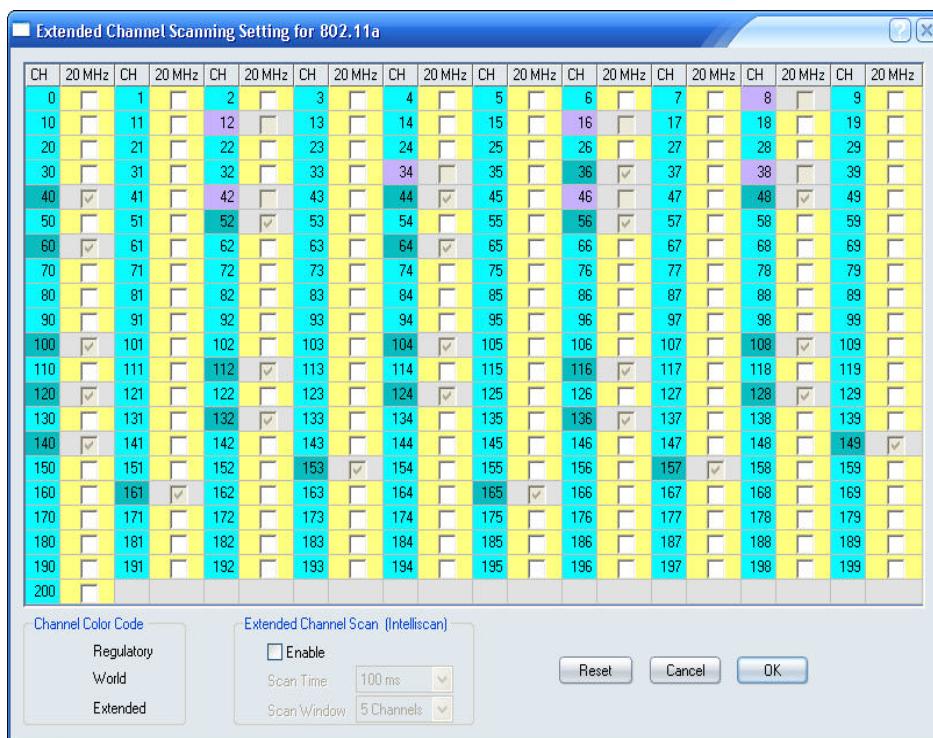


Figure 4-34: Extended Channels Scan

You may configure as many channels as you desire for 802.11a scanning. AirMagnet WiFi Analyzer will include the channels you select here in its scanning process along with the standard channels. Further, you can use the tools at the bottom to customize how AirMagnet WiFi Analyzer scans the channels you don't check as well.

During a normal scan, AirMagnet WiFi Analyzer will scan the standard channels and the extended ones that you select. It will then scan a number of the 802.11a channels you don't have selected, which you can control using the Scan Time and Scan Window options at the bottom. Scan time refers to the amount of time spent on the scan, and

the window is the number of channels scanned at a time. After your specified window of channels has been scanned, AirMagnet WiFi Analyzer will re-scan the standard channels and then continue with the extended ones.

The Intel 2915ABG card does not support extended 802.11a channel scanning.

Configuring System Address Book

AirMagnet captures the MAC addresses of all wireless devices it has discovered since it was turned on, and saves them in its internal database. Creating an address book allows you to match the MAC address of each wireless device with an alias so that it is easy to remember and manage your wireless LAN assets.

Creating an Address Book

This section shows how to configure an address book by adding MAC address-alias pairs to the address table one at a time.

To create an address book:

- 1) From the AirMagnet Config screen, click the Address tab. The AirMagnet Config>Address screen appears. See [Figure 4-35](#).

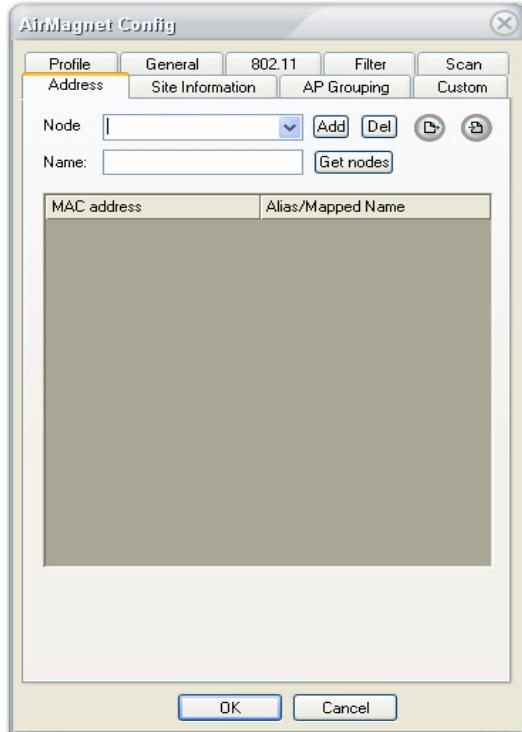


Figure 4-35: Configuring an address book

- 2) Click the down arrow next to the Node field, and select a MAC address from the drop-down list.
- 3) Click in the Name field, and enter an alias.
- 4) Click Add. The newly created MAC address – alias pair appears in the address table below.
- 5) Repeat Steps 2 through 4 to add more entries to the address table.

*Alternatively, you can click the **Get nodes** button to let the program automatically populate the address book with all the MAC addresses*

AirMagnet WiFi Analyzer has captured since the moment it was turned on. Once the table is populated, you can match the entries with aliases.

To create an address book using the Get Nodes button:

- 1) From the AirMagnet Config>Address screen, click Get nodes. The MAC address column of the address table will be filled with MAC addresses that AirMagnet has captured. See Figure 4-36.

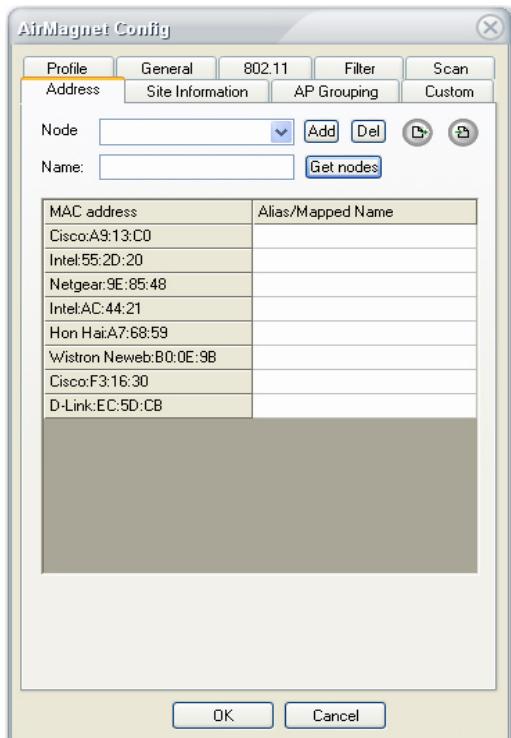


Figure 4-36: Adding devices to an address book

- 2) Click in the Mapped Name column, and enter an alias to match the MAC address on the left.
- 3) Repeat Step 2 to add additional aliases.
- 4) Click OK when completed.

Removing an Entry from the Address Book

You can delete an entry (i.e., a MAC address, or a MAC address—alias pair) from the address book.

To delete an entry from the address book:

- 1) Highlight the entry you wish to delete.
- 2) Click Delete.
- 3) Click OK to exit the AirMagnet Config>Address screen.

Adding Site Information

After all the system parameters are set up, you may want to add some site-specific to the profile. This will help you archive your site surveys and system profiles.

To add site information to the profile:

- 1) From the AirMagnet Config screen, click the Site Information tab. The AirMagnet Config>Site Information screen appears. See [Figure 4-37](#).

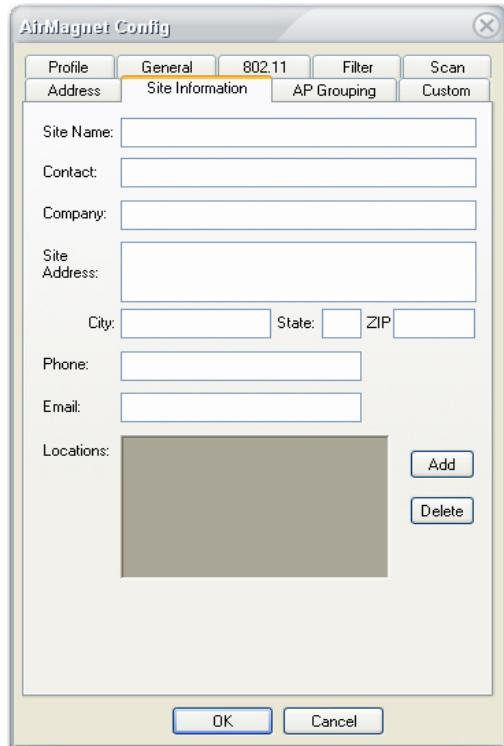


Figure 4-37: Configuring site information

- 2) Fill out the form by entering the information.

- 3) Click Add. An entry “Location 1” will appear in the Locations field. See Figure 4-38.

The screenshot shows a configuration window for site information. It includes fields for Site Name (Plant A), Contact (John Doe III), Company (ABC Inc.), Site Address (1 Street St.), City (Anywhere), State (US), ZIP (00000), Phone ((555) 555-1234), Email (JDoe@company.com), and Locations (Location 1). The 'Locations' field contains the entry 'Location 1'. To the right of the locations list are two buttons: 'Add' (highlighted with a mouse cursor) and 'Delete'.

Figure 4-38: Adding site information

- 4) If you prefer, highlight “Location 1” and overwrite it with a unique name.
5) Click OK when completed.

AP Grouping

The AP Grouping tab allows you to set up specific names for single devices that utilize multiple VLANs under different SSIDs. This comes into play on many pages, where the separate SSIDs will show up and appear to be several different devices, when in truth, they belong to a single object. The AP Grouping feature will provide you with a means of seeing that these devices all belong to the same VLAN. See Figure 4-39.

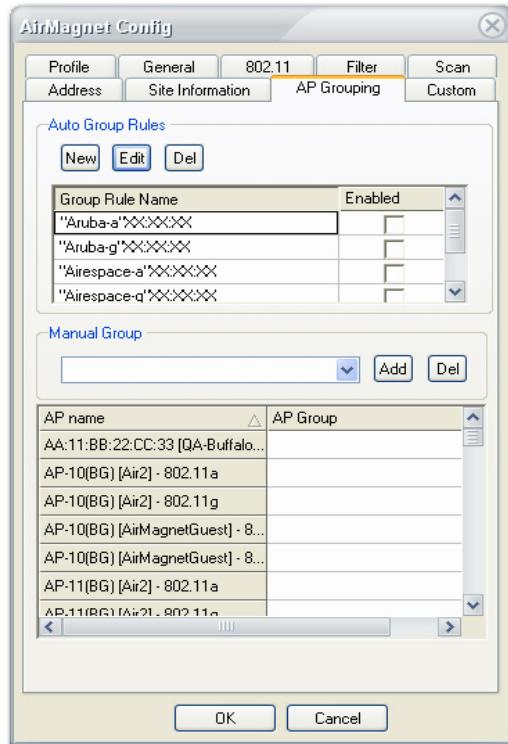


Figure 4-39: AP Grouping Tab

Auto Group Rules

AirMagnet WiFi Analyzer comes with several built-in “automatic” AP grouping rules. If you enable them, they will automatically group all devices meeting the criteria specified in the rule under a single AP Group. This is helpful if your company uses devices from a specific vendor; AirMagnet WiFi Analyzer will recognize those devices and group them accordingly. To see the criteria that the auto group rules use, select one and click the “edit” button. See Figure 4-40.



Figure 4-40: Editing an Auto Group Rule

Table 4-5 describes the different fields you may configure.

Table 4-5: Auto AP Group Rules

Field	Function
Vendor ID	This field allows you to specify the vendor name that the rule will apply to.
Media Type	This field specifies what device media type the rule is intended to classify.
MAC Address	Select the hex digit you wish the grouping to start from.
Contiguous MACs	Select the number of consecutive devices you wish to classify in the group.
Address Order	This determines whether your rule will count up or down towards your specified maximum.

Manual Group Rules

The lower half of the AP Grouping tab allows you to set up manual groups for your devices. Using this feature, you can create your own AP Group name and then select exactly which devices you wish to be classified under it.

To create a new group:

- 1) Click the Add button. The Manual Group dialog box appears. See Figure 4-41.



Figure 4-41: Creating a New Manual Group

- 2) Enter your new AP Group name and click OK.
- 3) Then simply click the devices you wish to add to it.

Whenever you select a device, a drop-down box will appear to the right of its name, allowing you to select which group it belongs to. See Figure 4-42.

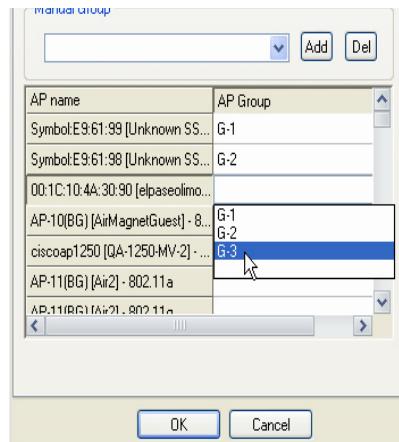


Figure 4-42: Adding Devices to a Manual Group

Customizing the User Interface

The Custom tab allows you to modify the appearance of AirMagnet WiFi Analyzer; it contains several options to adjust your layout. See Figure 4-43.



Figure 4-43: Custom Tab

As shown in [Figure 4-43](#), there are three main fields in the custom tab. Table 4-6 describes each field and its function.

Table 4-6: Custom Options

Field	Description
Skin	The Skin drop-down allows you to select from the three pre-defined skins. Alternatively, you can select Custom and select a skin of your own, as described below.
Custom Skin Name	If you have selected Custom from the skin drop-down, you can click the Browse button and browse to the location you have saved your custom skin. Skins must be in the .msstyle format, and can be downloaded from various sources on the Internet.
Show Menu Bar	Checking this box will display the File, Tools, and Help menus across the top of the program. These options perform many of the same tasks as the buttons in the tool bar do.

Chapter 5: Managing Network Policies

Chapter Summary

This chapter discusses how to configure and manage wireless network security and performance policies. From our discussions in the preceding chapters, it is apparent that network policies are an important component of the AirMagnet solution. Therefore, the ability to create and manage policies to address the specific needs of your network is essential to successful implementation of the AirMagnet technology.

The security and performance alarms generated by the AirMagnet AirWISE expert engine have proved powerful in WLAN network management, especially for managing large-scale enterprise WLAN networks. AirMagnet uses a three-level policy structure that greatly facilitates WLAN event management and analysis. Understanding this structured policy configuration not only helps WLAN administrators characterize and interpret the nature of various network policy violations, but also enables them to take the right course of action when needed.

This chapter covers the following main topics:

- Customizing the default alarms settings to your needs.
- Creating event alarms using the Notification Wizard.
- Configuring network policies using the Policy Wizard.

The Policy Management Screen

Managing network policies involves creating new policy rules and modifying or removing existing ones. All these tasks are performed through the AirMagnet Policy Management screen.

To access the AirMagnet Policy Management screen:

- 1) Click the drop-down arrow attached to (Configure) and select Policy Management... The AirMagnet Policy Management screen appears. See Figure 5-1.

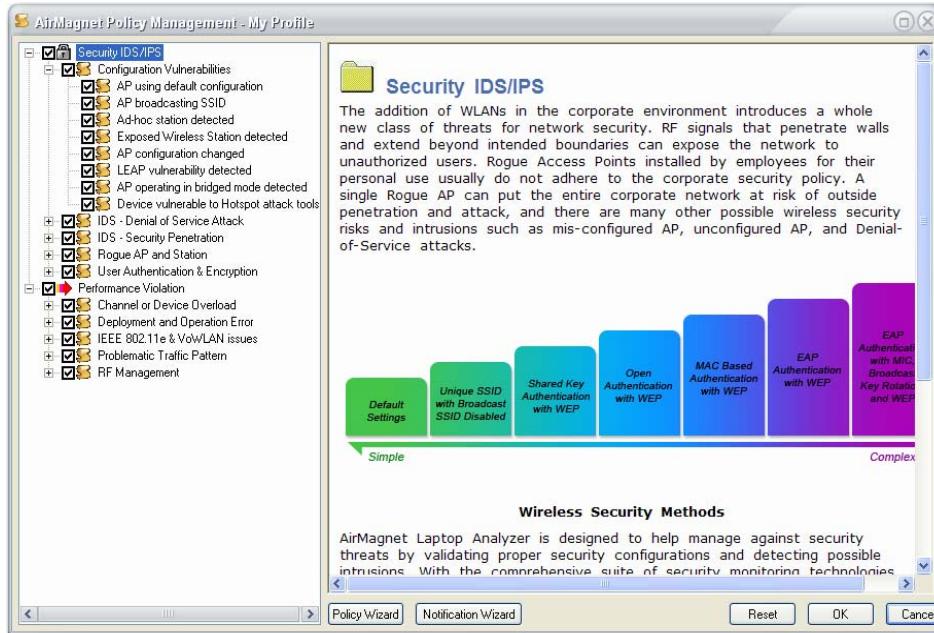


Figure 5-1: AirMagnet Policy Management screen (1)

As shown in Figure 5-1, the AirMagnet Policy Management screen consists of two parts: the Policy Tree on the left and the policy description on the right. There are also some control buttons along the bottom of the screen for managing policies.

The Policy Tree

The Policy Tree displays all the network policies that AirMagnet supports. The policies are divided into two major categories: Security IDS/IPS and Performance Violation. Each category can be further divided into several subcategories. At the lowest level of each subcategory are individual policy violation alarms. This layered policy structure makes it easy to manage your network policies. You can click the plus sign to expand a node or a minus sign to collapse it. The check mark in the box means that the policy is activated. When an upper-level policy is activated (checked), all entries below it will be activated as well. You can deactivate an alarm by unchecking the corresponding check box.

The Policy Description

The policy description section offers detailed explanation of the policy or alarm selected from the Policy Tree, along with a recommended solution to the identified problem. The content of the policy description is directly associated with what is being selected in the Policy Tree.

Managing Network Policy Profiles

A network policy profile contains various policy rules that dictate the issuance of alarms when the rules are being violated and the way the responsible parties should be notified should an alarm be generated. Therefore, managing a network policy profile involves adding, changing, and/or deleting policy rules that contain alarms, notifications, and a number of other parameters.

Creating New Policy Rules

A policy rule is a set of parameters a user selects in relation to a policy alarm. The parameters are used as the alarm trigger, automatically telling the program to generate the alarm when they are being violated. Policy rules are part of a profile. The default AirMagnet WiFi Analyzer profile comes with some pre-configured policy rules that address the needs of the WLAN in general. For novice users unfamiliar with AirMagnet WiFi Analyzer's policy management procedures, these default policies come handy and offer some basic protection for the wireless network. However, to take full advantage of the AirMagnet WiFi Analyzer's policy management feature,

network administrators must be able to configure and manage network policy rules that best match the specific needs of their networks. This section discusses the procedures involved in creating a policy rule.

To create a new policy rule:

- 1) From the AirMagnet Policy Management screen (Figure 5-1), expand the Policy Tree and select a policy alarm of interest. The AirMagnet Policy Management screen refreshes. See Figure 5-2.

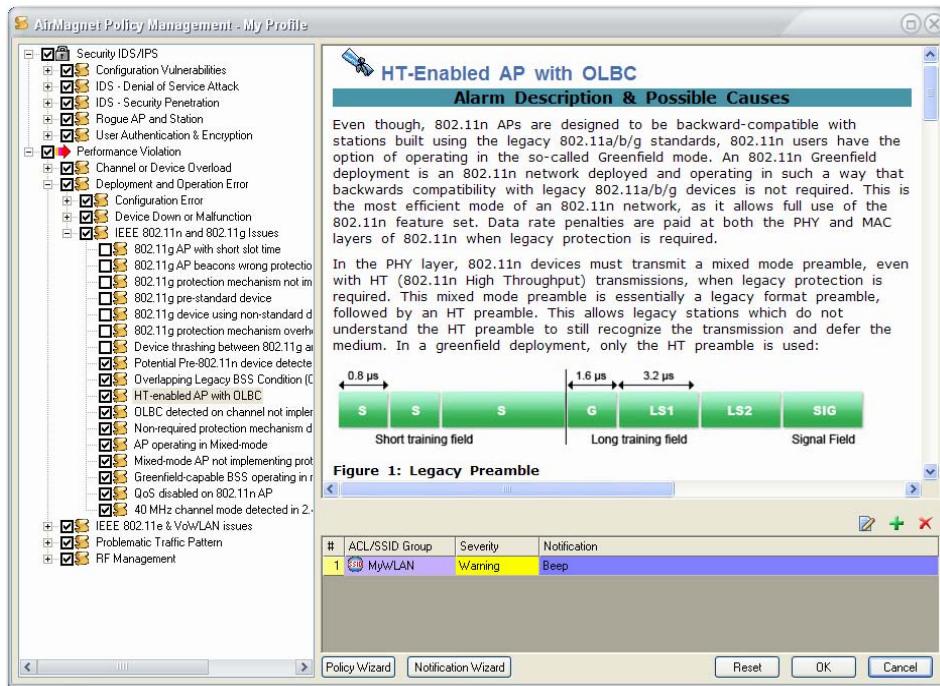


Figure 5-2: AirMagnet Policy Management screen (2)

As shown in Figure 5-2, a table appears in the bottom-right side of the AirMagnet Policy Management screen when an alarm is selected in the Policy Tree. The table lists all the policy rules that have been configured in relation to that alarm. Whereas many alarms may have multiple

policy rules, some alarms may only support one policy rule. By default, an alarm should have at least one policy rule associated with it.

- 2) Click  (Add New Policy Rule). The AirMagnet Policy Rule dialog box appears. See Figure 5-3.

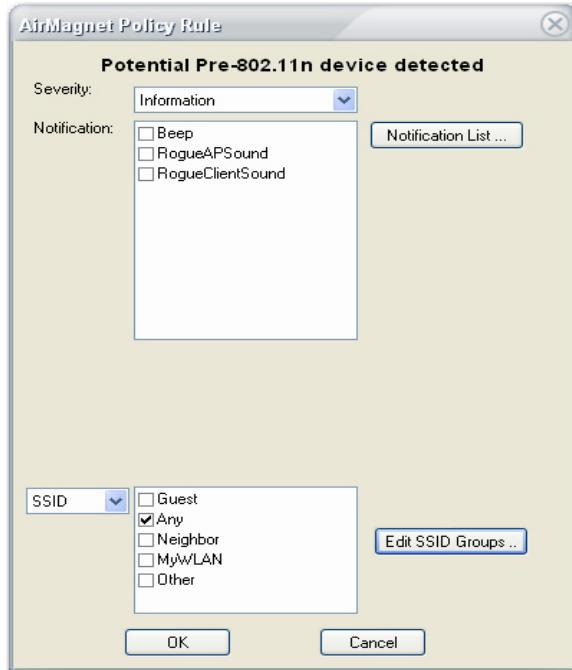


Figure 5-3: AirMagnet Policy Rule dialog box

The AirMagnet Policy Rule dialog box may look different depending on the alarm you select. This is because the parameters are alarm-specific and may apply only to certain alarms. Figure 5-3 shows one variation of the AirMagnet Policy Rule dialog box.

- 3) From the AirMagnet Policy Rule dialog box, make the entries and/or selections as described in Table 5-1.

Table 5-1: Configuring New Policy Rules

Entry	Description
Severity	Click the down arrow and select a level of severity for the alarm.
Notification	Specify the method(s) of notification for the alarm by checking the corresponding check box(es).
	<p>Note:</p> <p><i>If you need to add more notification options to the alarm, click Notification List.... This will open the AirMagnet Policy Notification List dialog box where you can configure more notification options and add them to the list of available notifications (the top part of Figure 5-3). See “Adding Notification Options to an Alarm” on page 227 for details on how to configure and add notification options.</i></p>
ACL/SSID	Click the down arrow and select ACL or SSID.
	<p>Note:</p> <ul style="list-style-type: none"> • <i>If you choose to use ACL, make sure that you have an ACL already configured.</i> • <i>If you choose to use SSID, select the SSID(s) from the list on the right.</i> • <i>You may also edit the SSIDs by clicking the Edit SSID Groups... button. Refer to the relevant section later in this chapter for instructions on how to edit an SSID group.</i>

- 4) Click OK when completed.

The policy rule you have just created will appear in the policy rule table on the AirMagnet Policy Management screen. Refer to Figure 5-2.

Modifying Existing Policy Rules

AirMagnet WiFi Analyzer comes with pre-configured network policies and alarms. They are meant to cover common wireless LAN security and performance issues, and may not quite fit the reality of your network. Also, any policy rule you have configured may become obsolete as your network evolves. Therefore, you need to update your policy profiles by editing the policy rules from time to time.

To edit an existing policy rule:

- 1) From the table on the AirMagnet Policy Management screen (Figure 5-2), select a policy rule of interest and click (Edit Policy Rule). The AirMagnet Policy Rule dialog box appears. See Figure 5-4.

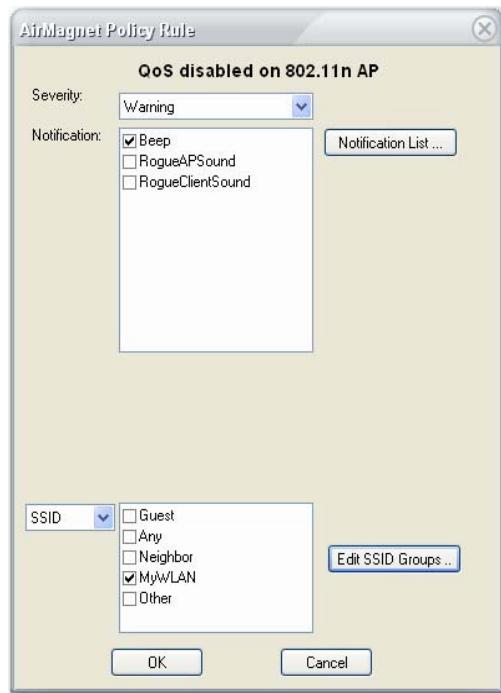


Figure 5-4: Editing an existing policy rule

Unlike Figure 5-3, Figure 5-4 shows an AirMagnet Policy Rule dialog box with the parameters configured for an existing policy rule. Editing an policy rule involves modifying the existing parameters associated with it.

- 2) Make the desired changes as described in Table 5-1.
- 3) Click OK when completed.

The changes you have made to the policy rule will be reflected in the policy rule table on the AirMagnet Policy Management screen. Refer to Figure 5-2.

Deleting an Existing Policy Rule

With the evolution of your WLAN, certain policy rules in a policy profile may become dated to the extent that they should be removed from the policy profile.

It is important to note that AirMagnet WiFi Analyzer requires that an alarm must have at least one policy rule associated with it. For this reason, a policy rule cannot be deleted if it is the only one in the policy table.

To delete a policy rule:

- 1) From the AirMagnet Policy Management screen (Figure 5-2), highlight the policy rule of interest.
- 2) Click  (Delete Policy Rule).
- 3) When a confirmation message appears, click Yes.

The policy rule will be removed from the policy table on the AirMagnet Policy Management screen as soon as you click  , provided that there is more than one policy rule in the table.

Assigning Notifications to Policies

Notifications are an important part of policy rules. They are the ways that AirMagnet WiFi Analyzer uses to notify the responsible parties when policy alarms are being generated. AirMagnet WiFi Analyzer provides a number of notification options. Managing alarm notifications involves the configuration of notification options and assigning them to alarms.

Adding Notification Options to an Alarm

Each alarm can be linked with one or more notification options to notify the responsible parties whenever the alarm is generated. Failure to do so may result in delayed response to looming threats, thus putting the security and performance of your entire network at risk. Adding notification options involves assigning more notification options to an alarm provided that the options are applicable to the alarm. It may also require you to configure some new options from scratch and then assign them to the alarm.

To add notifications to an alarm:

- 1) From the Policy Tree on the AirMagnet Policy Management screen (Figure 5-1), highlight the policy alarm of interest. The AirMagnet Policy Management screen refreshes, showing the policy rule table containing all the policy rules for the alarm. Refer to Figure 5-2.
- 2) From the policy rule table, highlight the policy rule (or the policy rule of interest if there is more than one policy rule) and click  (Edit Policy Rule). The AirMagnet Policy Rule dialog box appears. See Figure 5-5.

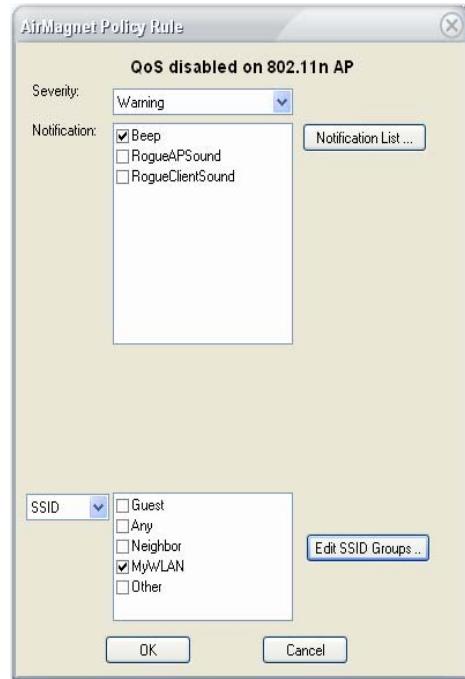


Figure 5-5: Adding more notification options to an alarm

By default, the AirMagnet WiFi Analyzer comes with three basic notification options available for use and “Beep” is assigned to all alarms in any pre-configured policy profile/rule, as shown in Figure 5-5. However, the user can configure the other advanced notification options that the AirMagnet WiFi Analyzer supports and add them to the list of available notifications in the AirMagnet Policy Rule dialog box, where they can be assigned to the selected alarm. The following steps show how to configure and assign notification options to an alarm.

- 3) If want to assign any of the available and applicable notification options to the alarm, check the corresponding check box(es) and click OK.

Once you click **OK**, the AirMagnet Policy Rule dialog box will close and the notification option(s) you have selected will be added to the Notification field of the policy table on the AirMagnet Policy Management screen. See Figure 5-2.

- 4) If you want to configure and use some other notification options, then click **Notification List**. . . . The AirMagnet Policy Notification List appears. See Figure 5-6.

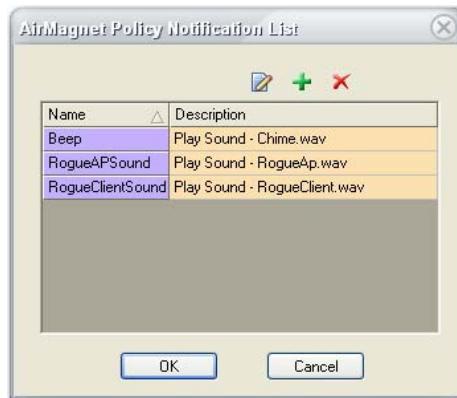


Figure 5-6: AirMagnet Policy Notification List dialog box

The AirMagnet Policy Notification List dialog box is where the user can create and/or modify notification options, which can then be sent to the list of available notification options in the AirMagnet Policy Rule dialog box. Therefore, it contains the same options as those shown in the AirMagnet Policy Rule dialog box. See Figure 5-6.

- 5) Click **+** (Add New Notification). The Notification Type Selection dialog box appears. See Figure 5-7.

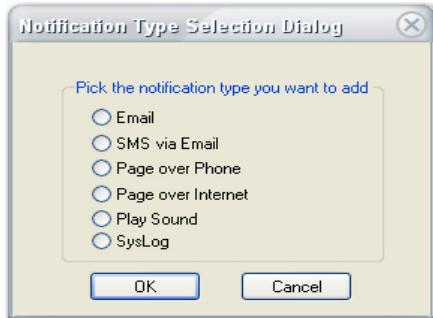


Figure 5-7: The Notification Type Selection Dialog Box

The Notification Type Selection dialog box contains the advanced notification options that AirMagnet WiFi Analyzer supports. These options require custom configurations on a case-by-case basis. See Table 5-2 for a summary of each option.

Table 5-2: Advanced Notification Options

Option	Description
Email	Allows you to configure the notification to send an email to you notifying you of the alarm. You will need to set up your basic email settings (account name, password, outgoing server, etc.) in order to use this option.
SMS via Email	This option is similar to the basic Email option, except that it sends a text message that can be received via a mobile phone. You will need to enter your pager/phone number and an SMS server.
Page over Phone	You can configure the alarm to page your pager/phone upon generating an alert. You will need to enter a TAP Server number to send the pages from.

Table 5-2: Advanced Notification Options

Option	Description
Page over Internet	This option is similar to the Page over Phone selection, but it will use an internet paging service to send the page. You will need to enter a SNPP server instead of a TAP Server Number.
Play Sound	The basic notification option, this allows you to simply assign a sound file to alert you whenever the alarm is generated.
SysLog	This setting will cause the alarm to record an alert in the Windows System Log. You will need to point it to your SysLog server.

- 6) From the Notification Type Selection dialog box, select an option, and click OK. A unique dialog box will appear where you can configure the option.
- 7) Configure the option, and click OK. The dialog box for the selected notification configuration will be closed.
- 8) Click OK to close the AirMagnet Policy Notification List dialog box.
- 9) From the AirMagnet Policy Rule dialog box, select the newly created notification option and click OK. The notification option will be added to the policy table on the AirMagnet Policy Management screen. Refer to Figure 5-2.
- 10) Click OK to close the AirMagnet Policy Management screen.

Modifying Alarm Notification Options

Modifying alarm notifications involves changing the notification options assigned to an alarm. You may replace an existing notification option with another option, provided that the new option is applicable to the alarm, or you may modify the configuration of an existing notification option.

To edit an existing alarm notification:

- 1) From the policy rule table on the AirMagnet Policy Management screen, highlight the policy rule and click  (Edit Policy)

Rul e) . The AirMagnet Policy Rule dialog box appears. See Figure 5-8.

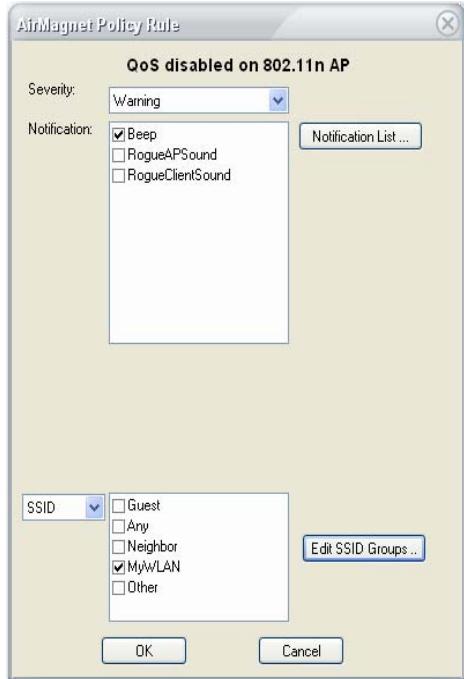


Figure 5-8: Assigning alarm notification options

- 2) If you want to replace the existing notification option with another available option, uncheck the existing option and check another one from list of available options, and then click OK.

Once you have clicked OK, the AirMagnet Policy Rule dialog box will close and the newly assigned notification option will appear in the policy table on the AirMagnet Policy Management screen, replacing the previous old notification option.

- 3) If you want to modify the settings of an existing notification option, click **Notification List...** . The AirMagnet Policy Notification List dialog box appears. See Figure 5-9.



Figure 5-9: Editing a notification option

- 4) Highlight the notification option (e.g., “Beep” in Figure 5-9) and click (Edit Notification). The configuration dialog box for the notification option appears. See Figure 5-10.

Since you are modifying the settings of an existing notification option, the name of the notification is greyed out. This means that the name of the name of the notification cannot be changed. See Figure 5-10.



Figure 5-10: Editing the settings of a notification

- 5) From the configuration dialog box, make the desired changes, and click OK to close the configuration dialog box. The changes

you have made appears in the AirMagnet Policy Notification List dialog box.

- 6) Click OK to close the AirMagnet Policy Notification List dialog box.
- 7) Click OK to close the AirMagnet Policy Rule dialog box.
- 8) Click OK to close the AirMagnet Policy Management screen. The changes in the notification option will be implemented in the policy rule for the selected alarm.

Deleting Existing Alarm Notifications

The AirMagnet Policy Rule dialog box contains all the notification options that have been configured. While you can assign or remove any of them to or from an alarm from the AirMagnet Policy Rule dialog box, you must delete the notification from the AirMagnet Policy Notification List dialog box if you want to remove it permanently from a policy profile.

To delete an alarm notification option:

- 1) From the AirMagnet Policy Notification List dialog box, highlight the notification option to be deleted and click  (Delete Notification). A confirmation message box appears. See Figure 5-11.



Figure 5-11: Deleting a notification option

- 2) Click Yes to confirm. The selected notification option will disappear from the AirMagnet Policy Notification List dialog box.
- 3) Click OK to close the AirMagnet Policy Notification List dialog box.
- 4) Click OK to close the AirMagnet Policy Rule dialog box.
- 5) Click OK to close the AirMagnet Policy Management screen.

The notification option will be permanently removed from the current policy profile. If you want to remove the same notification option from all the other policy profiles, you have to remove it from one profile at a time; if you want to restore a deleted notification option, you must reinstall the AirMagnet WiFi Analyzer.

Assigning Policies to ACL or SSID Groups

As mentioned at the beginning of this chapter, ACL and SSID groups are also an important part of AirMagnet network policy profiles and play a vital role in network security and performance management. Each ACL or SSID group contains information of specific wireless devices. When an ACL or SSID group is included in a policy rule, it tells the program that only the devices that belong to the ACL or SSID group are legitimate and that any other device is rogued, and will trigger the policy alarm if detected.

Whether to use ACL or SSID in a policy rule depends on the policy alarm you select. While some alarms can only be associated with ACLs, others may be applied only to SSIDs. There are also alarms that can be applied to either ACLs or SSIDs. Therefore, you may notice the differences in the AirMagnet Policy Rule dialog box when configuring policy rules involving different alarms.

Assigning Policies to ACL Groups

An ACL group is a list of wireless devices grouped together by MAC address. AirMagnet WiFi Analyzer uses ACL groups to effectively manage and control access to the wireless network. When an ACL group is assigned to a policy, it becomes the trigger to the alarm to which it is assigned. Access to the network will only be granted to devices within the ACL group. Any device from outside the ACL group will not only be denied access but also trigger the alarm whenever it is detected on the network.

To assign a policy to an ACL group:

- 1) From the AirMagnet Policy Rule dialog box (Figure 5-8), Select ACL and click Edit ACL Groups. . . . The ACL Groups dialog box appears. See Figure 5-12.



Figure 5-12: Adding an ACL Group

- 2) From the ACL Groups dialog box, click (Add ACL Group). A new entry "New Group" appears in the table. See Figure 5-13.



Figure 5-13: Adding a new ACL Group

- 3) Highlight the entry and type a unique name over it, and click OK. The new ACL group will be added to the list of available ACL groups in the AirMagnet Policy Rule dialog box.
- 4) Select the newly created ACL group and click OK to close the AirMagnet Policy Rule dialog box.
- 5) Click OK to close the AirMagnet Policy Management screen.

Steps 1 through 5 above enable you to create a new ACL group, which is empty at this point because no devices have been added to it. In order to incorporate the ACL group in policy management, you must add devices to it. The following steps show how to add devices to an ACL group.

Adding Devices to an ACL Group

To add devices to an ACL Group:

- 1) From the Start page, click (Configure). The AirMagnet Config dialog box appears. See Figure 5-14.

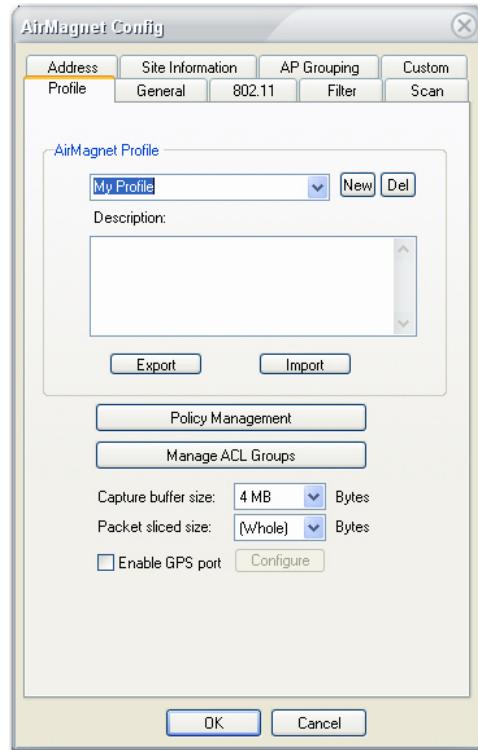


Figure 5-14: Configuring a profile

- 2) Click Manage ACL Groups. . . . The Manage Access Control List dialog box appears. See Figure 5-15.

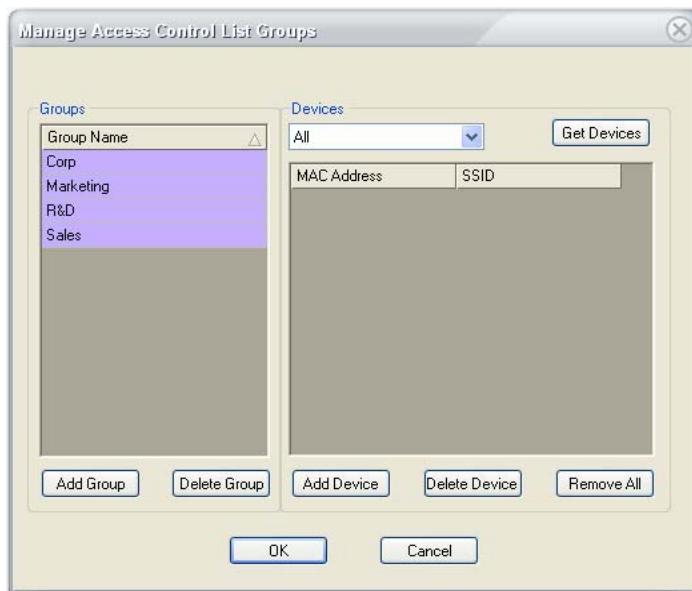


Figure 5-15: Configuring an ACL Group

Corp is the default ACL group that contains all the devices AirMagnet WiFi Analyzer has discovered on your network. You need to create new ACL groups and assign the devices to different groups. See Table 5-3 for descriptions on the buttons and options in the above dialog.

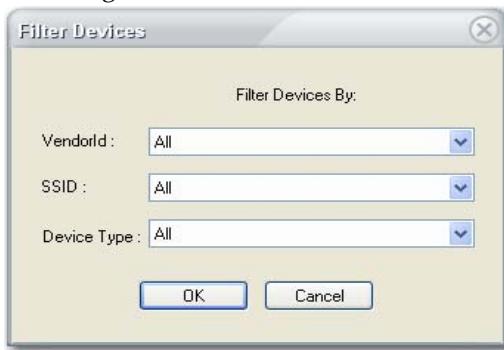
Table 5-3: Managing ACL Groups

Option	Description
Devices	This drop-down box allows you to specify the type of devices you wish to include (AP, STA, or Ad-Hoc).
Get Devices	This button will bring up the Filter Devices dialog (see Figure 5-16) and allow you to scan for the devices to add to the selected group.

Table 5-3: Managing ACL Groups

Option	Description
Add Group	This button allows you to create a new ACL group. To rename the group, double-click the group name and enter your own custom name.
Delete Group	This button will delete the selected ACL group.
Add Device	This button allows you to manually add a device by entering its MAC Address.
Delete Device	This button will delete the selected device.
Remove All	This button removes all device entries in the selected group.

- 3) Select the name of the newly created ACL group (such as "R&D" in Figure 5-15).
- 4) Click Get Devices. The Filter Devices dialog box appears. See Figure 5-16.

**Figure 5-16: Adding devices to an ACL group**

- 5) Use the three filters to select the devices to be added to the ACL group, and click OK to close the Filter Devices dialog box. See Table 5-4 for a description of the filter options.

Table 5-4: Filter Options

Field	Description
Vendor ID	This field allows you to select the vendor that produces your network devices. The list will be filtered automatically to include only devices from that specific vendor.
SSID	This field will allow you to add only devices that use a specific SSID.
Device Type	This field will let you specify the device type you are interested in adding (AP, STA, or Ad-Hoc).

- 6) Click OK to close the Manage Access Control List Groups dialog box.
- 7) Click OK to close the AirMagnet Config dialog box. The “R&D” ACL Group is now populated with the devices you specified.

Assigning Policies to SSID Groups

SSID groups can also be tied to network policies to protect a wireless network against potential security and performance threats. This is done by putting wireless devices into different SSID groups and then assigning policies to them. It's another efficient way to apply network policies to devices.

Assigning Policies to Existing SSID Groups

An existing SSID group is one that is already in the AirMagnet Policy Rule dialog box when it opens. AirMagnet WiFi Analyzer comes with a list of SSID groups which can be used right away. See Figure 5-17.

To assign a policy to an existing SSID group:

- 1) From the AirMagnet Policy Management screen, select a policy and click  (Add Policy Rule).
- 2) Select SSID and check the individual SSID or SSIDs of interest.

- 3) Click OK.

Modifying Existing SSID Groups

The existing SSID groups come handy when assigning policies to them. Sometimes, you may want to modify an existing SSID group before assigning policies to it. Modifying an SSID group may involve changing its name as well as the SSIDs in it.

To modify an existing SSID group:

- 1) From the AirMagnet Policy Rule dialog box, Select SSID and click Edit SSID Groups. . . . The SSID Groups dialog box appears. See Figure 5-17.

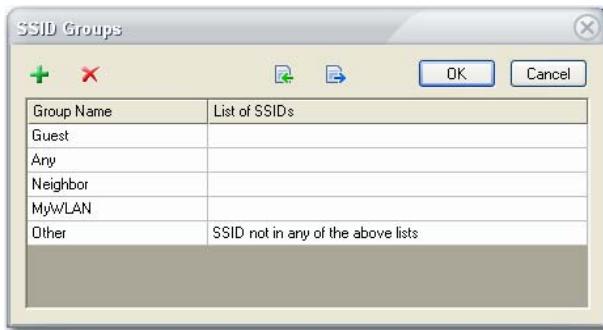


Figure 5-17: Modifying an SSID group

- 2) Highlight the name of the SSID group and type a unique name over it (if you want to rename it).

Note that you may not rename the pre-generated groups.

- 3) Click to highlight the corresponding SSID List field and enter the SSIDs to be included in the SSID group.

Entries are case-sensitive and must be separated by commas (e.g., SSID1, SSID2, etc.).

- 4) Click OK to close the SSID Groups dialog box.

- 5) From the Policy Rule dialog box, select the SSID group and click OK.

Creating a New SSID Group

AirMagnet WiFi Analyzer also allows users to create SSID groups from scratch, if they choose to do so.

To create a new SSID group:

- 1) From the SSID Groups dialog box (Figure 5-18), click  (New SSID Group). A new entry marked “New Group” appears in the dialog box. See Figure 5-18.

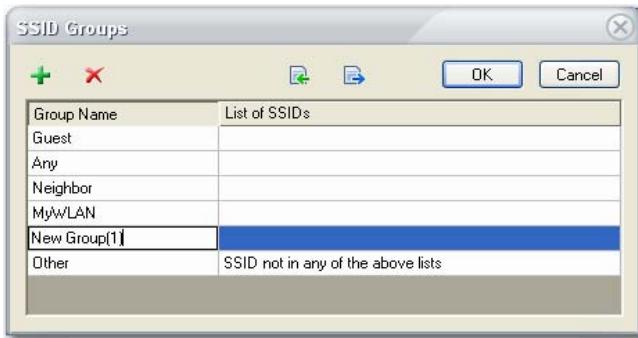


Figure 5-18: Creating a new SSID group

- 2) Highlight the new entry and type a unique name over it.
- 3) Highlight the SSID List field and enter the SSIDs to be included in this group.
- 4) Click OK to close the SSID Groups dialog box.
- 5) From the AirMagnet Policy Rule dialog box, select the newly created SSID group.
- 6) Click OK to close the AirMagnet Policy Rule dialog box.

Deleting an Existing SSID Group

Due to network update, some SSID groups may eventually become dated. As a result, you may want to remove those dated SSID groups off the SSID Groups table.

To delete an SSID group:

- 1) From the SSID Groups screen (Figure 5-18), highlight the SSID.
- 2) Click  (Delete Selected SSID Group).
- 3) Click OK.

Working with the Policy Wizard

The Policy Wizard provides an easy way for novice users to configure WLAN security and performance policies. It allows users to configure their WLAN policies based on their knowledge of their network settings. This utility offers an quick and easy start for first-time users unfamiliar with AirMagnet WiFi Analyzer's policy management mechanisms.

Configuring Policies with the Policy Wizard

The Policy Wizard walks you through the process using just a few easy-to-follow screens which cover the following areas:

- **Setting up SSID Groups** - This option asks you to organize the SSIDs on your wireless network into three SSID groups: MyWLAN, Neighbor, and Guest.
- **Setting up Authentication** - This option asks you to specify the authentication mechanisms that are used on your enterprise network. In this case, the system will automatically notify you when the selected authentication mechanisms are being violated.
- **Setting up Vendor Lists** - This option lets you associate policy configuration with the hardware devices used on your network. You specify the vendors for APs and stations in separate fields. In this way, the system can generate an alarm if any hardware device other than the ones you have specified are detected on your network.

For more information on network security and performance policies, refer to the AirMagnet WiFi Analyzer Policy Reference Guide on the CD.

To configure policies using the Policy Wizard:

- 1) From the AirMagnet Policy Management screen (Figure 5-2), click Policy Wizard. The Setup SSIDs screen appears. See Figure 5-19.

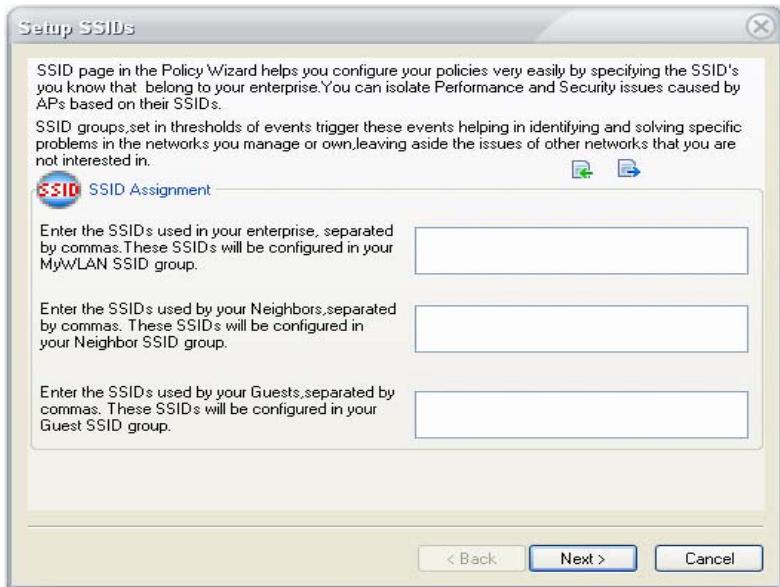


Figure 5-19: Configuring SSID groups

- 2) Enter the SSIDs in each group (i.e., your enterprise, neighbors, and guests), and click Next. The Setup Authentication Types screen appears. See Figure 5-20.

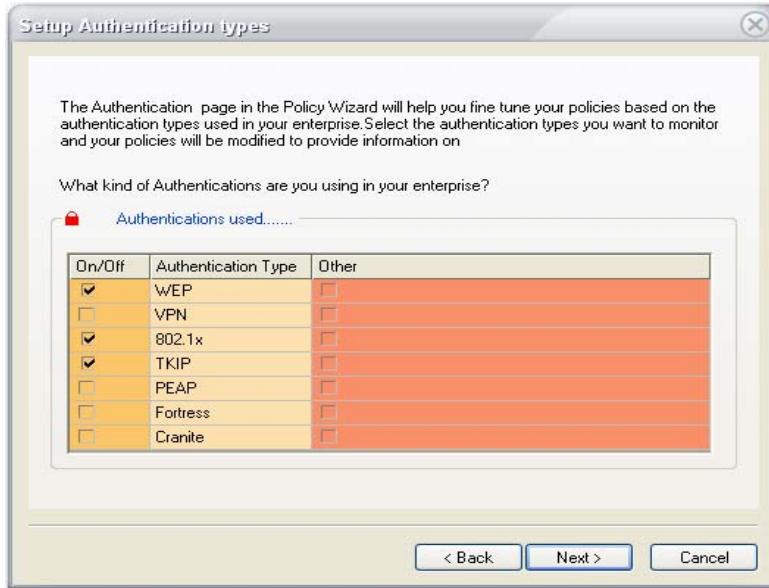


Figure 5-20: Specifying authentication mechanisms

- 3) Select the type(s) of authentication for your network, and your neighbor, guest and other networks; and click Next. The Setup Vendor Details screen appears. See Figure 5-21.

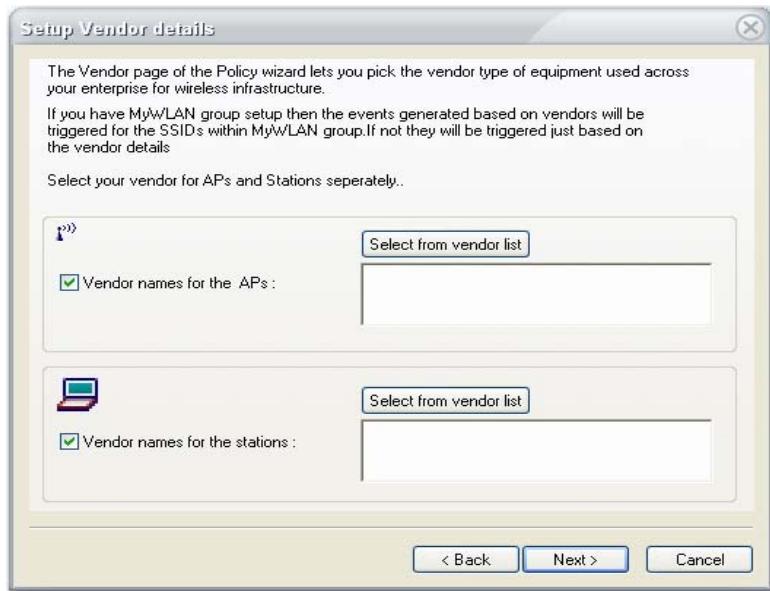


Figure 5-21: Specifying network device vendors

- 4) Check the Vendor Names for the APs check box, and click Select from Vendor List. The Vendor List screen appears. See Figure 5-22.

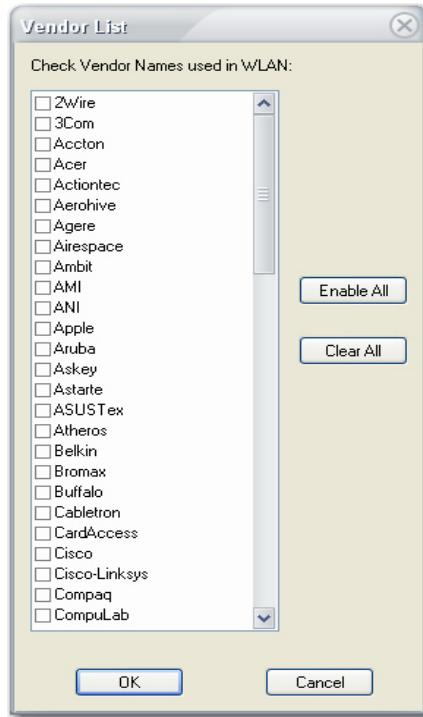


Figure 5-22: Selecting vendors

- 5) Select the AP vendors to be included in the policy profile and click OK.
- 6) Check the Vendor Names for the stations check box, and click Select from Vendor List. The Vendor List screen appears. Refer to Figure 5-22.
- 7) Select the station vendors to be included in the policy profile and click OK.
- 8) Then click Next. The Confirmation screen appears. See Figure 5-23.



Figure 5-23: Policy Wizard confirmation page

- 9) Click **Finish**.

Working with the Notification Wizard

Notifications are the ways AirMagnet WiFi Analyzer uses to notify the designated party when policy violations occur. The Notification Wizard is designed to help novice users to easily configure alarm notifications and apply them to network policies. Using a series of screens, the Notification Wizard can walk you through the key steps in notification configuration in no time, thus giving you a jump start in policy configuration.

Assigning Notifications to Policy Alarms

To assign notification to policy alarms:

- 1) From the AirMagnet Policy Management screen (Figure 5-2), click **Notification Wizard**. The Notification Selection Page appears. See Figure 5-24.

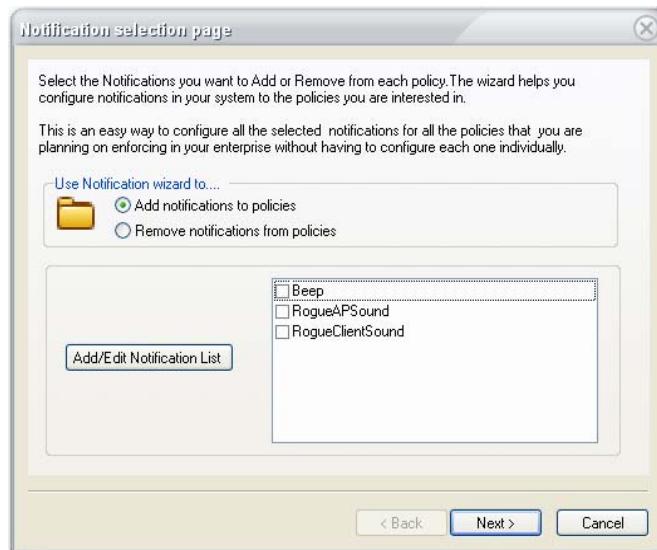


Figure 5-24: Selecting notification options

Figure 5-24 shows the default notification options that come with AirMagnet WiFi Analyzer. The user can add more notification options by using the **Add/Edit Notification List** button. See “[Adding Notification Options to an Alarm](#)” on page 227 for more information.

- 2) Select the **Add Notifications to Policies** radio button.
- 3) Select the notification(s) and click **Next**. The Policy Selection Page appears. See Figure 5-25.

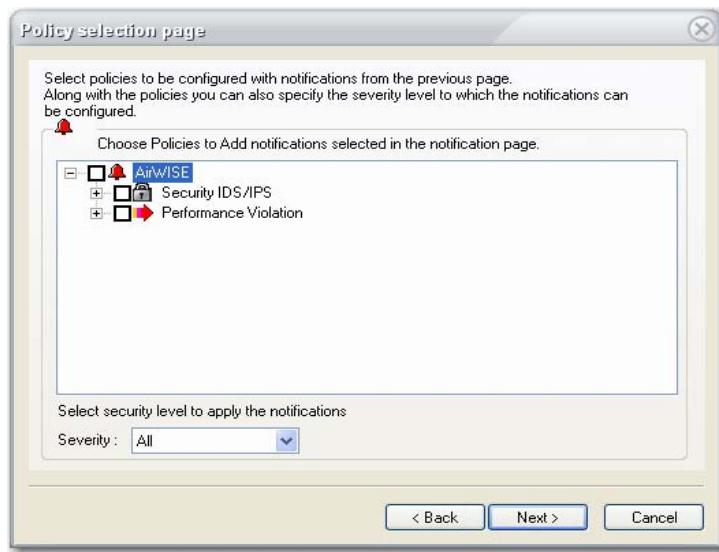


Figure 5-25: Selecting Policies

- 4) Select the policies and alarms to which the notifications are to be applied.
- 5) Select a level of severity and click **Next**. The Confirmation Page appears. See Figure 5-26.

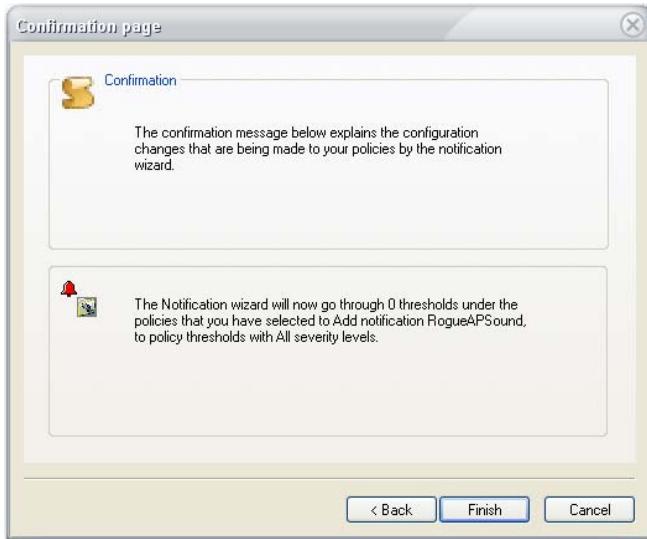


Figure 5-26: Notification Wizard confirmation page

- 6) Click **Finish**.

By default, each alarm contains only one notification. For most alarms, the default notification is a beep; for Rogue APs and clients, the default is a sound. The user can add, change, or delete notifications as needed.

Other Controls on Policy Management Screen

The *AirMagnet Policy Management* screen also provides the following control buttons:

- **Reset** - lets you restore the original policy settings set by the manufacturer.
- **OK** - confirms the policy setting you've just created or modified.
- **Cancel** - discards all the additions or changes you've made and return the system to the previously saved settings.

AirMagnet Policy Management Procedures

The following steps are suggested to illustrate how to expand the policy structure in the AirMagnet Policy Management screen:

- 1) Choose a policy group, e.g., Security vs. Performance.
- 2) Select policy category in that policy group, e.g., User Authentication and Encryption.
- 3) Select a subcategory of the selected policy category, e.g., WPA-802.1x &TKIP.
- 4) Highlight a specific alarm under the policy subcategory, e.g., 802.1x Rekey Timeout Too Long.

For detailed descriptions of AirMagnet WLAN policies, refer to the AirMagnet WiFi Analyzer Policy Reference Guide, which is included on the software CD.

Chapter 6: WLAN Management Tools

Chapter Summary

This chapter discusses the use of various advanced WLAN network management tools that come with AirMagnet WiFi Analyzer. The tools allow you to conduct the following WLAN management duties:

- Measuring 802.11n network efficiency
- Analyzing 802.11n network issues
- Simulating WLAN throughout
- Calculating device throughput
- Measuring WLAN or cell coverage
- Testing site RF signal distribution
- Conducting a site survey
- Performing WLAN diagnostics
- Troubleshooting link connection with Ping tool
- Tracing network device
- Conducting roaming tests
- Measuring WLAN performance with Iperf
- Measuring RF jitter
- Locating WLAN devices
- Measuring FTP upload and download performance
- Measuring HTTP upload and download performance
- Web Access Testing

802.11n Network Tools

AirMagnet WiFi Analyzer 9.0 comes with 802.11n tools that allow the user to analyze the performance of the 802.11n wireless network – the next generation of wireless networking technology that offers unprecedented network throughput, range, and stability. The tools are focused on helping the user to understand and troubleshoot the most common 802.11n-related issues they may encounter.

All these 802.11n Tools described in this section are available in AirMagnet WiFi Analyzer PRO only. They also require the use of an AirMagnet-supported 802.11n wireless network adapter or USB drive to operate.

AirMagnet WiFi Analyzer provides the following 802.11n-related tools:

- Efficiency
- Analysis
- WLAN Throughput Simulator
- Device Throughput Calculator

802.11n Efficiency

The 802.11n wireless network protocol introduces substantial enhancements in WLAN efficiency at both the physical (PHY) and the medium access control (MAC) layers. The Efficiency tool is intended to provide the basic knowledge that the user needs in order to take full advantage of the benefits of the 802.11n network.

The Efficiency tool allows you to see the network efficiency between any (chosen) pair of AP and STA, or AP alone. The Efficiency tool screen displays 802.11n issues in the following categories:

- **PHY** – covers the issues related to improved data throughput at the physical layer.

- **MAC** – covers issues related to protocol efficiency improvements at the Medium Access Control layer such as frame aggregation and block acknowledgements.
- **Coexistence** – covers issues related to 802.11n network's backward compatibility with legacy 802.11 networks (i.e., 802.11a/b/g).

To analyze the network efficiency between an AP and a STA:

- 1) From the navigation bar, click  . The WiFi Tools screen opens.

By default, the 802.11n Tools>Efficiency screen when the WiFi Tools screen opens. If you are on another WiFi Tools screen, you can navigate to the Efficiency screen simply by clicking Efficiency. See Figure 6-1.

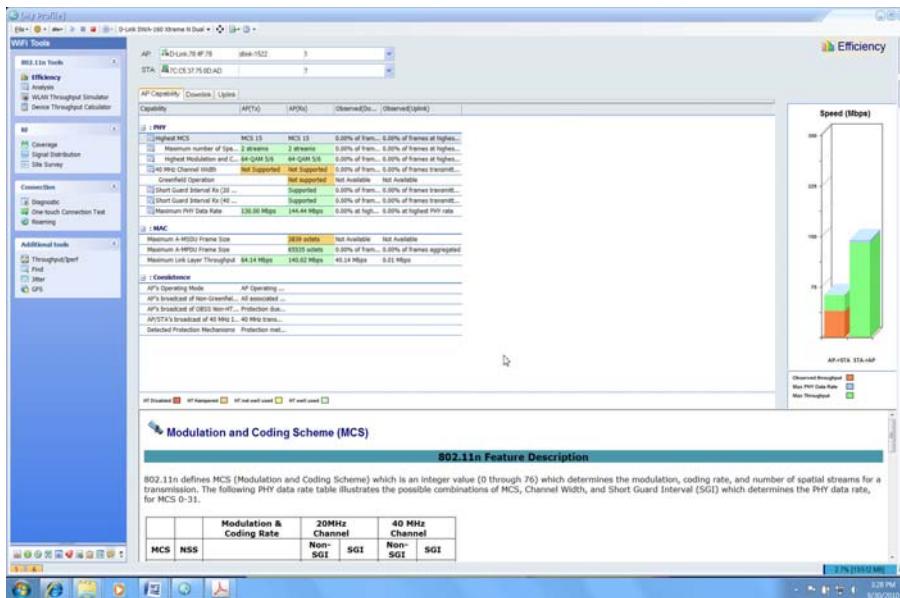


Figure 6-1: Analyzing 802.11n network efficiency

- 2) From the Efficiency screen, select an AP and a STA.

The STA marked in bold green in the STA list is the one that is associated with the AP selected from the AP list above.

- 3) Use the tabs on the upper part of the screen to view the various data regarding the network efficiency between the AP and the STA, as described in Table 6-1.

Table 6-1: 802.11n Efficiency Tool Parameters

Parameter	Description
Tab	<p>Click any of the following tabs to view the pertinent data in the table.</p> <ul style="list-style-type: none">• AP Capability—Shows the maximum theoretical capability that an AP could reach if associating with a hypothetical “golden” STA that supports all 802.11n features.• Downlink—Displays data about the link from the selected AP to the selected STA.• Uplink—Displays data about the link from the selected STA to the selected AP.

Table Fields

Table 6-1: 802.11n Efficiency Tool Parameters

Parameter	Description
	<ul style="list-style-type: none">• Capability—Lists major features that an 802.11n device is capable of.• AP (TX)—The transmit capabilities of the AP.• AP (Rx)—The receive capabilities of the AP.• AP->STA—The downlink capabilities (from the AP to the STA).• STA->AP—The uplink capabilities (from the STA to the AP).• Observed (Downlink)—The level or state of a certain capability as observed from the downlink (i.e., from the AP to the STA).• Observed (Uplink)—The level or state of a certain capability as observed from the uplink (i.e., from the STA to the AP).
Color Legends	
<ul style="list-style-type: none">• HT Disabled (Red)—High Throughput feature disabled or not used.• HT Hampered—High Throughput feature is impaired.• HT Not Well Used—High Throughput feature is used for only 50~75%.• HT Well Used—High Throughput is used almost to its full potential.	

- 4) Observe the various data rates for both the downlink (AP->STA) on the left and the uplink (STA->AP) on the right in the bar chart, as described in Table 6-2.

Table 6-2: 802.11n Efficiency Bar Chart

Screen Data	Description
Bar Chart	Left Chart —Shows downlink (AP->STA) data rate. Right Chart —Shows uplink (STA->AP) data rate.
Color Legend	<ul style="list-style-type: none"> • Light green—Represents Maximum throughput. • Light blue—Represents Maximum PHY Data Rate • Brown—Represents Observed Throughput.

Note: The Observed (Downlink) and Observed (Uplink) columns in Table 6-1 show any of the following depending on the situation:

- When an AP-STA pair which is known to be associated by AirMagnet WiFi Analyzer, the Observed column contains metrics which are specific to the AP-STA association (i.e., only displays traffic measurements made between the combination of the AP and STA).
- When an AP-STA pair is not known to be associated, the Observed column contains metrics which are independent of any association (i.e., all outgoing [data] traffic metrics from the AP and STA are displayed).
- When an AP and “any” STA are selected, the APs outgoing (data) traffic metrics are used and the STA (and subsequently Uplink) metrics are zero (i.e., no traffic is indicated). In this case, the AP’s capability is compared against a “virtual” STA, which has parameters defined at the limit of the 802.11n specification.

802.11n Analysis

The Analysis screen provides detailed analysis (explanation) about a number of 802.11n-related issues. You can navigate to the Analysis tool screen by clicking Analysis under 802.11n Tools.

The Analysis tool allows you to see the following 802.11n network data between any (chosen) pair of AP and STA, or AP alone:

- 20/40 MHz Statistics
- Short Guard Interval (SGI)
- A-MPDU
- MCS
- PHY Data Rate

To analyze 802.11n data on your WLAN:

- 1) From the WiFi Tools screen, click Analysis in the 802.11n Tools section. See [Figure 6-2](#).

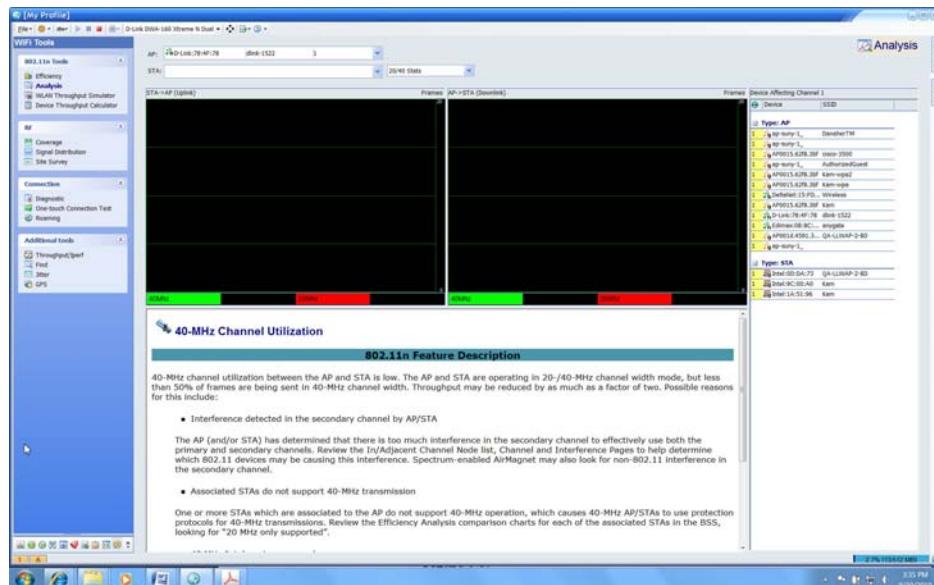


Figure 6-2: Analyzing 802.11n data

- 2) From the top of the screen, select a AP and station, as shown in [Figure 6-3](#).

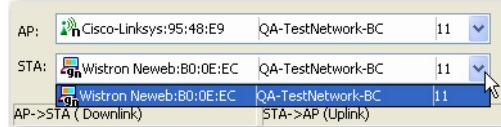


Figure 6-3: Selecting an AP

- 3) Select a data type of interest, as shown in [Figure 6-4](#).

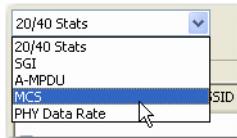


Figure 6-4: Selecting a station

- 4) Use the bar charts to observe the downlink (AP->STA) and uplink (STA->AP).
- 5) Read the description in the lower-middle part of the screen.
- 6) From the right-hand side of the screen, look through the list of devices that are affecting the selected channel.

Simulating WLAN Throughput

The WLAN Throughput Simulator is a utility for calculating network, node and media throughput, utilization and overhead (as measured at the 802.11 Link Layer) under various network and node configurations. It allows the user to add and configure up to fifty 802.11a, 802.11b, 802.11g and/or 802.11n nodes on a “virtual channel”. The Simulator’s engine applies additional network and node parameters based upon the type and settings of the nodes present. The Simulator runs in a “perfect” environment, assuming that all nodes can “hear” each other (negating the possibility of packet collisions and frame retries) and that all nodes transmit as much (and as fast) as they possibly can (based upon their individual and overall network parameters). The result of such simulation provides a baseline measurement of the (somewhat theoretical) maximum link-layer throughput that can be achieved for a particular configuration.

Configuring WLAN Throughput Simulator

Before using the WLAN Throughput Simulator, you may want to configure it in a way so that the tool can best simulate the WLAN throughput you desire.

To configure the WLAN Throughput Simulator:

- 1) From the WLAN Throughput Simulator screen, click  and select **Configure Simulator...** from the drop-down menu. The Simulator Configuration dialog box appears. See Figure 6-5.

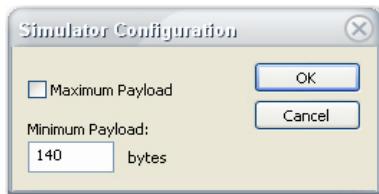


Figure 6-5: Configuring WLAN Simulator

- 2) Check the **Maximum Payload** check box or specify a minimum packet size.

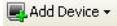
If the Maximum Payload check box is checked, the Simulator will simulate the condition in which all nodes will transmit the maximum packet size possible. Otherwise, the WLAN Throughput Simulator will simulate WLAN throughput using a payload value between the specified Minimum Payload and the Maximum Payload, which varies depending on the 802.11 protocol used on the devices. According to the IEEE 802.11n Specifications, the maximum payload that can be transmitted is up to 2.3 Kb for 802.11a/b/g devices and 65 Kb for 802.11n devices if MPDU is enabled.

- 3) Click OK.

Conducting WLAN Throughput Simulations

The WLAN Throughput Simulator allows the user to simulate WLAN throughput under user-specified conditions. All you have to do is to select the APs and STAs, set the parameters, and then click **Simulate**. AirMagnet WiFi Analyzer will generate the results and display them on the screen.

To simulate your WLAN throughput:

- 1) From the 802.11n Tools screen, click WLAN Throughput Simulator.
- 2) Select the appropriate frequency band by clicking the 2.4 GHz or 5 GHz radio button.
- 3) From the menubar, click  and select an option from the drop-down menu.

Depending on the frequency band being used, the options in the Add Device drop-down list may vary slightly. Table 6-3 describes all possible options.

Table 6-3: Adding Device Drop-Down Menu Options

Menu Option	Description
Add Existing Device	Opens a dialog box that allows you to select and add APs and/or STAs from a list of devices detected on the WLAN.
802.11a Device	Adds 802.11a APs and/or STAs.
802.11b Device	Adds 802.11b APs and/or STAs.
802.11g Device	Adds 802.11g APs and/or STAs.
802.11n Device	Adds 802.11n APs and/or STAs.

- 4) Associate STAs with APs by clicking an STA and then the down arrow next to it to select an AP to associate with, as shown in Figure 6-6.

Device to simulate						
Device	Associated AP	R..	T...	T...	Th...	Status
AP_1		1..	0	0	0.00	Idle
STA_1	AP_1	1..	0	0	0.00	Idle
AP_2		5..	0	0	0.00	Idle
STA_2	Associate...	0	0	0	0.00	Idle

Figure 6-6: Associating station with AP

- 5) Repeat Step 3 to make sure that all APs and STAs are associated.

Note that every STA needs to be associated with an AP in order to run WLAN throughput simulation.

- 6) Click the Run button in the upper-right corner of the screen. The simulation starts and the results are shown on the screen. See Figure 6-7.

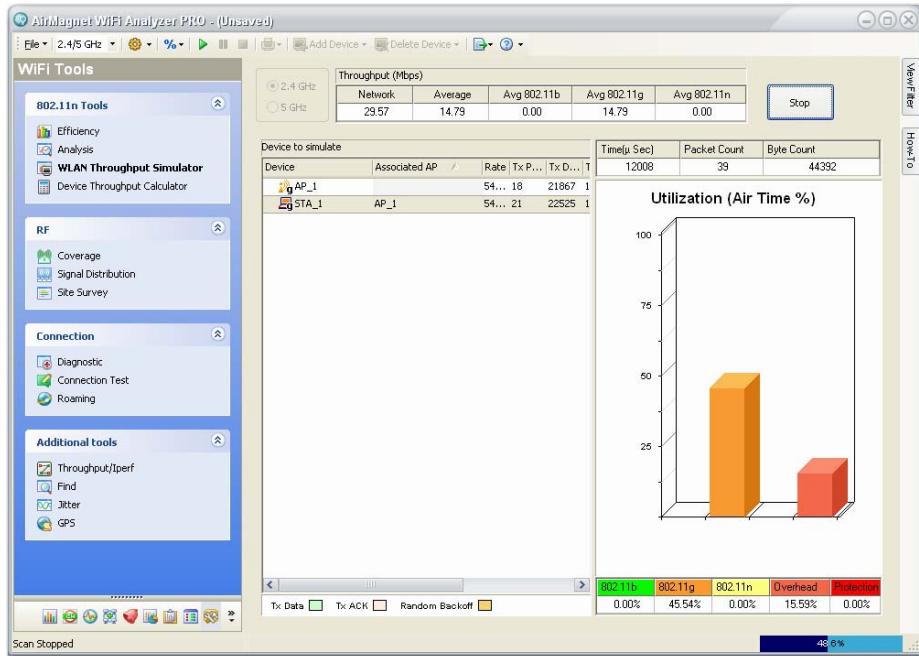


Figure 6-7: Simulated WLAN Throughput

Simulated WLAN Throughput

The table below explains the simulated WLAN data as shown on the WLAN Throughput Simulator screen.

Table 6-4: WLAN Throughput Simulator Screen Data

Data Field	Description
Throughput (Mbps)	Shows WLAN throughput in Mbps in the following categories: <ul style="list-style-type: none">• Network—The network throughput which is the combined, aggregate throughput of the wireless all media (which may include 802.11a/b/g/n, depending on the frequency band selected, i.e., 2.4 GHz vs. 5 GHz).• Average—The average node throughput (which the network throughput divided by the number of nodes).• Avg 802.11a—The average node throughput for all 802.11a devices. (5 GHz only).• Avg 802.11b—The average node throughput for all 802.11b devices.• Avg 802.11g—The average node throughput for all 802.11g devices.• Avg 802.11n—The average node throughput for all 802.11n devices.

Table 6-4: WLAN Throughput Simulator Screen Data

Data Field	Description
Device to Simulate	<p>Shows information about each of the devices involved in the simulation:</p> <ul style="list-style-type: none"> • Device – The name or MAC address of the node. • Associated AP – The name of APs associated with a station or stations. • Rate – The PHY Data Rate used by the node for all DATA transmissions. • Tx Packets – The number of DATA frames (packets) sent from the node. • Tx Data Bytes – The number of DATA bytes sent from the node. • Throughput – The throughput of individual nodes. • Status – The current operating state of the nodes which can be TX Data, Tx ACK, Random Backoff, and Virtual Carrier Sense. • Time (μsec) – The simulation time (in μsec). <p><i>Note: The simulation engine runs at 1/1000th time scale, which means that every second of "real-time" represents one millisecond of "simulation time".</i></p> <ul style="list-style-type: none"> • Packet Count – The number of packets sent over the channel. • Byte Count – The number of bytes sent over the channel.

Calculating Device Throughput

The Device Throughput Calculator is a utility for calculating a device's theoretical throughputs. The user simply clicks to specify the parameters such as MCS index, SGI, bandwidth, max frame size, block ACK, least capable device, and/or protection mechanism used, and AirMagnet will calculate the maximum PHY rate, maximum data rate, percentage of overhead, the number of spatial frames, and the modulation coding rate in a flick of second. It also displays 802.11 frame exchange data in a graph which showing the percentage of DIFS, preamble/PLCP, Data, SIFS, preamble/PLCP, and ACK frames.

The Device Throughput Calculator allows the user to calculate the maximum throughput level of a device based on user-specified parameters and coexistence conditions. The results of all calculations can be retained on the screen. They can serve as a quick reference as to the level of performance a device can achieve in various conditions.

To calculate device throughput:

- 1) From the WiFi Tools screen, click Device Throughput Calculator. The Device Throughput Calculator screen appears. See Figure 6-8.

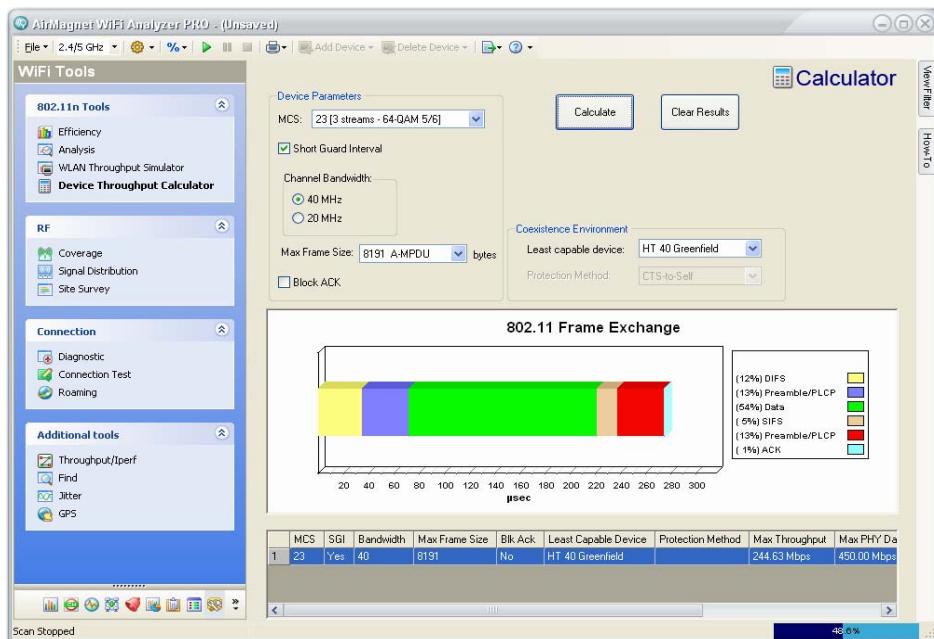


Figure 6-8: Calculating Device Throughput

- 2) On the Device Throughput Calculator screen, make the selections as described in the Table 6-5.

Table 6-5: Device Throughput Calculator Parameters

Parameter	Description
MCS	Click the down arrow and select an option from the drop-down list. <i>Note:</i> Each Modulation and Coding Scheme (MCS) is associated with a specific number of spatial streams and a modulation and coding rate, as indicated by the values within the brackets.
Short Guard Interval	If checked, Short Guard Interval (SGI) is enabled. <i>Note:</i> When SGI is enabled, PHY data rate (in Mbps) is increased by roughly 11% for each Modulation and Coding Scheme (MCS) on both the 20- and 40-MHz channels.
Channel Bandwidth	Select either of: <ul style="list-style-type: none">• 40 MHz• 20 MHz
Max Frame Size	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none">• 3839 A-MSDU• 7935 A-MSDU• 8191 A-MPDU• 16383 A-MPDU• 32767 A-MPDU• 65535 A-MPDU
Block ACK	If checked, Block Acknowledgement is enabled.

Table 6-5: Device Throughput Calculator Parameters

Parameter	Description
Least Capable Device	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none">• HT 40 Green Field• HT 40 Mixed Mode• HT 20 Green Field• HT 20 Mixed Mode• 802.11g• 802.11b• 802.11a
Protection Method	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none">• CTS-to-Self• RTS/CTS• L-SGI TXOP <p><i>Note:</i> None of these protection methods applies to HT 40 Greenfield.</p>

- 3) Click the Calculate button. AirMagnet WiFi Analyzer starts to calculate the device throughput based on the parameters you have specified, displaying the result on the screen.
- 4) Repeat Steps 2 through 3 to make more calculations using different combinations of the parameters.

AirMagnet WiFi Analyzer generates a calculation result at each click of the Calculate button. All results will be shown on the screen, making it easy to compare the device's throughputs under various conditions.

Figure 6-9 shows a Device Throughput screen with calculation results.

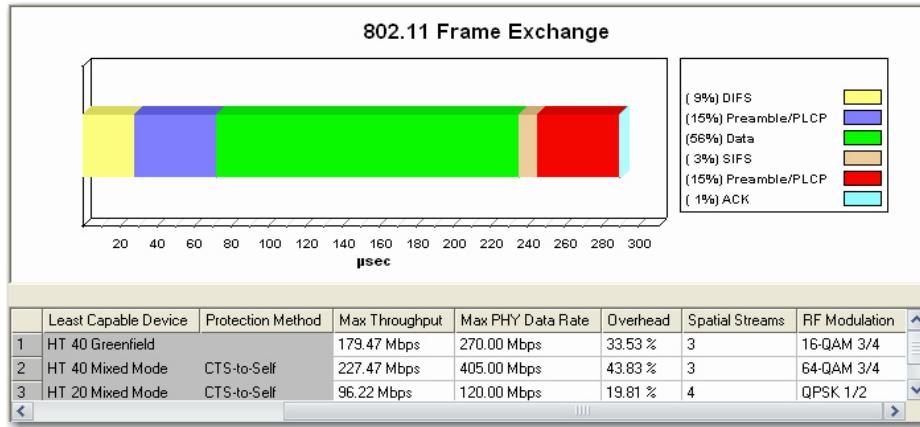


Figure 6-9: Device throughput calculation results

Analyzing WLAN RF Conditions

AirMagnet WiFi Analyzer provides RF tools that assist network administrators to learn and understand the RF conditions on or around their WLAN site. The real-life RF data obtained through these tools help them make well-informed decisions regarding their WLAN deployment and enhancement.

AirMagnet WiFi Analyzer provides the following RF tools:

- Coverage – Measures WLAN site or cell RF signal coverage.
- Signal Distribution – Analyzes the pattern of RF signal distribution.
- Site Survey – Collects RF data on a WLAN site.

Signal Coverage Tool

The Coverage tool is designed to provide an overview of RF signal coverage on a wireless network. It can assist in the analysis of either pre- or post-installation networks.

While analyzing the network RF environment, you will be able to view the signal coverage by roaming over the cell boundaries. In so doing, you will get a log file which contains valuable data that can be used as the basis to adjust the RF cell size to ensure that the required coverage is being provided.

Configuring Signal Coverage Tool Settings

You may want to set up some parameters before you actually start a signal coverage test. This will ensure that you'll get the data you want.

To configure signal coverage tool settings:

- 1) From the WiFi Tools screen, click the Coverage button. The WiFi Tools>Coverage screen appears. See [Figure 6-10](#).

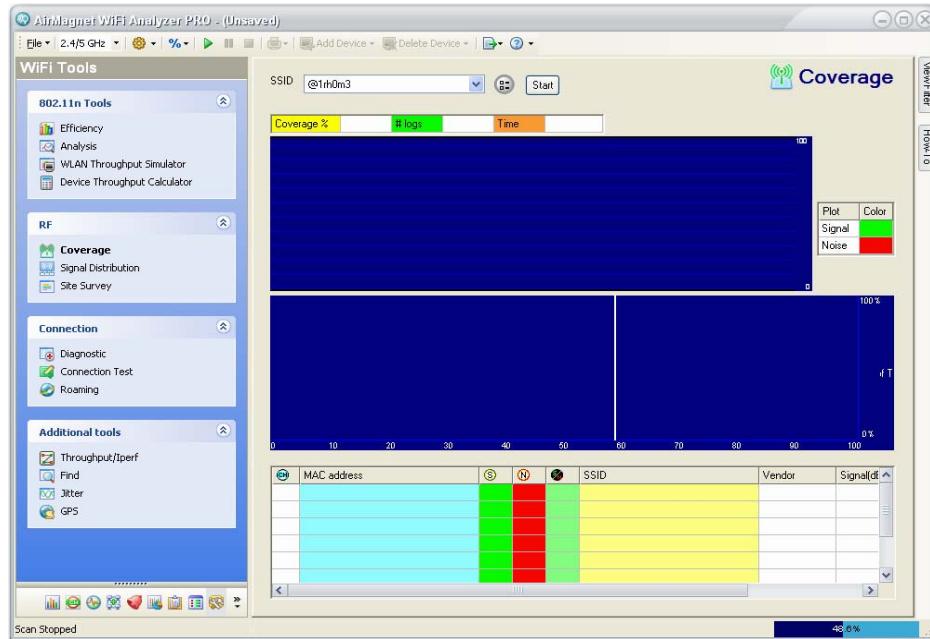


Figure 6-10: Signal Coverage tool screen

- 2) Click (Configure). The Coverage Configuration screen appears. See [Figure 6-11](#).

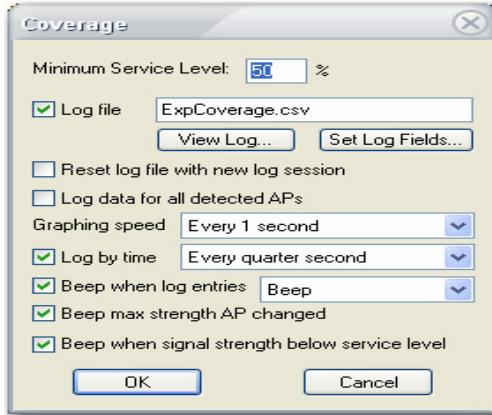


Figure 6-11: Configuring Signal Coverage tool

- 3) Make the desired selections and click OK.

Measuring Site RF Signal Coverage

To measure WLAN site RF signal coverage:

- 1) From the WiFi Tools>Coverage screen (Figure 6-11), select an SSID from the drop-down list.
- 2) Click **Start** (Start). Data will start to appear on the screen. See Figure 6-12.

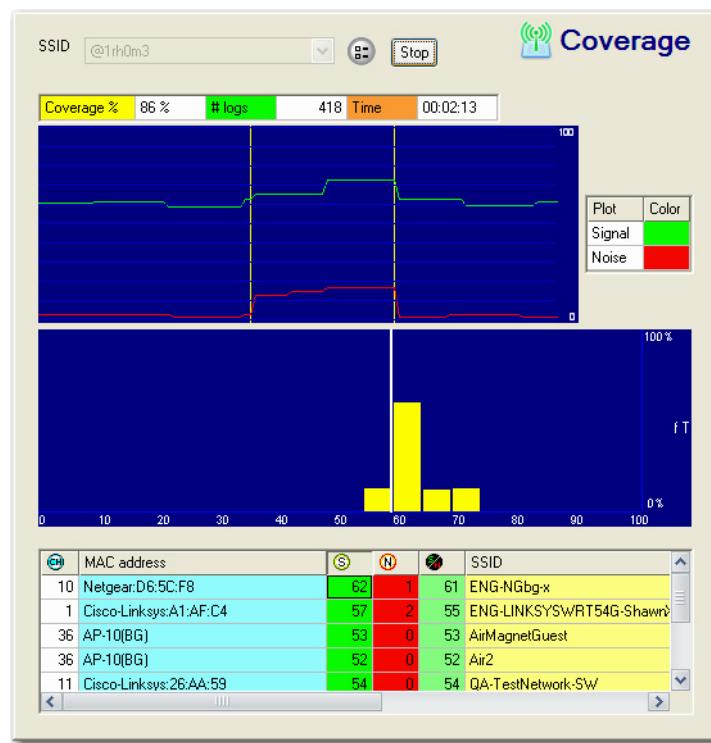


Figure 6-12: Measuring signal coverage

- 3) Click **Stop** to end the coverage test.

The Coverage tool screen provides a complete picture of the RF signal coverage for the selected SSID. The tool also shows the amount of traffic that is above the specified Minimum Service Level which is represented by the white vertical line in the bar graph. The bars to the right of the white line represent APs whose signal strengths meet or exceed the Minimum Service Level and those to the left of the white line represent APs whose signal strengths are below the Minimum Service Level. The figure above shows that 86% of the SSID is adequately covered when the Minimum Service Level is set to 60%.

If you have three APs set up to cover your facility, you can simply take AirMagnet WiFi Analyzer and roam through the coverage area. Then by viewing the signal levels of all the APs, you can either adjust the APs' transmission power or relocate the APs to provide adequate or optimized RF signal coverage.

Signal Distribution Tool

The Signal Distribution tool is designed to detect RF signal problems such as signal multipath. It provides the user with an easy way to monitor WLAN RF signal distribution patterns and to visualize issues that would otherwise be difficult to see and analyze.

Configuring Signal Distribution Tool Settings

To configure the Signal Distribution tool settings:

- 1) From the AirMagnet Tools screen, click the **Signal Distribution** button. The Signal Distribution screen appears. See [Figure 6-13](#).

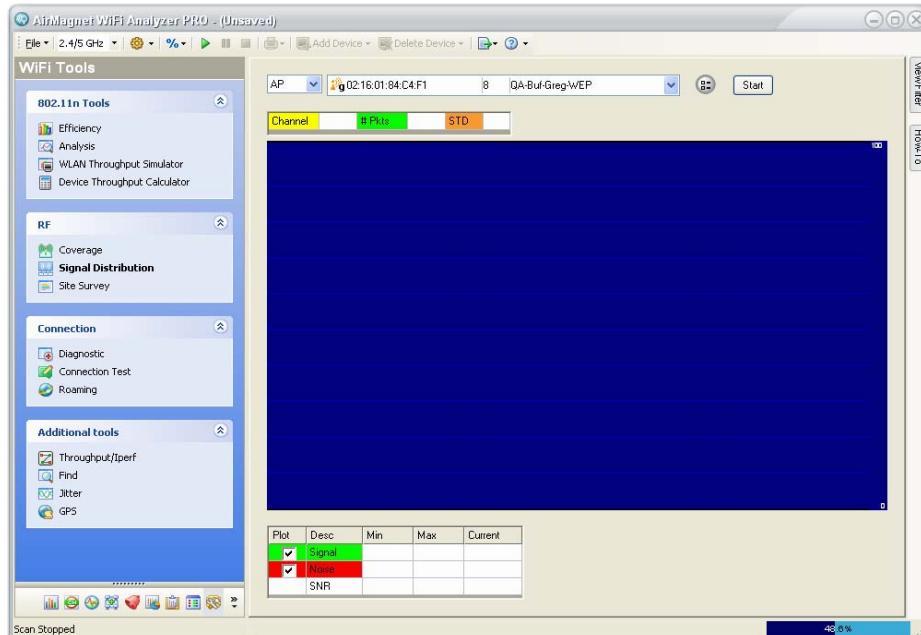


Figure 6-13: Signal Distribution tool screen

- 2) From the WiFi Tools>Signal Distribution screen, click  (Logging Options). The Signal Distribution Option dialog box appears. See Figure 6-14.

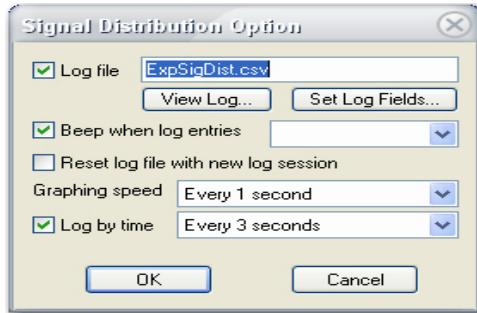


Figure 6-14: Configuring Signal Distribution tool

- 3) Make the desired selections and click OK.

Conducting a Signal Distribution Test

To conduct a signal distribution test:

- 1) From the WiFi Tools>Signal Dist screen, select AP or STA and then select a specific AP or STA on the right.
- 2) Click  (Start). Signal distribution data start to appear on the screen. See Figure 6-15.

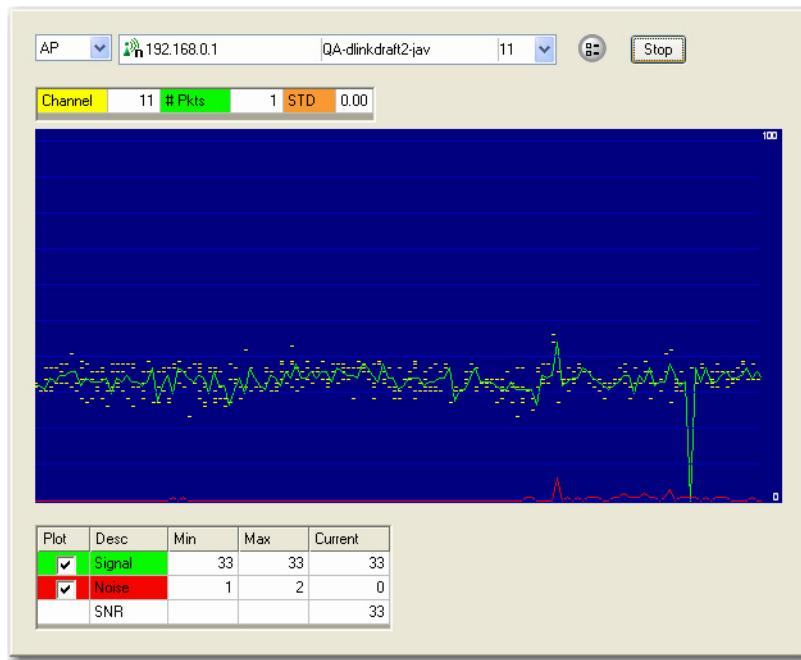


Figure 6-15: Measuring signal distribution

- 3) Click **Stop** to end the test.

The cluster of yellow dots shown in the figure above represents the RF signal per packet being seen from the current location. In case of good signal distribution, the dots should be all close together within a narrow range. It means that the site RF signals are consistent in strength with little variation. On the other hand, if the dots are scattered all over the screen, it means the signal strength is varying and you may be having a problem that warrants your attention.

Site Survey Tool

A site survey is an in-depth inspection and analysis of RF conditions on a proposed or existing WLAN site. The primary objective of a site survey is to ensure that wireless stations receive good radio signals and transmission throughput rate in the area where they operate and

determine the number of access points needed to cover the area and the optimal locations to place them. A thorough site survey helps ensure that the design and deployment of the WLAN meet the RF signal coverage and network bandwidth requirements. The Site Survey tool enables you to conduct WLAN site surveys to evaluate the RF quality of the site in terms of signal strength, noise level, speed, etc. directly from within AirMagnet WiFi Analyzer.

AirMagnet WiFi Analyzer's built-in Site Survey utility complements the site survey program that comes with the WLAN products you purchased from your WLAN vendor. Consult your manufacturer's site survey guide, supplied as part of your WLAN equipment, for complete requirements and procedures for a WLAN site survey.

Before you start gathering data of your site survey project, you must obtain a blueprint or a CAD drawing of the building or office layout. You should also determine the location where you wish to take survey data with simple identifications; for example, Location 1, Location 2, etc.

Configuring Site Survey Tool

To configure Site Survey tool options:

- 1) From the WiFi Tools screen, click the Site Survey tool. The WiFi Tools>Site Survey screen appears. See Figure 6-16.

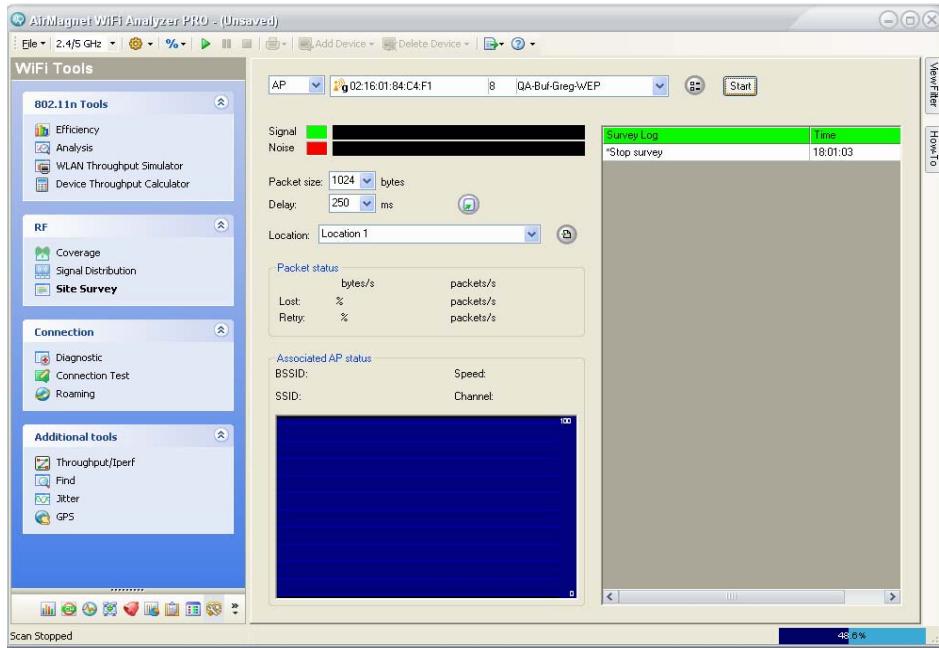


Figure 6-16: The default Survey tool screen

- 2) Click (Logging Options) to display the Survey Log Options screen. See Figure 6-17.

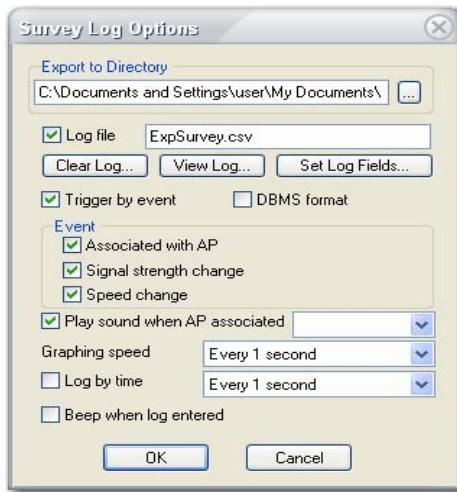


Figure 6-17: Configuring survey log settings

- 3) Specify a path for exporting the survey file.
- 4) Name the file in a way that is unique to the location of the survey.
- 5) Uncheck Trigger by event.
- 6) Make the other selections as you desire.
- 7) Click OK.

Conducting WLAN Site Survey

To conduct a WLAN site survey:

- 1) Walk to Location 1 as you have planned with your laptop PC (with AirMagnet WiFi Analyzer running on it).
- 2) From the WiFi Tools>Site Survey screen (Figure 6-16), select AP or SSID from the filter on the left and then choose a specific AP or SSID from the drop-down list on the right.
- 3) Click **Start** (Start). RF signal and noise data start to appear on the graph screen as they are captured. Data packets are displayed in the Survey Log pane on the right. See Figure 6-18.

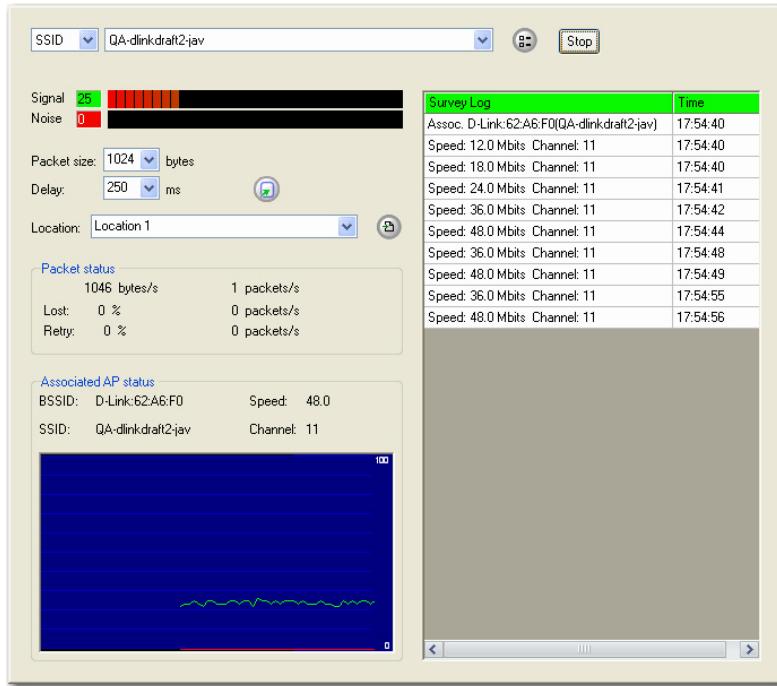


Figure 6-18: Starting an RF data survey

- 4) Click (Stop) to stop the survey.
- 5) Walk to Location 2, repeat Steps 1 through 4.
- 6) Follow the same procedures to collect data at other locations.

Upon completion of the survey, you can use a third-party software, such as Excel or Visio, to tabulate or plot the RF signal coverage.

Configuring Roaming Controls

The (Roaming Option . . .) button to the right of the Packet Size and Delay fields of the survey window allows you to control your computer's roaming status. It allows you to define when your computer will roam, based on several different values.

To set roaming options on AirMagnet WiFi Analyzer:

- 1) From the WiFi Tools>Site Survey screen, click . The Set Roaming Criteria dialog box opens. See [Figure 6-19](#).

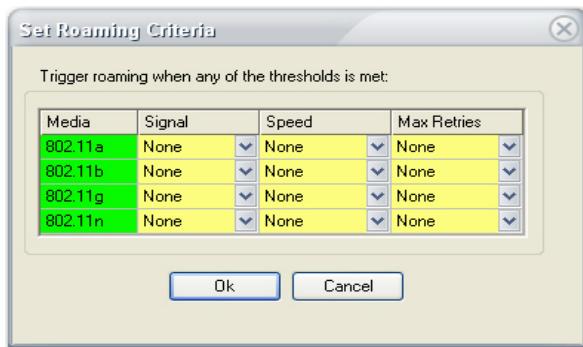


Figure 6-19: Roaming Control Settings

- 2) Click the down arrows to adjust the Signal, Speed, and Max Retries values for the 802.11 protocols on your laptop computer when it enters roaming state.

Roaming starts when any of these values is met. Configuring roaming based on signal strength will cause your computer to roam once it reaches a specific minimum signal strength, whereas configuring roaming based on speed will cause it to roam once a minimum transmission speed is met. Max retries refers to the number of times the computer has to re-send lost data to the AP.

The content of the Set Roaming Criteria dialog box varies depending on the media band (2.4 GHz vs. 5 GHz) being used. When 2.4 GHz band is selected, then the 802.11a row will be greyed out (inapplicable); when the 5 GHz band is used, 802.11b and 802.11g will be greyed out.

The roaming control option will only work with the following wireless network adapters:

- 3Com 802.11 a/b/g Wireless PC card (3CRPAG175 and 3CRPAG175B)
- AirMagnet Trio 802.11 a/b/g wireless adapter (NL-5354CB ARIES), Wireless cardbus adapter Super A/G (NL-5354CB PLUS Aries2 and NL-5354 B PLUS Aries2-F), AirMagnet 802.11a/b/g Wireless LAN Mini PCI Adapter, and AirMagnet 802.11a/b/g/n Wireless PC Card
- Buffalo AirStation WLI-CB-AMG54 wireless adapter (For Japan only)
- Cisco 802.11 a/b/g Wireless Adapter AIR-CB21AG
- Enterasys a/b/g RoamAbout CB-500AG
- LANCOM Systems Airlancer 54-ag
- Linksys Wireless A+G Notebook Adapter WPC55AG ver 1.2
- Netgear WAG511 802.11 a/b/g wireless adapter, WAG511v2 802.11 a/b/g, and WG511U Double 108 Mbps wireless adapter
- Nortel Networks 802.11 a/b/g wireless adapter 2202
- Proxim ORiNOCO 802.11 a/b/g ComboCard Gold (8480-XX) and ORiNOCO 802.11 b/g PC Card Gold (8470-XX)
- TRENDnet 802.11 a/g Wireless CardBus PC Card (TEW 501 PC)
- Ubiquiti SRC 802.11 a/b/g MMCX adapter

WLAN Connection Tools

AirMagnet WiFi Analyzer offers tools for analyzing connections between network nodes and/or devices. They enable network administrator to effectively troubleshoot and resolve network connection issues.

The following are the connection tools:

- Diagnostic – Identifies mismatched configurations, such as SSIDs, WEP keys, transmission rates, preamble, or RF channels.

- One-Touch Connection Test – Troubleshoots and pinpoints the root cause to any network connectivity issue.
- Roaming – Troubleshoots VoWLAN roaming issues that may cause dropped calls.

Diagnosing Network Connectivity Issues

Without intelligent tools, the process of troubleshooting a problem connection between a client station and an AP can be an incredible drain on professional resources. The AirMagnet Diagnostic tool identifies mismatched configurations, such as SSIDs, WEP keys, transmission rates, preamble, or RF channels. It also helps isolate the problem to the specific step in the association process where the connection is failing. These steps include probe discovery, authentication, re-association, and potential hardware failures.

To diagnose a station connection problem:

- 1) Locate the station's MAC address from the client configuration utility program, or from the back of the 802.11 WLAN card.
- 2) Keep the client station running.
- 3) Place the laptop PC (with AirMagnet WiFi Analyzer running on it) next to the station.
- 4) From the WiFi Tools screen, click the Diagnostic tool. The Tools>Diagnostic screen appears. See [Figure 6-20](#).

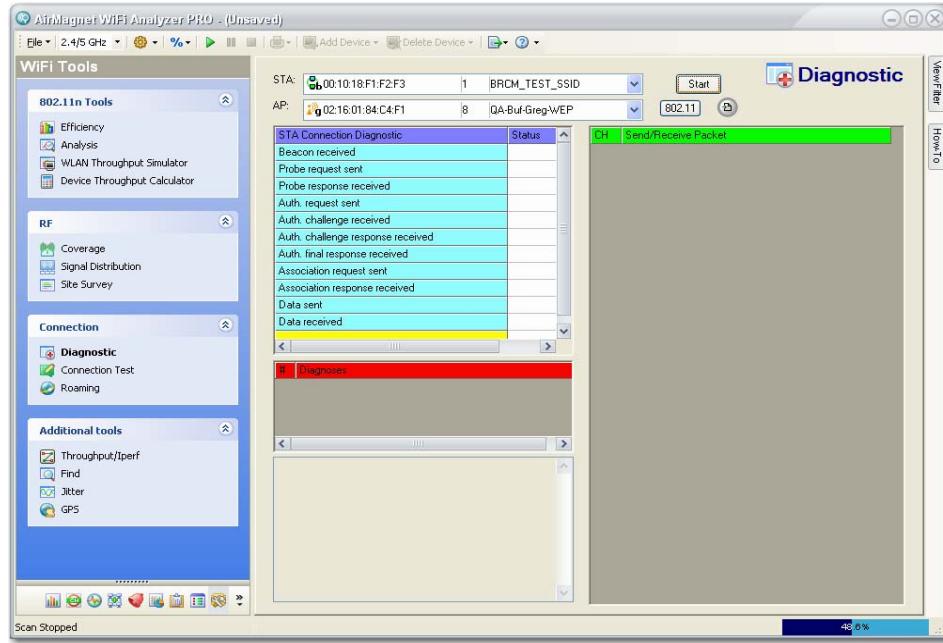


Figure 6-20: Diagnosing Network Connection

- 5) For STA, select the client station MAC address from the STA drop-down list.
- 6) For AP, select the AP that the client is supposed to connect with from the AP drop-down list.

You may select ANY if you are not sure which AP to use, but the accuracy of the diagnosis will be reduced.

- 7) Click **Start** (Start). The Diagnostic tool screen shows the progress in the association process with the AP. See Figure 6-20.

The diagnostic test automatically ends once it is 100% completed. However, if you want to stop a diagnostic test that is still in progress, simply click .

- 8) Look in the middle- and lower-left parts of the screen for diagnostic results (which suggest the likely causes of the connection and association problems).
- 9) Look in the right part of the screen for step-by-step log.
- 10) Click  to display 802.1x information.
- 11) Click  (Export) to export the log data.

One-touch Connection Test Tools

WLAN connectivity problems can stem from 802.11 data link layer malfunction or IP network layer misconfiguration. In order to troubleshoot and pinpoint the root cause to any connectivity issue, the interaction between the two networking layers must be investigated. AirMagnet WiFi Analyzer One-touch Connection Test tools allow the user to easily conduct a number of end-to-end connectivity tests from the same one user interface.

AirMagnet WiFi Analyzer provides the following uniquely integrated active tools to address these anomalies:

- Ping
- Trace
- FTP
- HTTP

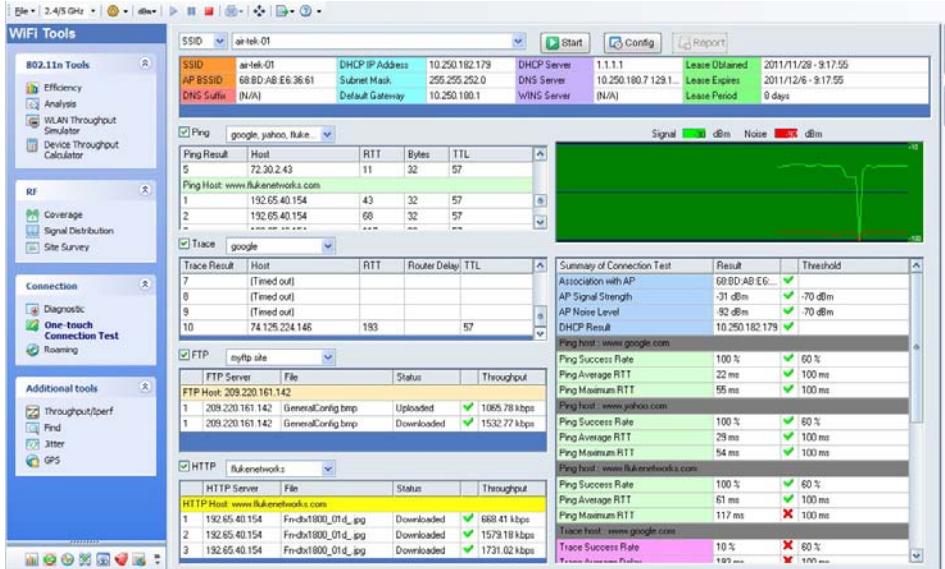


Figure 6-21: One-touch Connection Test Completed

Configuration

Tests inside the One-Touch Connection Test tool can be configured by selecting “Config” at the top of the screen, next to the Start button. See Figure 6-22.

Generate Report

Select Report Tab in Config and check the “Create One-Touch Connection Test Report”. Once the One-Touch Connection Test is started, the application will scan channels to gather information on the WiFi network. Once the test is complete, the user will be able to view the report by selecting the Report button.

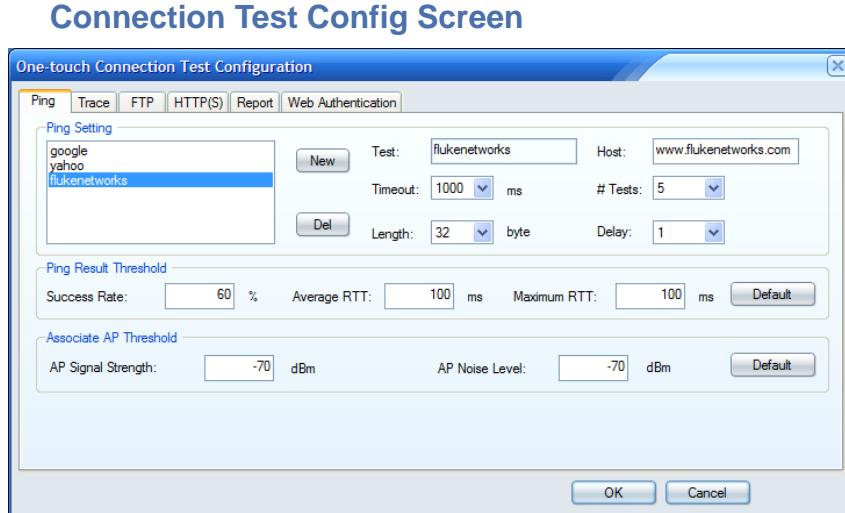


Figure 6-22: Connection Test Config screen

Multiple Destinations

For each of the following tests, multiple destinations may be run during the test. First, when configuring a test, add multiple destinations as shown in [Figure 6-22](#). Then, when using the dropdown to select destinations, check the destinations to run during the test. See [Figure 6-23](#).

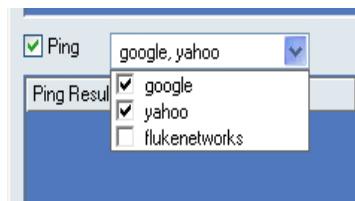


Figure 6-23: Multiple Destinations

Using the Ping Tool

After the proper association to the desired AP has been confirmed, the next step is to verify the DHCP acquisition of IP addresses for client service, default gateway, and DNS server using the Ping tool.

Verifying the DHCP Acquisition of IP Address

To verify DHCP acquisition of IP addresses:

- 1) Check the Ping check box.
- 2) Use the drop-down menu provided to select one or more desired destinations.
- 3) Click **Start**. You should see Ping responses on the screen with RTT (Round Trip Time) less than 100 milliseconds. See Figure 6-24.

Ping Result	Host	RTT	Bytes	TTL
5	72.30.2.43	11	32	57
Ping Host: www.flukenetworks.com				
1	192.65.40.154	43	32	57
2	192.65.40.154	68	32	57

Figure 6-24: Viewing Ping results

If the Ping test shows a timeout, then the IP connectivity with the local LAN must have failed. At this point, check on the health of the default gateway and the physical connection between the associated AP and the wired LAN.

Using the Trace Tool

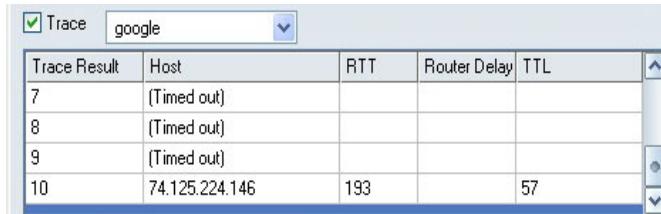
If Ping requests time out, the AirMagnet WiFi Analyzer's Trace utility can be used to isolate the routing path and locate breakage.

To run the AirMagnet Traceroute utility:

- 1) From the Connection Test screen, check the Trace check box.
- 2) Use the drop-down menu to select one or more destinations and click **Start**.

Functional IP routers capable of responding to ICMP messages on the path between AirMagnet WiFi Analyzer and the end node will then

appear on the screen. By examining the list of routers, you may be able to spot routing anomalies that exist. See Figure 6-25.



The screenshot shows a software interface titled 'Trace' with a dropdown menu set to 'google'. Below is a table with the following data:

Trace Result	Host	RTT	Router Delay	TTL
7	(Timed out)			
8	(Timed out)			
9	(Timed out)			
10	74.125.224.146	193		57

Figure 6-25: Viewing a trace result

Using the FTP Tool

The FTP tool allows the user to connect to a specified FTP server and transfer a selected file back and forth as many times as required to verify FTP connectivity. Prior to starting the test, the appropriate FTP server information must be configured using the Config button located at the top of the screen.

To use the FTP tool:

- 1) Click the Config button across the top of the screen.
- 2) Select the FTP tab.
- 3) Enter the desired information for the FTP server and click OK to save the changes.
- 4) From the Connection Test screen, check the FTP check box and select one or more destinations from the drop-down.
- 5) Click **Start**. Information about the Website will appear on the screen. See Figure 6-26.

	FTP Server	File	Status	Throughput
FTP Host: 209.220.161.142				
1	209.220.161.142	GeneralConfig.bmp	Uploaded	✓ 1065.78 kbps
1	209.220.161.142	GeneralConfig.bmp	Downloaded	✓ 1532.77 kbps

Figure 6-26: Information obtained with FTP tool

Using the HTTP Tool

The HTTP tool functions much like the FTP tool, testing HTTP upload/download instead of FTP. It allows the user to connect to a specified HTTP server and transfer a selected file back and forth as many times as required to verify connectivity. Prior to starting the test, the appropriate HTTP server information must be configured using the Config button located at the top of the screen.

To use the HTTP tool:

- 1) Click the Config button across the top of the screen.
- 2) Select the HTTP tab.
- 3) Enter the desired information for the HTTP server and click OK to save the changes.
- 4) From the Connection Test screen, check the HTTP check box, and select one or more destinations from the drop-down.
- 5) Click **Start**. Information about the Website will appear on the screen.

	HTTP Server	File	Status	Throughput
HTTP Host: www.flukanetworks.com				
1	192.65.40.154	Fn-dtx1800_01d.jpg	Downloaded	✓ 668.41 kbps
2	192.65.40.154	Fn-dtx1800_01d.jpg	Downloaded	✓ 1579.18 kbps
3	192.65.40.154	Fn-dtx1800_01d.jpg	Downloaded	✓ 1731.02 kbps

Figure 6-27: Information obtained with HTTP tool

Roaming Tool

The Roaming tool is another utility for troubleshooting VoWLAN installations. A key component of VoWLAN QoS is its ability to allow stations to roam between APs without dropping calls. If roam time is too long, the chances that calls will be dropped increases considerably. With AirMagnet WiFi Analyzer's Roaming tool, the user can measure the roaming delay between when a station disassociates from one AP and then associates with another AP. The illustration below shows AirMagnet WiFi Analyzer's Roaming tool screen.

Configuring Roaming Tool Settings

To measure roaming connectivity:

- 1) From the WiFi Tools screen, click the Roaming tool. The Roaming tool screen appears. See Figure 6-28.

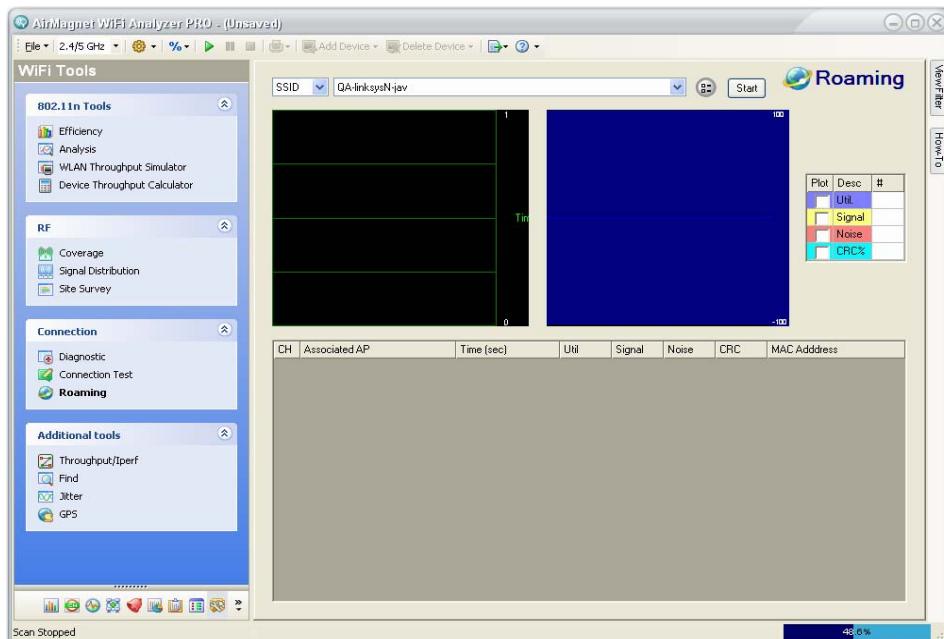


Figure 6-28: Roaming tool screen

- 2) Click  (Configure). The Roaming Options screen appears. See Figure 6-29.

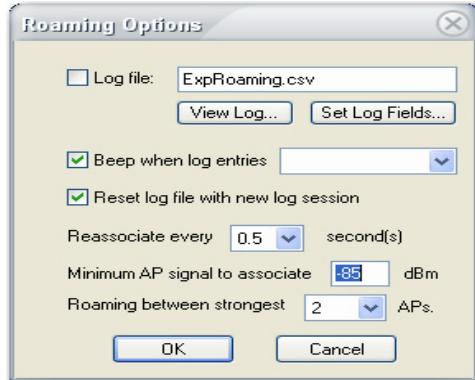


Figure 6-29: Configuring Roaming tool

- 3) Make the desired selections and click OK.

Conducting a Roaming Test

To conduct a roaming test:

- 1) From the top of the Roaming tool screen, select SSID or AP and then choose a specific SSID or AP from the drop-down list.
- 2) Click . Data will start to appear on the screen. See Figure 6-30.

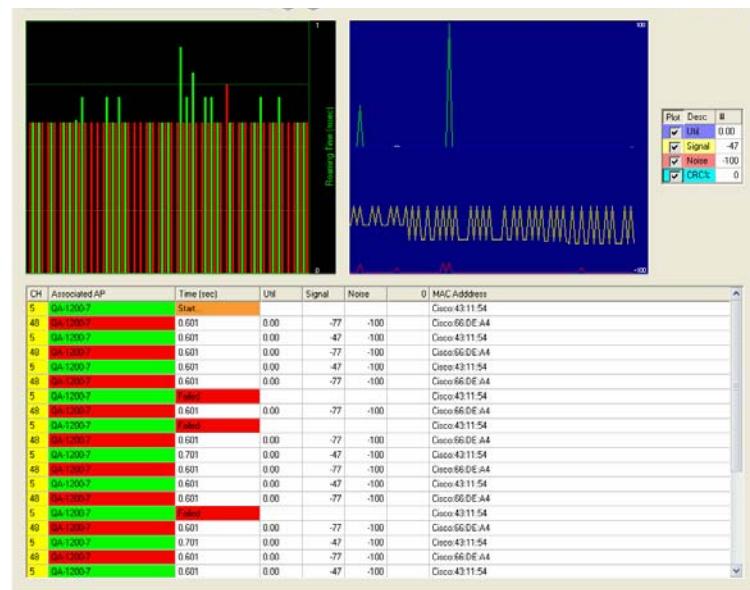


Figure 6-30: Measuring roaming connectivity

As seen from Figure 6-30, the Roaming tool tests the device's ability to switch between two APs and the time it takes for the associations. By looking at the data on the screen, the user can discover issues that may exist.

The graph pane on the right displays the data you have checked in the section to the right of it. You can check any or all of the different data fields to chart whichever type of data you're interested in.

Additional WLAN Tools

AirMagnet WiFi Analyzer comes with some additional tools for troubleshooting network performance, locating network devices, etc. The tools in this group include:

- Throughput/Iperf
- Find
- Jitter
- GPS

Throughput/Iperf Tool

AirMagnet WiFi Analyzer integrates with Iperf – a free, open-source software tool for network performance analysis. The integration allows the user to analyze bandwidth and throughput (TCP and UDP) as well as jitter and lost/total datagram from within the AirMagnet WiFi Analyzer user interface.

In order to take advantage of AirMagnet's integration with Iperf, the user has to download and install Iperf Version 1.7.0, which has been tested and verified to be working with AirMagnet WiFi Analyzer 9.0 PRO.

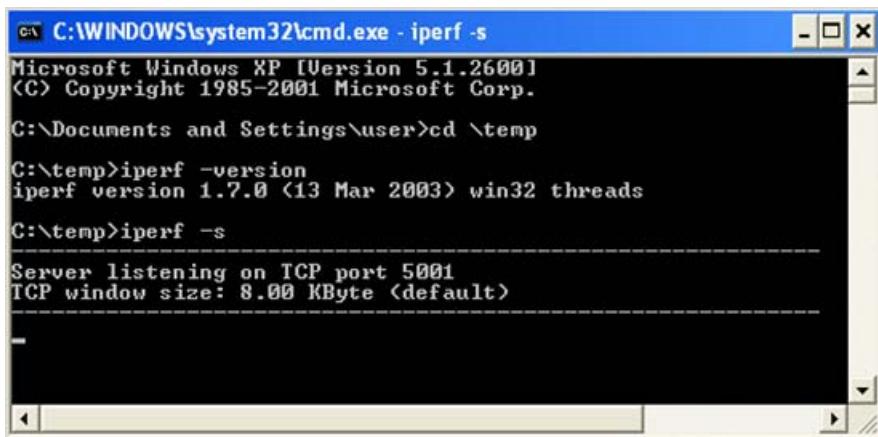
Downloading and Installing Iperf Software

To download and install Iperf:

- 1) Open your web browser and type <http://www.noc.ucf.edu/Tools/Iperf/>.
- 2) Under Windows, click the Local Download: [iperf.exe](#) (iperf version 1.7.0 (13 Mar 2003) win32 threads) link.
- 3) When the Download File dialog box appears, click Run.
- 4) Follow the instructions onscreen to complete downloading and installing Iperf.

Make sure to make a note of the destination to which Iperf is downloaded, for you'll need this information when running the Iperf Server.

- 5) From your PC on which Iperf is installed, open the Windows' Command Line Interface and perform the following tasks (Refer to [Figure 6-31](#) for commands used for the following tasks):
 - Check the version number of Iperf and make sure that it matches what is shown in the figure below.
 - Run the Iperf Server.



The screenshot shows a Windows XP Command Prompt window titled 'cmd.exe - iperf -s'. The window displays the following text:

```
C:\WINDOWS\system32\cmd.exe - iperf -s
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd \temp

C:\temp>iperf -version
iperf version 1.7.0 (13 Mar 2003) win32 threads

C:\temp>iperf -s
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
```

Figure 6-31: Iperf command line interface

- 6) Create a shortcut to the iperf.exe file and place it on your desktop.
- 7) Specify the target for the shortcut, as explained below.

Note: When creating the shortcut, you are required to specify the target location. The command for reaching the target location differs slightly depending on whether TCP or UDP protocol is used, as demonstrated in [Figure 6-32](#) and [Figure 6-33](#), respectively.

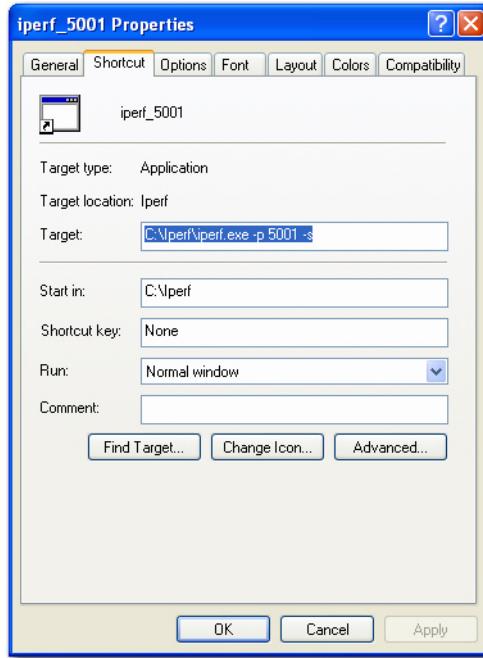


Figure 6-32: Creating Iperf shortcut for TCP

Figure 6-32 above shows the target as C:\Iperf\iperf.exe -p 5001 -s: where -p stands for port; 5001 for the port number; and -s for server. The protocol is TCP (default).

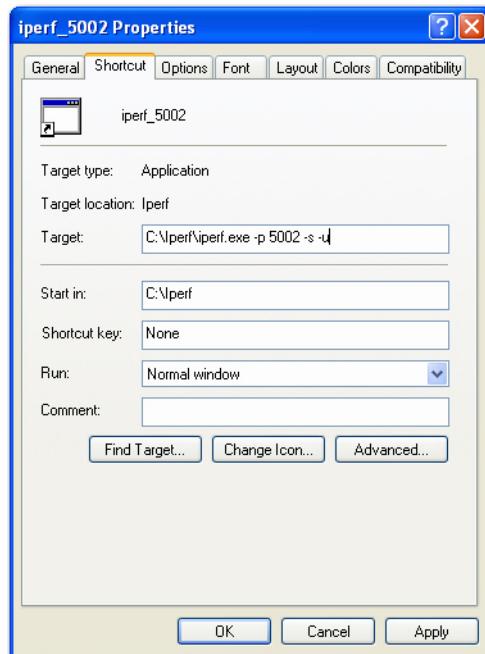


Figure 6-33: Creating Iperf shortcut for UDP

The target location in Figure 6-33 is `C:\Iperf\iperf.exe. -p 5002 -s -u`: where `-p` stands for port; `5002` for the port number; `-s` for server, and `-u` stands for UDP.

Analyzing Network Bandwidth and Throughput with Iperf

To analyze network bandwidth and throughput with Iperf:

- 1) From WiFi Tools screen, click the Throughput/Iperf tool. The Throughput/Iperf screen appears.
- 2) Select an AP.
- 3) Specify the length of the Test Period, e.g., 120.
- 4) Select a Chart Type, e.g., PHY Data Rate.
- 5) Make sure to check the Iperf Performance Test check box.

- 6) Select TCP or UDP and specify the Server and Port.
- 7) Check the Up/Downlink check box.
- 8) Click **Start**. Data start appearing on the screen, as shown in Figure 6-34.

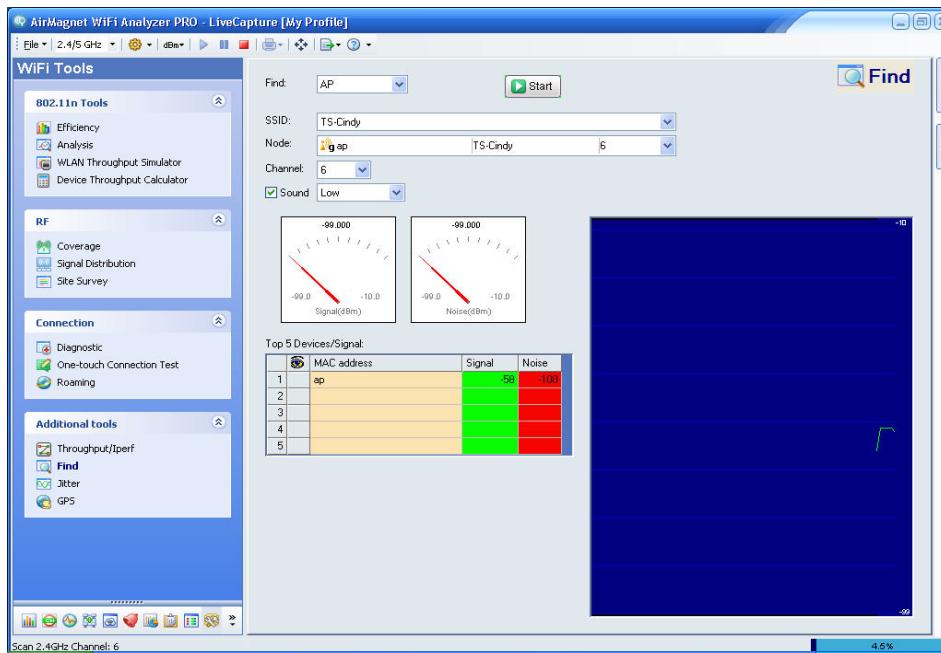


Figure 6-34: Throughput/Iperf test in progress

*The test ends automatically once the specified test period is timed out. You may also stop a live test at any time by clicking **Stop**. Figure 6-34 above shows that the network's throughput, measured by PHY Data Rate. PHY data rates for the downlink and the uplink are 2072 Kbps and 696 Kbps (the bar on the far right of each bar graph), respectively. For the downlink, 100% of the throughput (2072 Kbps) is using the 27-Mbps data rate; for the uplink, 100% of the throughput (696 Kbps) is using 108-Mbps data rate.*

The Throughput/Iperf screen contains two separate tools for conducting network performance tests: The upper half is the “old” AirMagnet WiFi Analyzer Performance tool that are available in AirMagnet WiFi Analyzer 7.x or earlier; the lower half is the Iperf tool that has become available with this AirMagnet WiFi Analyzer 9.0 release. If you do not check the Iperf Performance Test check box, then you will be running the “old” Performance test. If you check the check box, then you will be running both the old Performance tool and the new Iperf tool. The Iperf tool is a feature that is available in AirMagnet WiFi Analyzer PRO only.

When running an Iperf performance test using UDP with the Up/Down Link option enabled (checked), do not interrupt the test by clicking **Stop**. Doing so may cause the Iperf server to close down.

Using Advanced Iperf Properties

The Throughput/Iperf tool offers some Advanced Iperf Properties, which can be displayed by clicking **Advanced >>** button on the screen.

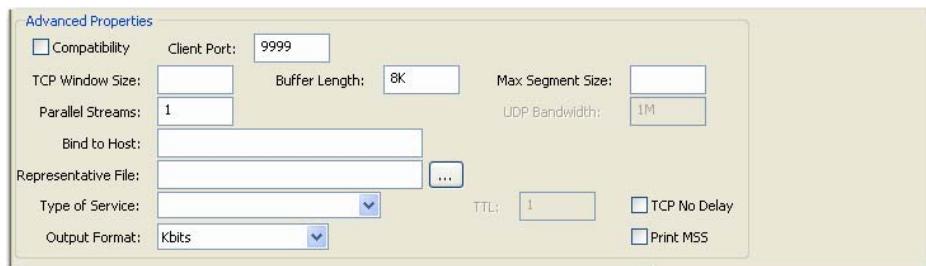


Figure 6-35: Advanced Iperf Properties

Table 6-6 describes the advance properties on Iperf tool.

Table 6-6: Advanced Iperf Properties

Property	Description
Compatibility	This option, if selected, allows for backward compatibility with older version of Iperf.
Client Port	The port through which the Iperf server will connect to the client. It defaults to the port used to connect to the Iperf server from the client.
TCP Window Size	Sets the socket buffer size to the specified value. For TCP, this sets the TCP window size. For UDP, it is just the buffer in which datagrams are received and so limits the largest receivable datagram size.
Buffer Length	The length of buffer to read or write. Iperf works by writing an array of len bytes a number of times. The default is 8 KB for TCP and 1470 bytes for UDP. Note for UDP, this is the datagram size and needs to be lowered when using IPv6 addressing to 1450 or less to avoid fragmentation.
Max Segment Size	Sets the TCP maximum segment size (MSS). TMSS is usually the MTU-40 bytes for the TCP/IP header. For ethernet, the MSS is 1460 bytes (1500 byte MTU).
Parallel Streams	The number of simultaneous connections to make to the server. Default is 1. <i>Note:</i> This feature requires thread support on both the client and the server.
UDP Bandwidth	The UDP bandwidth to send at, in bits/sec. The default is 1 Mbit/sec.

Table 6-6: Advanced Iperf Properties

Property	Description
Bind to Host	One of this host machine's addresses. For the client, this sets the outbound interface; for the server, it sets the incoming interface. This is only useful on multi-homed hosts, which have multiple network interfaces. For Iperf in UDP server mode, this is also used to bind and join a multicast group, in which case addresses in the range from 114.0.0.0 to 239.255.255.255 should be used.
Representative File	Click the button to select a representative stream to measure the bandwidth.
Type of Service	Select the type-of-service for outgoing packets from the following options: <ul style="list-style-type: none"> • Low Cost • Low Penalty • Reliability • Throughput
TTL	The time-to-live for outgoing multicast packets. This is essentially the number of router hops to go through and is also for scoping. The default is 1, link-local.
TCP No Delay	If selected, this will set the TCP no delay option, disabling Naggle's algorithm. Normally this is only disabled for interactive applications such as telnet.
Output Format	Click the down arrow and select from the drop-down list menu the format in which bandwidth numbers are to be printed. The supported formats are: <ul style="list-style-type: none"> • Adaptive Bits • Adaptive Bytes • Bits • Bytes • Kbits • Kbytes • Mbits • Mbytes

Table 6-6: Advanced Iperf Properties

Property	Description
Print MSS	This option, if selected, enables the print of the reported TCP MSS size (via the TCP_MAXSEG option) and the observed read sizes which often correlate with MSS. The MSS is usually the MTU - 40 bytes for the TCP/IP header. Often a slightly smaller MSS is reported because of extra header space from IP options. The interface type corresponding to the MYU is also printed (ethernet, FDDI, etc.). This option is not implemented on many OS's, but the read sizes may still indicate the MSS.

Find Tool

AirMagnet WiFi Analyzer not only can detect the presence of any wireless devices (including rogue APs and stations), but can also help the user locate the physical location of any devices that have been detected. This can be easily done using AirMagnet WiFi Analyzer's Find tool.

Locating Rogue Devices

The Find tool enables you to locate any device shown up on AirMagnet WiFi Analyzer screen. This section shows how to use the Find tool to locate rogue devices that AirMagnet WiFi Analyzer has detected on your WLAN.

To locate a rogue device:

- 1) From the AirWISE screen, look for alarms under Rogue APs and Client.
- 2) Identify an rogue AP or client, and record its SSID and MAC address.
- 3) From the WiFi Tools screen, select the Find tool. The WiFi Tools>Find screen appears. See [Figure 6-36](#).

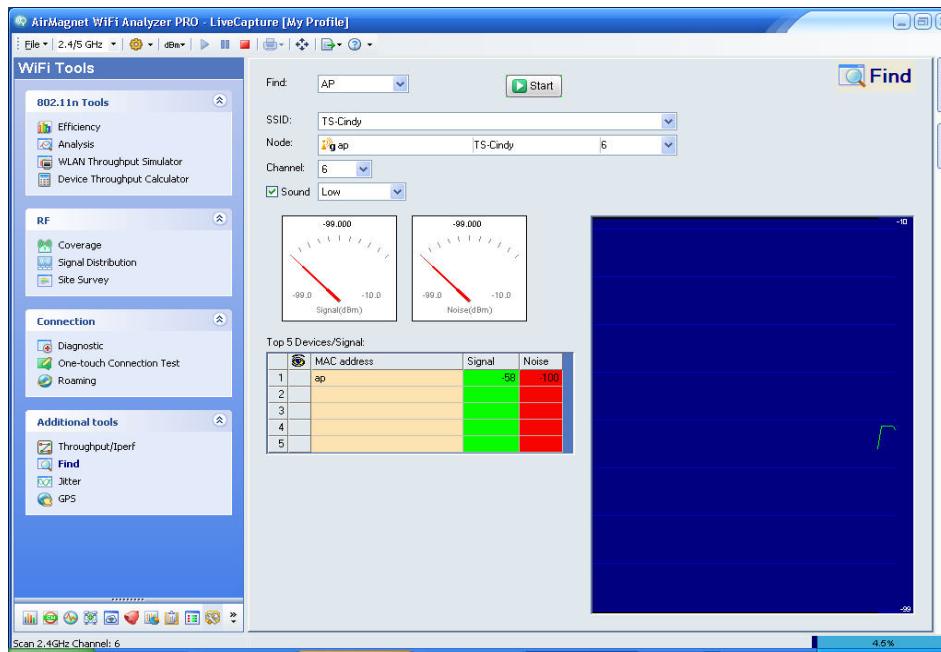


Figure 6-36: Selecting a rogue device to locate

- 4) Specify the type of rogue device you intend to find: AP vs. STA.
- 5) From the SSID list, select the SSID of the rogue device you have recorded.
- 6) Select the device and choose the channel the rogue device was using.
- 7) Click **Start**. The MAC addresses of the top 5 APs or stations with the same SSID will appear in the table, with the strongest one topping the list. See [Figure 6-37](#).

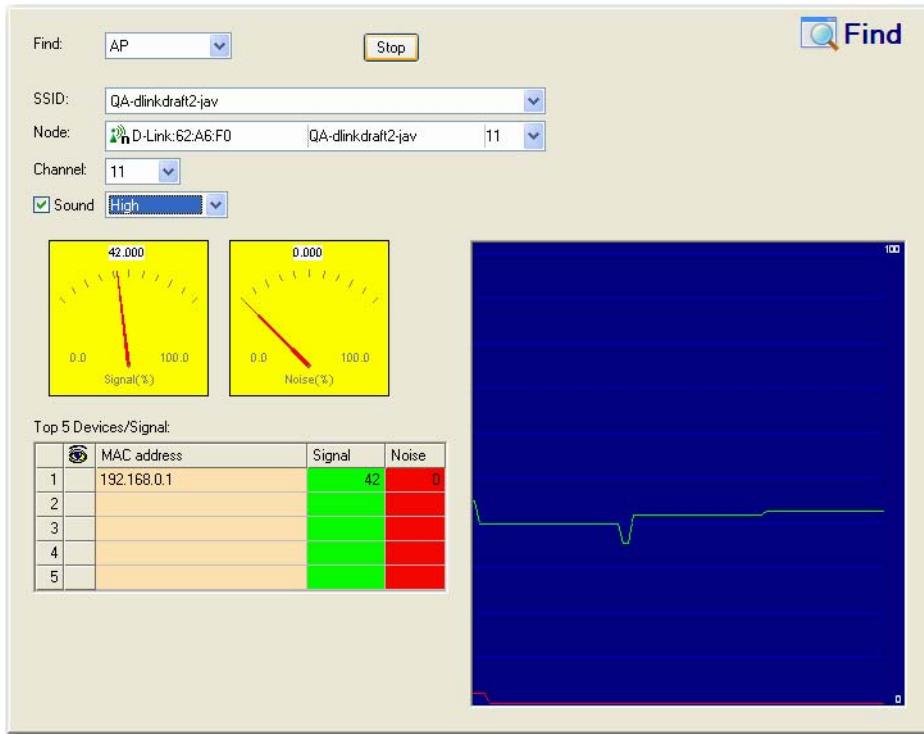


Figure 6-37: Locating a rogue device

- 8) In the Top 5 Devices/Signal pane, click the box next to the device you wish to locate.
- 9) Look at the signal meter, and walk in the direction in which the signal gets stronger as you walk.
- 10) Turn on the audio and set the volume to High to make it easier to locate the rogue device.
- 11) Click **Stop** to end the operation.

Jitter Tool

Jitter refers to unwanted variations in the frequency or phase of a digital or analog signal. VoWLAN phones and systems are designed to accommodate a certain amount of jitter in the network. However, if the jitter value gets too high, the quality of calls or network

connections may suffer. AirMagnet WiFi Analyzer's Jitter tool enables network administrators to easily test the jitter value on a VoWLAN to ensure the QoS for voice traffic. Figure 6-38 shows AirMagnet WiFi Analyzer's Jitter tool screen.

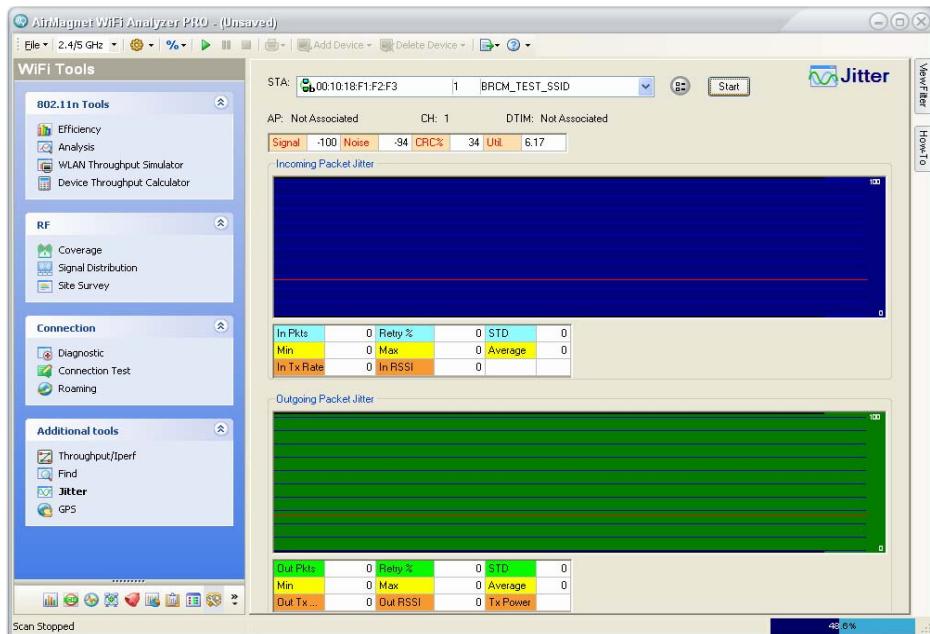


Figure 6-38: AirMagnet WiFi Analyzer's Jitter tool screen

Configuring Jitter Tool

You need to configure the Jitter tool so that it can function in a way that best serves your needs.

To configure Jitter tool settings:

- 1) From the WiFi Tools>Jitter screen, Click  (Configure). The Jitter Options dialog box appears. See [Figure 6-39](#).



Figure 6-39: Configuring Jitter tool

- 2) Make the desired selections and click OK.

Conducting a Signal Jitter Test

To measure RF signal jitter:

- 1) From the top of the Jitter tool screen, click the down arrow and select the station of interest from the drop-down list menu.
- 2) Select a station and click . The Jitter screen appears. See [Figure 6-40](#).

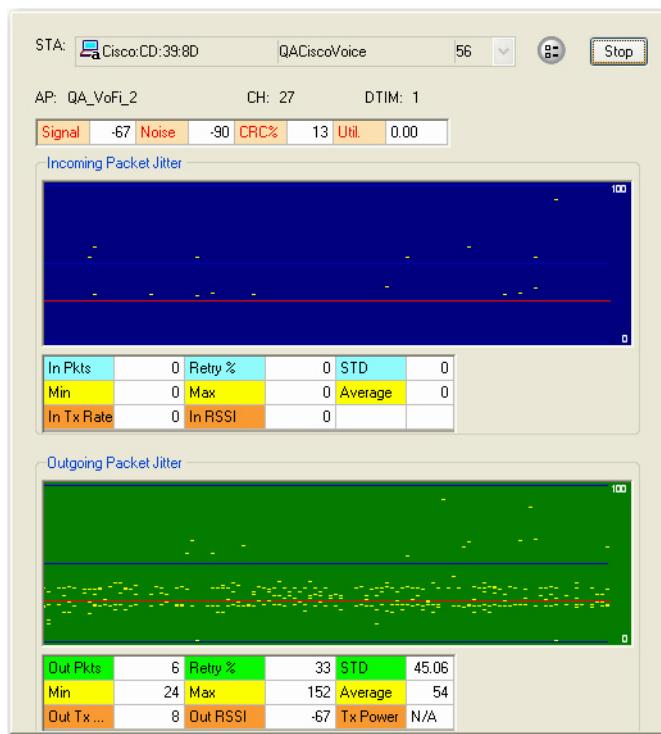


Figure 6-40: Measuring RF signal jitter value

- 3) Click **[Stop]** to end the test. See Table 6-7 for information shown on the Jitter tool screen.

Table 6-7: Jitter Tool Parameters

Parameter	Description
AP	The AP the station is associating with. Automatically detected.
CH	The channel the AP is operating on. Automatically detected.
Util	Channel utilization rate.

Table 6-7: Jitter Tool Parameters

Parameter	Description
Noise	Noise level in dBm.
CRC%	CRC error rate.
DTIM	DTIM configuration on the AP.
In Pkts	Incoming packets from the AP.
Retry%	Retry rate.
STD	Standard deviation
Min.	Minimum jitter value.
Max.	Maximum jitter value.
Average	Average jitter value.
Out Pkts	Outgoing packets to the AP.
Upper graph	Incoming packet jitter distribution from 0 to 100 ms.
Lower graph	Outgoing packet jitter distribution from 0 to 100 ms.
Red horizontal line	The expected jitter value.

GPS Tool

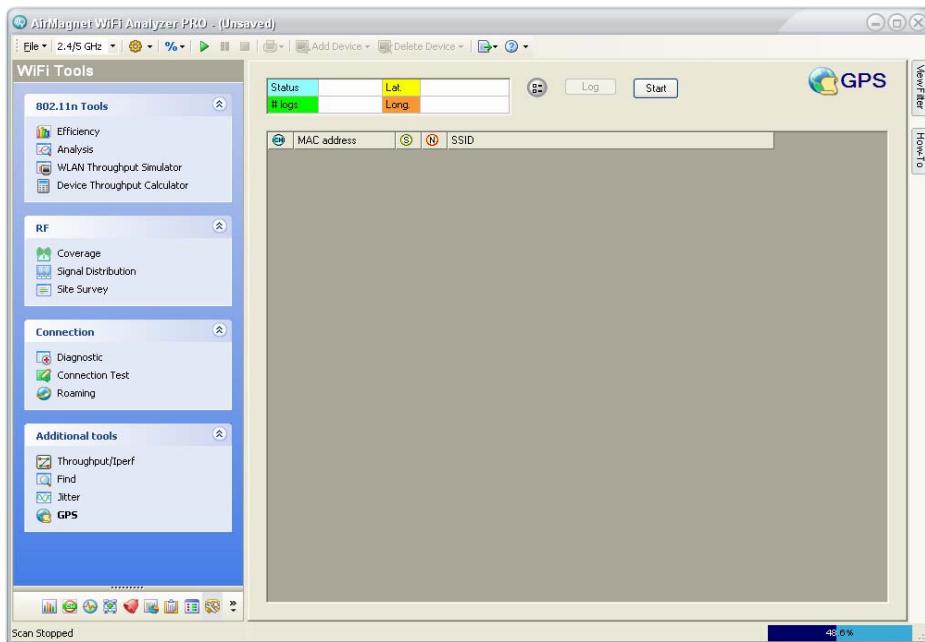
The GPS Log allows you to find the exact location of a device that AirMagnet has detected. You need to have a GPS device connected to the laptop in order to use this utility.

Configuring the GPS Log Tool

In order to properly use the GPS and AirMagnet WiFi Analyzer integration, you need to configure GPS tool.

To configure the GPS tool:

- 1) From the WiFi Tools screen, click the GPS tool. The GPS Log screen appears. See [Figure 6-41](#).

**Figure 6-41: GPS tool screen**

- 2) From the GPS tool screen, click (GPS Options). The GPS Options screen appears. See [Figure 6-42](#).

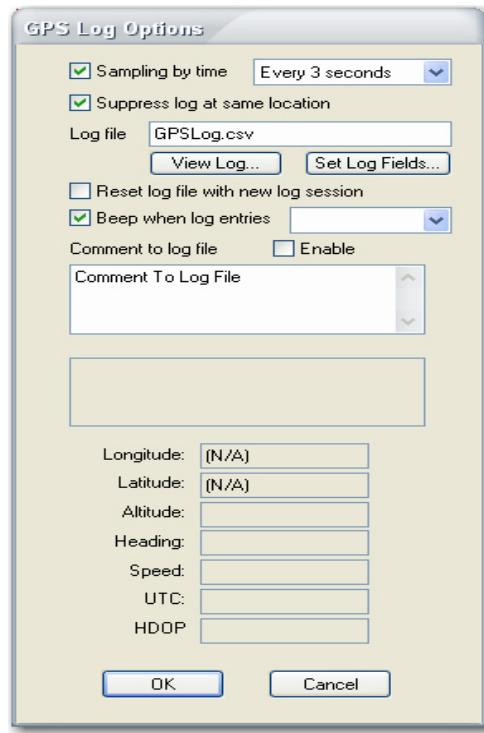


Figure 6-42: Configuring GPS tool

- 3) Make the desired selections, and click OK.

Collecting GPS Data

To collect GPS data:

- 1) From the GPS Log screen, click **Start**. Data start to appear on the screen.

Figure 6-43 shows the format of a GPS data file.

Figure 6-43: GPS log file format

Chapter 7: Managing Data Files

Chapter Summary

This chapter discusses how to manage the RF signal data log files you have captured using AirMagnet WiFi Analyzer. AirMagnet not only captures and displays wireless network data in real time, but also allows you to save, print, and export those data files for archiving, sharing, or further analysis.

This chapter covers the following topics:

- Saving the captured RF data
- Opening data files
- Previewing data before printing
- Viewing recently opened files
- Exporting data
- Exporting data to AirMagnet Reporter

Saving Captured Data

AirMagnet displays the data in real time as they are captured. However, due to the size limitation of the buffer, the system discards old data as new data come in. To keep certain data for further analysis, you need to save the data.

AirMagnet-supported File Formats

AirMagnet WiFi Analyzer supports the following file formats:

- **.amc** – AirMagnet’s proprietary file format, which can play back the saved data as if you were playing a video. It lets you revisit the data in the way they were captured.
- **.epc** – Ethereal’s file format.
- **.cap** – Sniffer’s file format.
- **.amm** – AirMagnet proprietary file format used for supporting Capture to Disk and Multi-adapter. Saving to this format is available only when one of these functions is enabled.
- **.pcap** – Files saved with the 802.11+ radio option.

Saving a New File

To save data:

- 1) From any AirMagnet WiFi Analyzer screen, click File>Save. The Save As dialog box appears. See Figure 7-1.

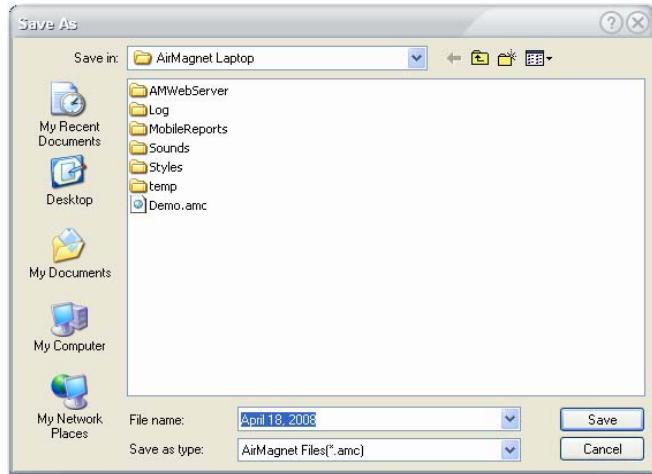


Figure 7-1: Saving a (.amc) file

- 2) Select a file path, name the file, and choose a file format.
- 3) Click Save.

By default, AirMagnet WiFi Analyzer automatically saves all trace (.amc) files to C:\Program Files\AirMagnet Inc\AirMagnet WiFi Analyzer on your PC, using the date and time when the file is saved as the file name. However, you can use a different directory and/or file name by overriding the default values. You can select another file format as well.

Saving an Existing File in a Different Name or Format

After viewing an existing file (see the following section), you can save it in a different name or format.

To rename a file:

- 1) Click File>Save As. The Save As dialog box appears.
- 2) Choose a file path, rename the file, or select another file format.
- 3) Click Save.

Opening a Saved File

Files saved in any of the AirMagnet-supported file formats can be opened in AirMagnet WiFi Analyzer. This allows you to revisit the historical RF data captured on your wireless network.

For AirMagnet WiFi Analyzer trace (.amc) files, there are two ways by which a file can be opened, depending on whether the **Load Statistics on Open Capture File**

(**File>Configure... General**) option is selected when opening the file. If the option is NOT used, AirMagnet WiFi Analyzer will only play back the amount of data saved in the buffer whose size was set at the time the trace file was saved. In that case, the title bar of the trace file being opened shows the progress of the file-loading operation in percentage (%) as it proceeds, as shown in Figure 7-3. However, if the **Load Statistics on Open Capture File** is used, AirMagnet WiFi Analyzer will loads all alarms (along with some other vital data) contained in the trace file, in addition to data in the buffer. In this way, the file loads much faster since the focus is on presenting all data on the screen rather than replaying them as they were captured. For that reason, the title bar of an opened trace file only shows the name of the file, as shown in Figure 7-4.

To open a AirMagnet-supported file:

- 1) Decide whether you want to use the Load Statistics on Open Capture File option (File>Configure...>General).
- 2) Click File>Open. . . . The Open screen appears. See Figure 7-2.

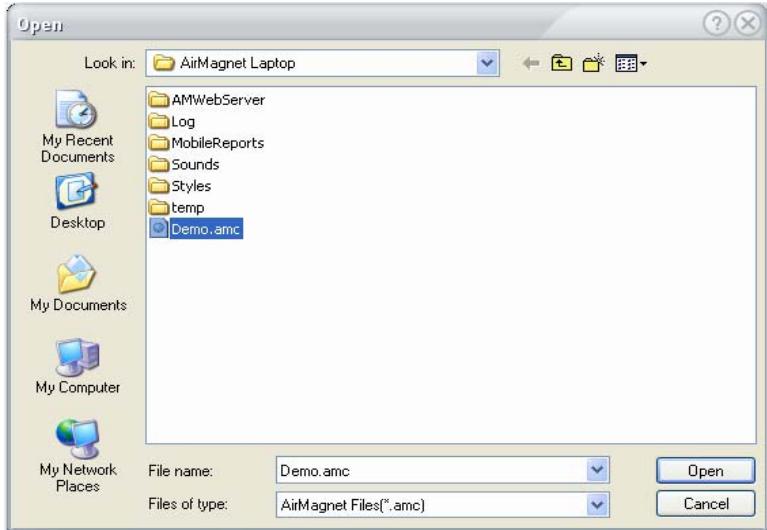


Figure 7-2: Opening a (.amc) file

- 3) Select the file and click Open. The file data start to appear on the screen. See Figure 7-3.

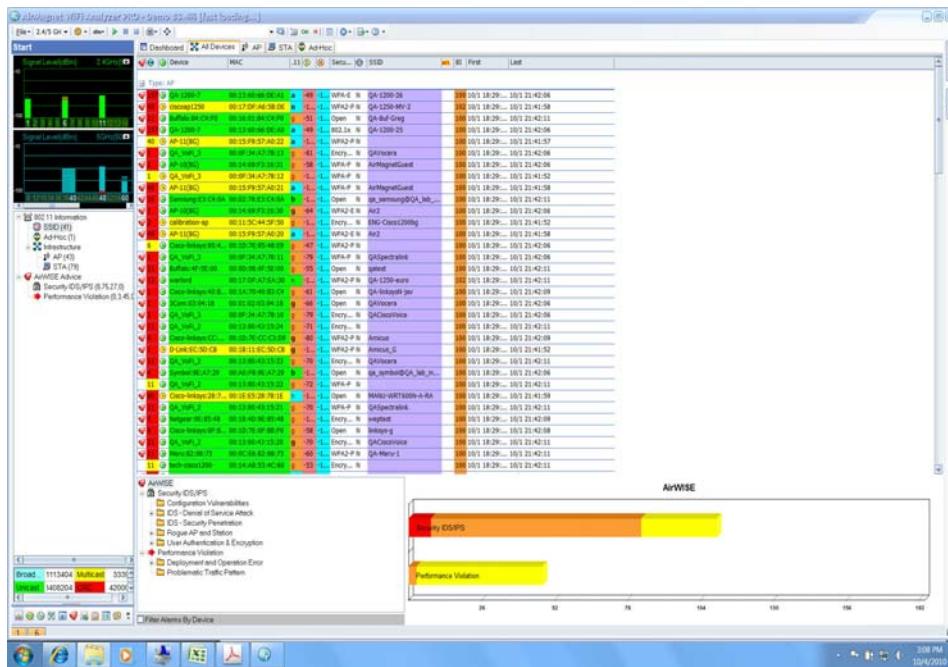


Figure 7-3: Playing back a trace file

- 4) Wait until the value on top of the screen becomes 100%, which means that the file is completely opened.

Figure 7-3 shows a trace file being opened without using the **Load Statistics on Open Capture File** option. It takes more time to open a trace file in this way, especially when it is a big trace file. However, you can always speed up the file loading process by pressing the F4 key. Alternatively, if you use the **Load Statistics on Open Capture File** option when opening the trace file, the file loads instantly and you can see a lot more data, as shown in Figure 7-4.

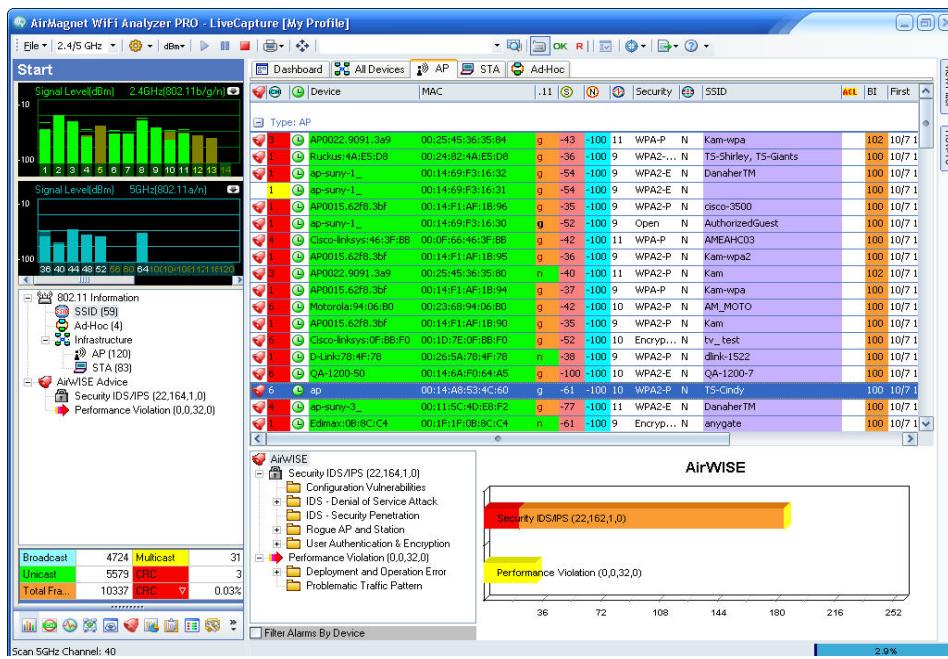


Figure 7-4: Loading statistics on open capture file

The live capture function is suspended while a trace file is being opened or after it is opened. To resume live capture, click (*Start Live Capture*).

Viewing Recently Opened Files

AirMagnet WiFi Analyzer keeps track of the four most recently opened files in its Recent Files list under the File menu. This makes it easier for you to access those files.

To access a recently opened file:

- 1) Click File>Recent Files. A pop-up list appears on the screen, displaying the four most recently opened files. See Figure 7-5.

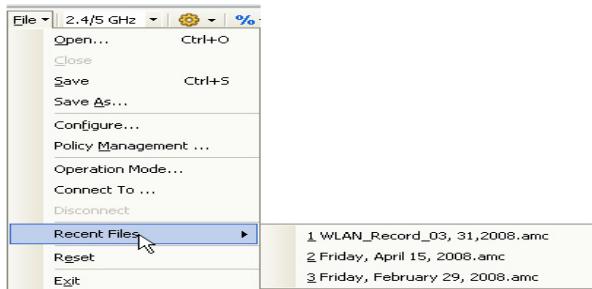


Figure 7-5: Viewing the list of recent files

- 2) From the Recent Files submenu, select a file to open it.

Exporting Database Files

AirMagnet WiFi Analyzer maintains complete wireless LAN device information, associated Layer-1 and Layer-2 statistics, and the generated alarms in its internal database as it scans and analyzes the packets it receives. The database contents can be exported as a set of comma-separated-value (.csv) files, which can then be uploaded to a host computer as sources for Excel spreadsheets or other database applications.

To export AirMagnet database files:

- 1) Click  (Import/Export) and select Export. . . The AirMagnet Export screen appears. See Figure 7-6.

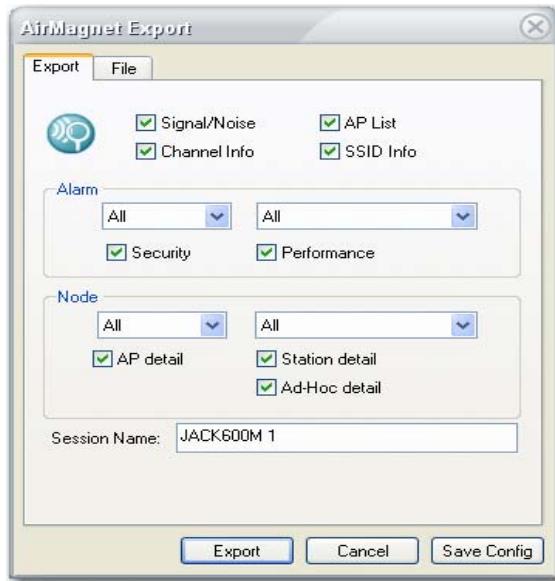


Figure 7-6: Export a (.csv) file

- 2) Overwrite the Session Name with a name unique to the site where the data are collected.

Each data export operation is called a session. Specifying session names will help you identify data exported at different times or on different occasions.

- 3) Make the desired selections and click Save Config.

- 4) Click the File tab. This will open another screen where you can modify the names of the files. See Figure 7-7.

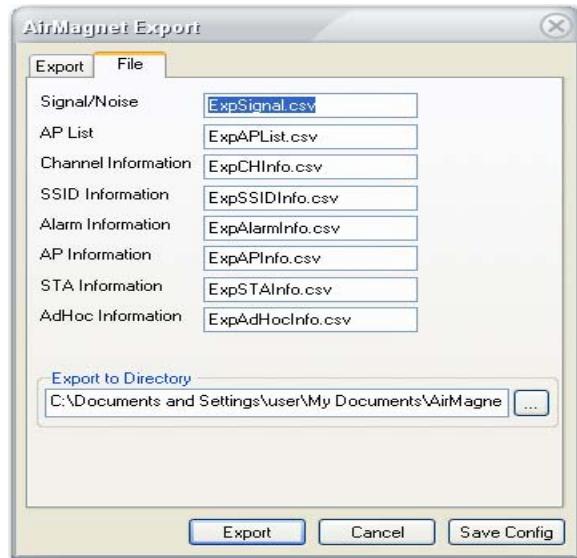


Figure 7-7: Configuring export file settings

- 5) Rename the files, if you want to.
6) Specify a file path.
7) Click Export.

THE FILE EXTENSION CANNOT BE CHANGED.

.csv files can be opened in Microsoft Excel. Figure 7-8 shows a sample .csv file.

Figure 7-8: The format of a .csv file

Chapter 8: Managing WLAN Reports

Chapter Summary

This chapter introduces the AirMagnet WiFi Analyzer's Reports feature and shows you how to use it to organize, view, share, and archive data of your network.

This chapter covers the following topics:

- Accessing Reports screen
- Reports screen UI components
- Compiling a report book
- Printing a report
- Exporting a report

AirMagnet WiFi Analyzer WLAN Reports

AirMagnet WiFi Analyzer automatically converts data it has captured on your network into a variety of network data reports. The Reports screen not only allows you to view your network data reports, but also provides the tools you need to build custom report books, which are collections of reports compiled with the reports selected by a user. It provides a convenient way for organizing, sharing, and archiving data that are collected on your network. You can navigate to the Reports screen simply by clicking  on the navigation bar. Alternatively, you can open the Reports screen directly from most of the major screens by clicking  (View Reports) and selecting a report option from the drop-down menu. Figure 8-1 shows AirMagnet WiFi Analyzer's Reports screen.

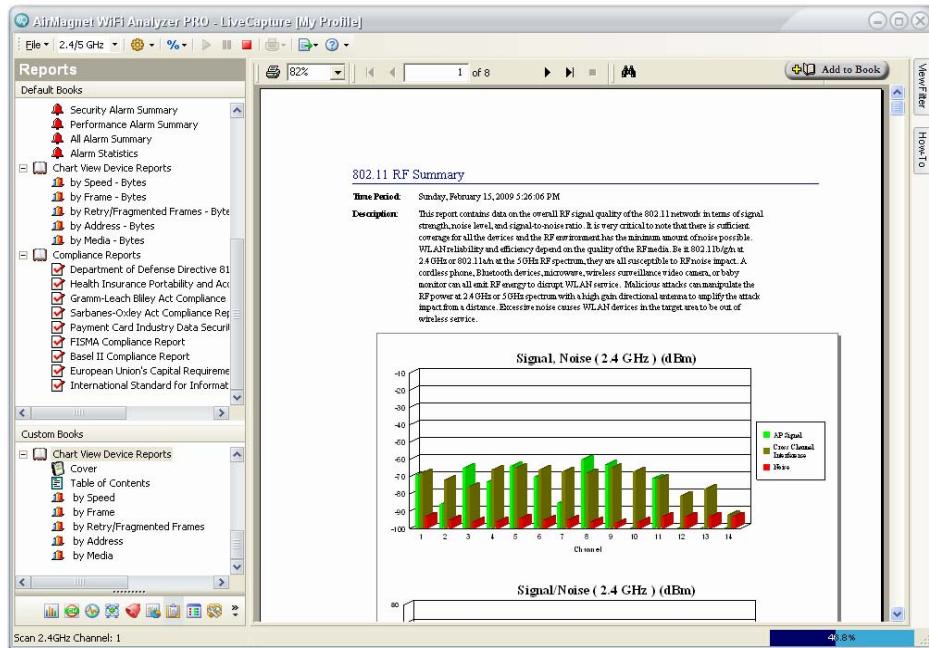


Figure 8-1: AirMagnet WiFi Analyzer Reports screen

Reports Screen UI Components

Figure 8-1 shows the major components of the AirMagnet WiFi Analyzer's Reports screen. Table 8-1 describes the functions of each of the components.

Table 8-1: Major Components of Reporter Screen

Screen Component	Description
Custom Books	This part of the screen allows you to compile your own report books using the reports the program automatically generates. By default, you'll see three sample report books when you first open the screen. They are intended to give you a quick look and feel of the AirMagnet Mobile Report Book. You can modify any of these books by adding or deleting reports to or from it. Clicking an entry will display the report in the Report Window. <i>For instruction on how to compile or modify a report book, see the specific sections later in this chapter.</i>
Default Books	This part of the screen shows all the reports that the program has generated. The reports are grouped by the screen the data are related to. Clicking an entry will display the report in the Report Window.
Report Window	The section display the content of the report that is currently selected.
	This button allows you to print the current report.,
 100%	This box show the current view ratio of the Report Window. You can customize the size of the window by clicking the down arrow and selecting a view option from the drop-down list.

Table 8-1: Major Components of Reporter Screen

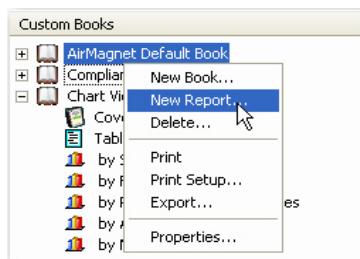
Screen Component	Description
	This part of the screen allows you to navigate through the current report back and forth by clicking the left and right arrows.
	This button opens the Search dialog box where you can search text through a report.
	This button enables you to add the report currently opened on the screen to a custom report book.
View Filter Tab	You may use the View Filter tab to narrow the results of your reports. For example, if you wish to eliminate a specific channel or SSID from your report, you can uncheck it from the filter and re-generate the report.

Compiling a Report Book

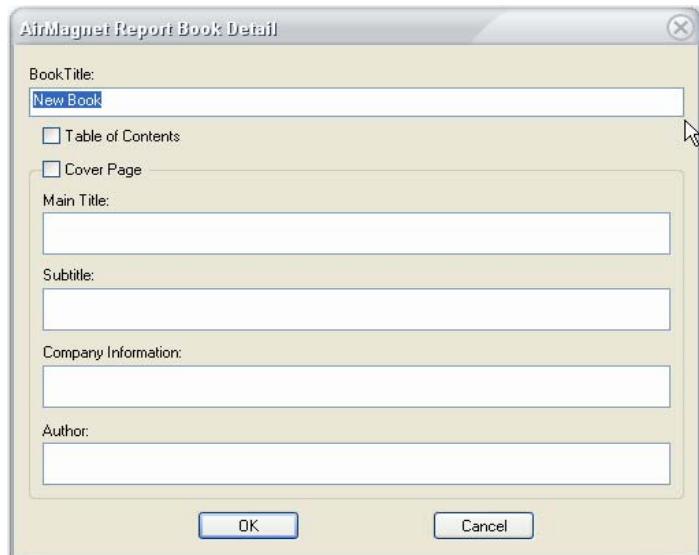
AirMagnet Mobile Reporter uses the book concept to enable users to organize reports into report books. This provides a simple and convenient way for organizing, sharing, and archiving WLAN data.

To compile a report book:

- 1) Right-click the top level of the Custom Books section and select New Book... from the drop-down menu. See Figure 8-2.

**Figure 8-2: Compiling a new book of reports**

Once you click *New Book...* in the drop-down menu, the AirMagnet Report Book Detail dialog box appears. See Figure 8-3.

**Figure 8-3: Specifying report book properties**

- 2) Make the entries and/or selections as described in Table 8-2.

Table 8-2: Parameters for a Report Book

Entry	Description
Book Title	Enter a title for the report book. This title appears on the highest level in the report book structure.
Table of Contents	If checked, the program will automatically create a table of contents for the book. Each individual report you add to a report book becomes a separate chapter of the book, and the report title becomes the chapter title and is automatically entered in the table of contents.
Cover Page	If selected, the program will automatically add a cover page to the book.
Main Title	Enter a main title for the book. This title appears on the top of the cover page.
Subtitle	Enter a subtitle for the book. It should help explain the main title.
Company Info	Enter some basic information about the company which the report is all about.
Author	Enter the name of the person who compiles the book.

- 3) Click OK. The newly created book will be added to the bottom of the Custom Books section.

At this point, the report book you have just created contains no reports. You need to add reports to it to make it complete. There are a number of ways for adding reports to a book.

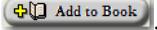
Adding Reports to Book

There are a number of ways for adding reports to a report book. Their operating procedures differ from one another as documented below.

Adding an Open Report to Book

This procedure is used for adding a report currently open in the report window to a report book.

To add an open report to a report book:

- 1) From the Default Books section, open a report of interest.
- 2) From the Custom Books section, highlight the title of the report book to which the report is to be added.
- 3) Click .

Dragging Default Reports to Book

This section describes the procedures for directly adding reports to a report book by drag and drop.

To add reports to a report book:

- 1) From the Default Books section, select a report of interest and drag and drop it directly to the book.
- 2) Repeat Step 1 until all relevant reports are added to the book.

Adding Custom Reports to Book

This section describes the procedures for adding custom reports to a report book. It differs from the other methods in that it allows you to custom the reports before adding them to the report book.

To add a custom report to a report book:

- 1) In the Custom Books section, right-click the title of the book of interest. The right-click menu appears. See Figure 8-4.

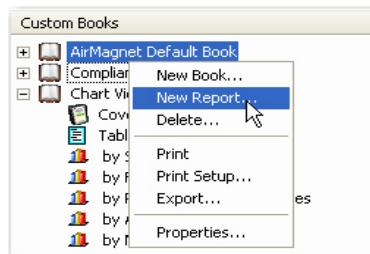


Figure 8-4: Adding a custom report

- 2) From the right-click menu, select New Report.... The AirMagnet Report Detail dialog box appears. See Figure 8-5.

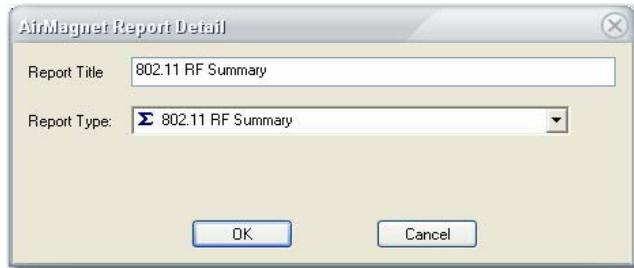


Figure 8-5: Report Detail dialog box

- 3) From where it says Report Type, click the down arrow to bring up the list of reports and select a report type from the drop-down menu. See Figure 8-6.

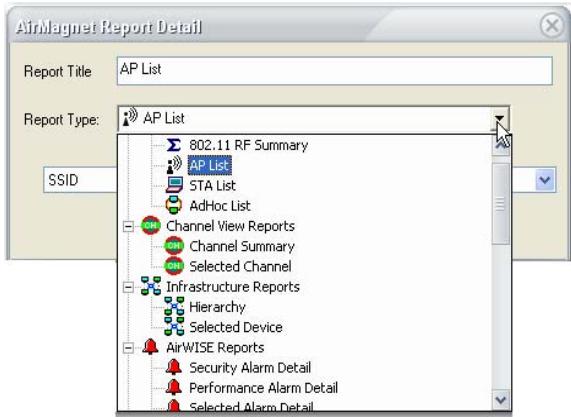


Figure 8-6: Selecting a report to add to book

Note: From here on, the dialog box may look different depending on the report the user selects. Some reports may provide more filters than others.

- 4) Follow the screens, if applicable, to fine-tune the selected report.
- 5) Click OK. The custom report is added to the report book.
- 6) Repeat Steps 1 through 5 to add all relevant custom reports to the book.

Modifying Book Properties

Book properties refer to all the information you entered in the AirMagnet Report Book Detail dialog box at the time a book was created. They include the book title, cover page, table of contents, etc.

To modify the properties of a book:

- 1) From the Custom Books section, right-click the book title and select **Properties...** from the pop-up menu. See Figure 8-7.

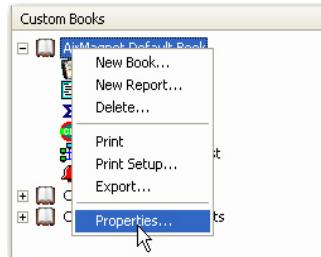


Figure 8-7: Modifying properties of a report book

The AirMagnet Report Book Detail dialog box appears, showing all the information that was entered when the report book was created. See Figure 8-8.

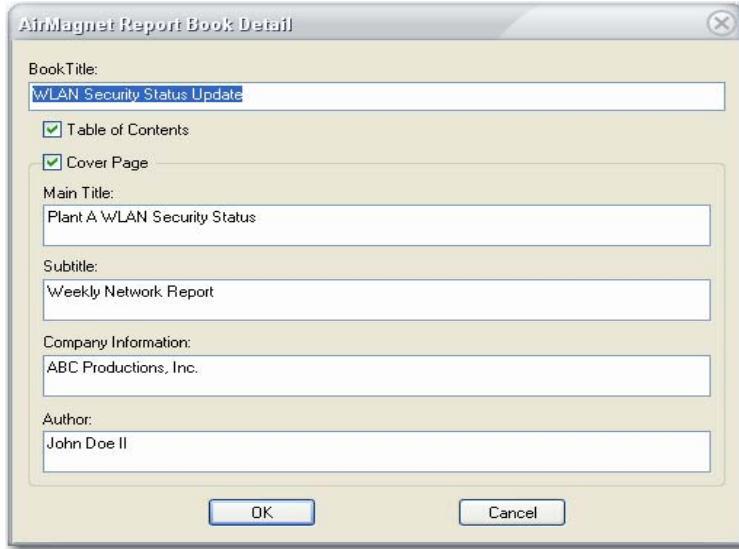


Figure 8-8: Modifying report book properties

- 2) Make any desired changes by highlighting the text in the corresponding fields and overwriting it with new information.
- 3) Click OK when completed.

Modifying Report Properties

Modifying the properties of a report book means making changes to data contained in the report by using different filters.

To modify the properties of a report:

- 1) From the Custom Books section, right-click the report of interest.
- 2) From the right-click menu, select **Properties...**. The AirMagnet Report Detail dialog box appears. See Figure 8-9.

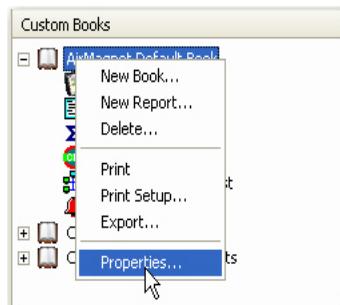


Figure 8-9: Modifying report properties

- 3) Make the desired changes and click OK.

Deleting Reports from a Report Book

You can remove any part of a report book, including the cover page, table of contents, and individual chapters.

To remove a part from a report book:

- 1) From the Custom Books section, right-click the part of the book you want remove.
- 2) From the pop-up menu, click Delete. . . . See Figure 8-10.

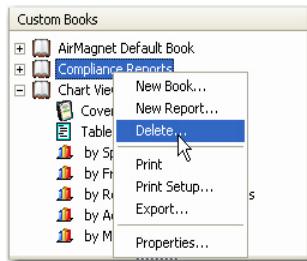


Figure 8-10: Deleting a report

A confirmation message appears.

- 3) Click Yes. The selected item will be removed from the report book after the screen refreshes.

Printing Out Reports

You can print any report or report book from either the Default Books or the Custom Books section on the Reports screen.

To print a report (Default Books or Custom Books):

- 1) Open the report of interest.
- 2) Click  (Print Report).

The instructions above apply when printing a report from the Default Books or Custom Books sections. You can also print reports from the Custom Books section using the right-click menu, as shown in the following paragraph.

To print a report (Custom Books only):

- 1) From the Custom Books section, right-click the report of interest.
- 2) From the right-click menu, click Print. See Figure 8-11.

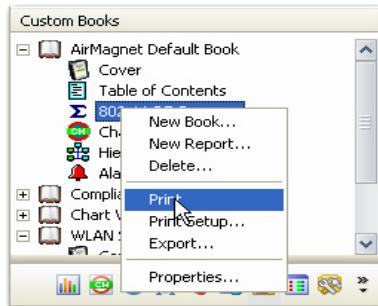


Figure 8-11: Print a custom report using right-click menu

The right-click menu is available only in the Custom Books section of the Reports screen.

Exporting a Report or Report Book

Reports or report books in the Custom Books section of the Reports screen can be exported in any of the following file formats:

- Adobe PDF
- HTML
- MS Word
- XML

To export a custom report or report book:

- 1) From the Custom Books section, right-click the entry of interest.
- 2) From the right-click menu, select Export.... The Export dialog box appears. See Figure 8-12.

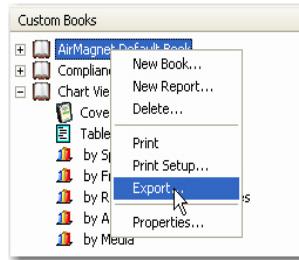


Figure 8-12: Exporting reports

- 3) From the Export dialog box, select a file format, specify a export path, and click OK.

Searching Text through a Report

You can conduct text-based searches through a report using (Search Text), which allow you to find any alphanumeric characters or string of characters.

To search text in a report:

- 1) Open a report from the Report screen.
- 2) Click . The Search dialog box appears. See Figure 8-13.

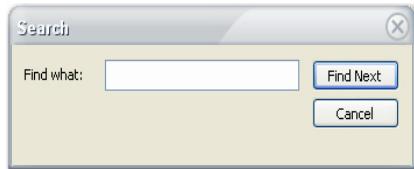


Figure 8-13: Searching text through report

- 3) Enter the text you want to find, and click **Find Next**.
- 4) The program will find the text, if it is available, and highlight it in the Report screen.
- 5) Keep clicking **Find Next** until you reach the end of the report.

Chapter 9: Scanning 4.9-GHz Spectrum

Chapter Summary

This chapter discusses how to use AirMagnet WiFi Analyzer to scan the 4.9 -GHz band, which is a radio band dedicated to public safety in the United States. It covers the following topics:

- About the 4.9-GHz band
- AirMagnet-supported 4.9-GHz wireless network adapters
- Scanning the 4.9-GHz band

This feature is available in AirMagnet WiFi Analyzer PRO only.

About the 4.9-GHz Band

Since early 2003, the Federal Communications Commission (FCC) has dedicated 50 MHz of radio spectrum in the 4.9-GHz band (i.e., between 4.940 MHz and 4.990 MHz) for public safety use. Use of the 4.9-GHz spectrum is controlled by license; communications in this radio band must support the protection of life, health, or property of the general public. Qualifying state or local government entities can hold licenses to use the 4.9 GHz spectrum within their own areas of jurisdiction; entities that are not eligible for holding licenses but provide services critical to the support of public safety may share licenses with 4.9-GHz license-holders. The newly allocated spectrum enables public safety entities to quickly deploy on-scene wireless networks for streaming video, instant Internet and database access, and speedy transfer of large data or image files such as maps, building blueprints, patients' medical records, and photographs.

The FCC Rules categorize the use of the 4.9-GHz band into primary use and secondary use. The former includes hot spots, temporary fixed point-to-point or point-to-multipoint base/mobile/portable operations; the latter refers to fixed point-to-point operations that are secondary to the primary use of the band. A license authorizes a public safety agency to use all 50 MHz of the spectrum within its legal jurisdiction. Different licensees that are operating in close proximity with one another share all the frequencies; they are responsible for interference prevention, mitigation, and resolution. The Rules further mandate that under no circumstances should secondary operations cause interference to primary operations and must tolerate the interference caused by primary operations.

Monitoring 4.9-GHz Band

As a licensed radio band, the greatest advantage of the 4.9-GHz spectrum lies in the fact that it offers an interference-free operating environment for public safety broadband communications. It is best suited for fixed wireless applications for point-to-point (P2P) and point-to-multipoint (PMP) communications. Used in the P2P and PMP mode, there are a number of services that a public safety agency can craft out of a 4.9-GHz radio transmission backbone. These services and applications can replace costly leased services, thus leading to an ROI and long-term savings for the agency. AirMagnet WiFi Analyzer is the first software application that is capable of monitoring and analyzing the 4.9-GHz band.

Supported 4.9-GHz Wireless Network Adapters

To take advantage of AirMagnet WiFi Analyzer's 4.9-GHz feature, the user must have a AirMagnet WiFi Analyzer PRO license and use one of the following 4.9-GHz wireless network adapters:

- Linksys Wireless A+G Notebook Adapter WPC55AG version 1.3
- Ubiquiti SR4C 4.9 GHz
- TRENDnet TEW-501PC ag

Setting AirMagnet WiFi Analyzer in 4.9-GHz Mode

To set AirMagnet WiFi Analyzer in 4.9-GHz mode:

- 1) Insert a supported 4.9-GHz wireless network adapter into the card slot on your laptop PC.
- 2) Start AirMagnet WiFi Analyzer.
- 3) From the menubar, click the Band button and select FCC 4. 9 from the drop-down list. See Figure 9-1.



Figure 9-1: Selecting the 4.9-GHz Band

- 4) Click File > Configure . . . > Scan 4. 9. See Figure 9-2.

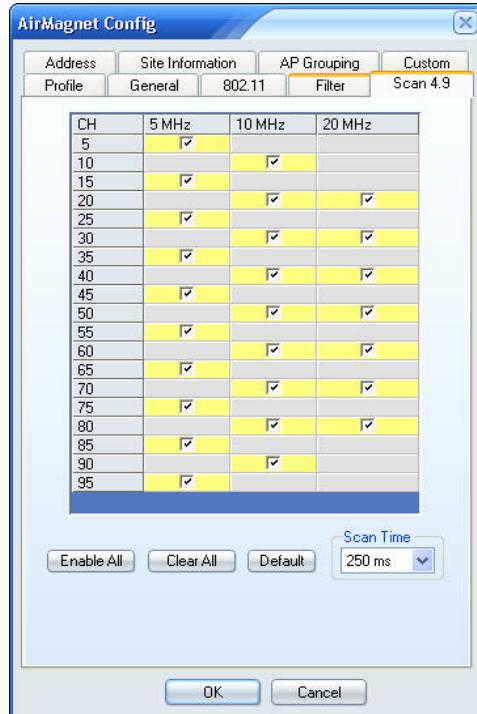


Figure 9-2: Specifying 4.9-GHz Channels and Bandwidths

Figure 9-2 displays all the 4.9-GHz channels dedicated to public safety in the US.

- 5) Select the desired 4.9-GHz channels and bandwidths.
- 6) Specify the Scan Time (interval).
- 7) Click OK.

When AirMagnet WiFi Analyzer is operating in the 4.9-GHz mode, its screens only display data detected on the selected 4.9-GHz channels. The amount of data shown on the screen depends on the number of 4.9-

GHz devices operating on your network. Figure 9-3 shows the Start screen in 4.9-GHz mode.

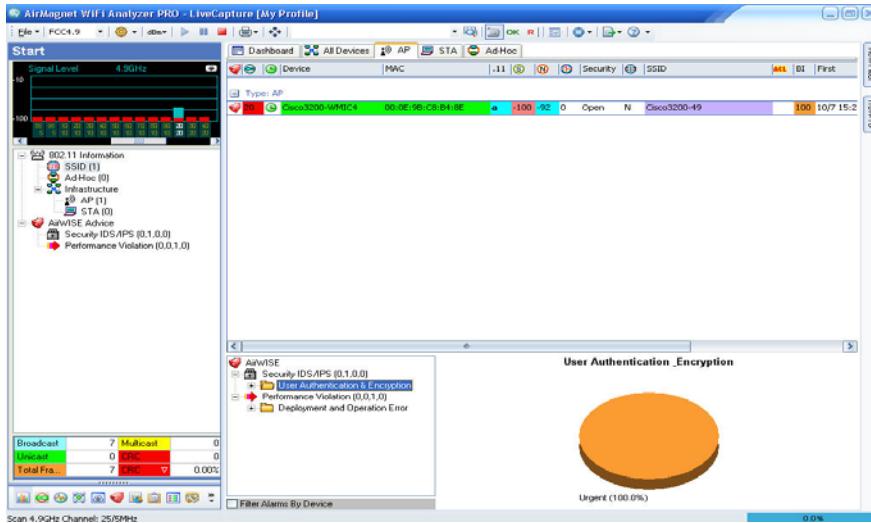


Figure 9-3: Start Screen in 4.9-GHz Mode

Chapter 10: Solving 802.11n Issues

Chapter Summary

This chapter discusses how to use AirMagnet WiFi Analyzer to monitor, troubleshoot, and resolve 802.11n-related issues on the network.

This chapter covers the following topics:

- How to find out 802.11n features on an AP?
- What 802.11n features are NOT used on an AP or STA?
- What happens If a particular 802.11n feature is (Not) used?
- How much traffic is sent using 40-MHz channel width?
- What channel settings should I use If I have a new AP?
- How to find out the maximum throughput of an installed AP?
- Why am I NOT getting the expected throughput from an AP?
- What is the expected device throughput for an AP?
- What should be taken into consideration when configuring new APs?
- What change in network throughput is expected when deploying new APs and/or STAs on the network?
- How to find out the network throughput between an AP and a STA?
- How can I know if my 802.11n AP is associated with any legacy devices?

- How much overhead does an 802.11n AP use to support legacy devices?
- How will associated legacy devices decrease 802.11n device throughput?
- How many legacy APs can be added to an 802.11n network?
- How will 802.11n STAs affect an existing 802.11a network?

How to Find Out 802.11n Features on an AP?

The IEEE 802.11n standard comes with a lot of new features.

According to IEEE, some of the features are mandatory while others are optional. To take full advantage of the new 802.11n protocol, it is important to know what 802.11n features are used on 802.11n APs deployed on your network. AirMagnet WiFi Analyzer offers the tool for the user to do just that.

To find out the 802.11n features used on an AP:

- 1) Open the Start screen.
- 2) From the menubar, click **Easy View** and select **View by 802.11n** from the drop-down menu. See Figure 10-1.

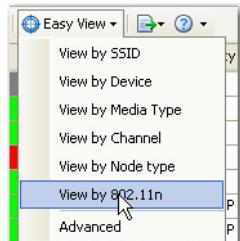


Figure 10-1: Viewing 802.11n features

The Start screen refreshes only to display 802.11n devices. You can then scroll up or down to view all 802.11n APs on the network and then scroll left and right to view the 802.11n features and what features are used on which APs. See Figure 10-2.

The screenshot shows a software interface for managing 802.11n devices. At the top, there's a toolbar with icons for Device, Tx C..., R..., PCO, Gr..., SGI, 2nd Ch, Operating ..., Non HT OBSS, 4..., and RIFS Mode. Below the toolbar is a table with the following data:

	Device	Tx C...	R...	PCO	Gr...	SGI	2nd Ch	Operating ...	Non HT OBSS	4...	RIFS Mode	
0	Wistron Neweb:B0:0...	0	20/40	20	N	N	40	None	All STAs HT	N	N	N
0	Wistron Neweb:B0:0...	67	20/40	20	N	N	40	None	All STAs HT	N	N	Prohibited N
0	Wistron Neweb:B0:0...	0	20	20	N	N	None	All STAs HT	N	N	N	Prohibited N
1	Intel:9E:6F:B3	0	20	20	N	Y	20	None	All STAs HT	N	N	Prohibited N
19	Apple:FA:B8:CE	67	20/40	2...	N	N	40	Above	All STAs HT	N	N	Prohibited N
83	ciscoap1250	40	20/40	2...	N	N	20/40	Below	One or mor...	Y	N	Prohibited N

Figure 10-2: Viewing 802.11n devices and features

To make it easy to know all 802.11n features that are available and which of those features are used on your AP, you can open the Field Chooser dialog box by right-clicking in the Start screen and selecting Set Display Columns. This dialog box shows all types of data, including all 802.11n features, that are currently available for the 802.11 network. You can even add all these 802.11n features onto the screen by drag and drop.

The Easy View>View by 802.11n can display the following 802.11n features (which are explained in detail in Table 3-4):

- Operating Mode
- Primary/Secondary Channels
- RIFS Mode
- SGI
- Non-Greenfield STAs Present
- OBSS Non-HT STAs Present
- Non-HT OBSS
- 40 MHz Tolerant
- LDPC
- Tx Channel Width

- Rx Channel Width
- PCO
- Greenfield Supported
- Tx STBC
- Rx STBC
- SM Power Save
- Dual Beacon
- Dual CTS Protection

You can get a quick definition or explanation of any of these terms simply by enabling Bubble Help by clicking  in the menu bar. Once the Bubble Help is enabled, you can simply mouse over the name of any of the column to get a tool tip for it.

What 802.11n Features Are Not Used on an AP or STA?

Numerous 802.11n-capable APs and STAs are now commercially available in the market by different vendors. Since some 802.11n features are mandatory and some are optional, according to the IEEE, it is important that you have a clear idea about all the 802.11n devices that are deployed on your network. First of all, you may want to know what 802.11n features are supported or NOT supported by your 802.11n devices.

To find out what 802.11n features are used on your 802.11n APs or STAs:

- 1) Open the WiFi Tools screen by clicking .
- 2) Select the Efficiency tool. See Figure 10-3.

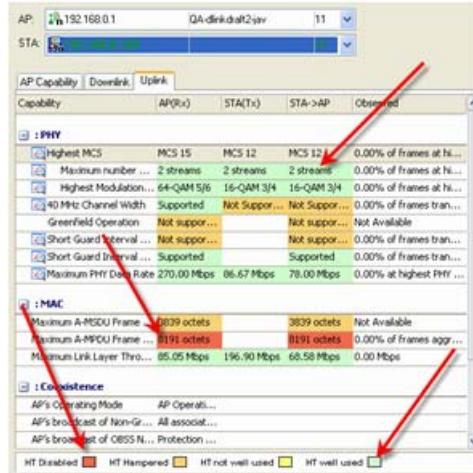


Figure 10-3: WiFi Tools>Efficiency screen

- 3) From the Efficiency screen, select an AP or STA of interest.

The Efficiency screen provides detailed description of all 802.11n features in three categories: PHY, MAC, and Coexistence. For instructions on how to use the Efficiency screen, see “802.11n Efficiency” on page 256.

What Happens If a Particular 802.11n Feature Is (Not) Used?

All 802.11n features will have some impact on the legacy network.

To find out how your network would be impacted due to the use or non-use of a certain 802.11n feature:

- 1) Open the WiFi Tools>Efficiency screen.
- 2) Use the AirMagnet 802.11n Learning Assistant feature which provides detailed explanation of each of the key 802.11n features, its advantages and disadvantages, of using or not using each of these features in plain, straightforward language. See Figure 10-4.

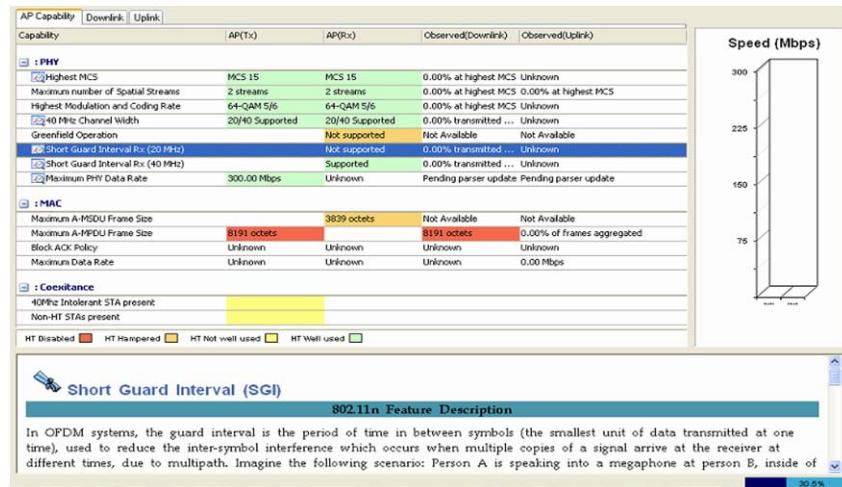


Figure 10-4: AirMagnet 802.11n Learning Assistant (Efficiency)

How Much Traffic Is Sent Using 40-MHZ Channel Width?

The 802.11n protocol supports both 20-MHz and 40-MHz channels. The latter adds more efficiency to network performance.

To find out how much traffic is sent using the 40-MHz channel width:

- 1) Open the WiFi Tools screen.
- 2) Click the Analysis tool.
- 3) Select an AP and a STA.
- 4) Select 20/40 Stats. See Figure 10-5.

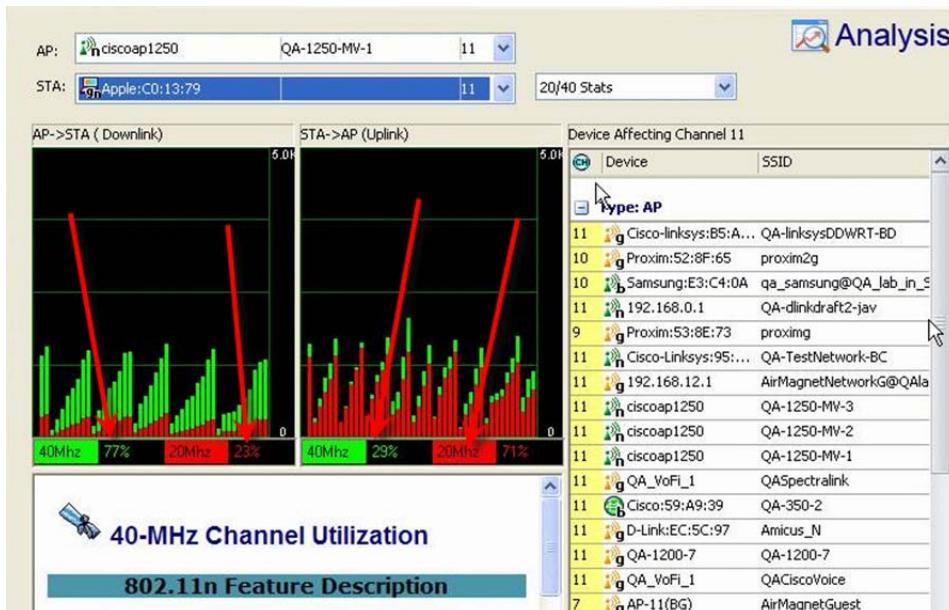


Figure 10-5: Viewing 20-/40-MHz Channel transmission data

The Analysis screen displays the percentage (%) of 20- or 40-MHz traffic between the selected AP and STA. It also provides statistics on SGI, A-MPDU, MCS Index, PHY Data Rate Analysis, etc. For more information, see “802.11n Analysis” on page 260.

What Channel Settings Should I Use If I Have a New AP?

More APs will be added onto the network as your employees’ networking need increases. In an already congested network, you need to know the optimal channel that is available before installing a new AP on the network.

To find out which channel is the best for a new AP:

- 1) Open the Channel screen.
- 2) Then click the Occupancy tab. See Figure 10-6.

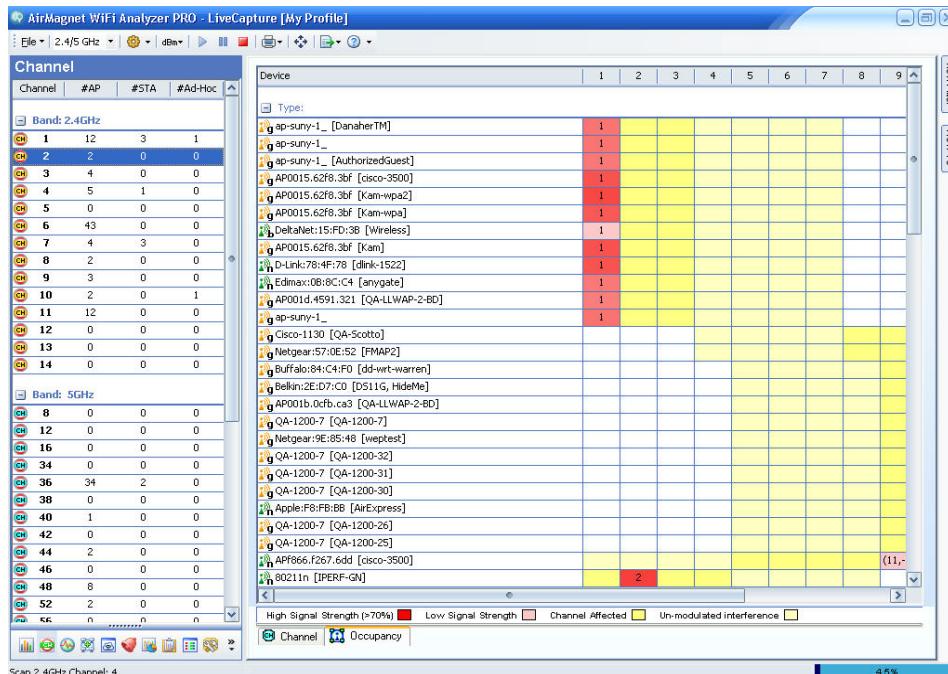


Figure 10-6: Viewing network channel occupancy

The Channel/Occupancy screen provides a bird's eye view of the RF spectrum usage of the network. It shows the center frequency and modulated and un-modulated spectrum usage. You can easily visualize the occupied and/or unoccupied channels. It provide vital information needed for making well-informed decision when planning for new network deployments or enhancement of existing installations.

The occupancy status of all the available channels shown on the Channel/Occupancy screen help the user to easily decide which channels to choose for new APs to be deployed on a congested network. As a rule of thumb, the user should choose those unused channels and avoid those congested ones.

How to Find Out the Maximum Throughput of an Installed AP?

You can find out the maximum throughput of any AP installed on your network using the Throughput/Iperf tool on AirMagnet WiFi Analyzer's WiFi Tools screen.

To find out the maximum throughput of an AP:

- 1) From WiFi Tools screen, click the Throughput/Iperf tool. Select an AP.
- 2) Specify the length of the Test Period, e.g., 120.
- 3) Select a Chart Type, e.g., PHY Data Rate.
- 4) Make sure to check the Iperf Performance Test check box.
- 5) Select TCP or UDP and specify the Server and Port.
- 6) Check the Up/Downlink check box.
- 7) Click . See Figure 10-7.

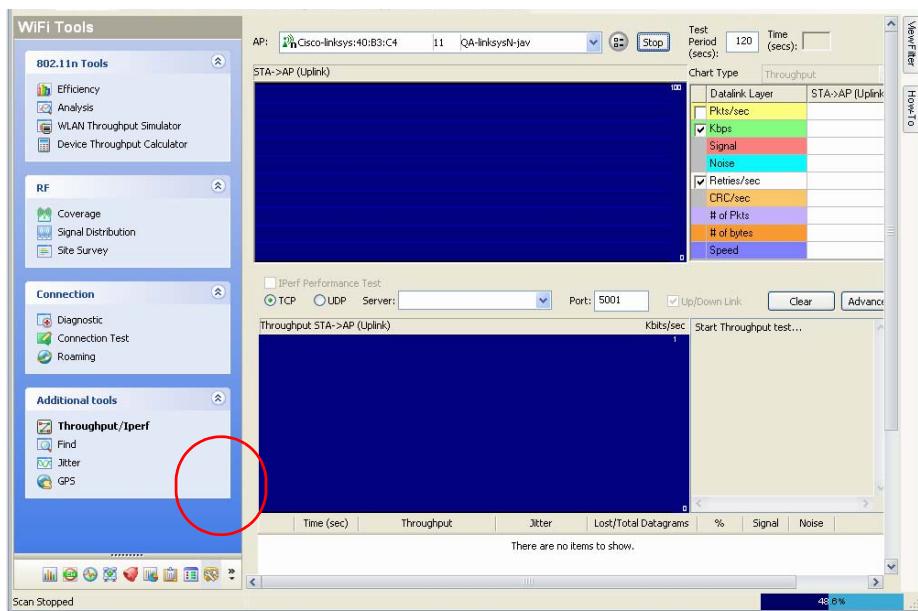


Figure 10-7: Testing maximum network throughput

As seen from Figure 10-7, the Throughput/Iperf screen shows both the up- and downlink throughput for the selected AP. It allows you to test the network performance using either the TCP or the UDP protocol. It shows various factors such as signal strength, noise level, retries, and CRC errors that may impact your network throughput. For more information, see “Analyzing Network Bandwidth and Throughput with Iperf” on page 299.

Why Am I Not Getting the Expected Throughput from an AP?

Network throughput is expected by various factors on the network. As a result, your network throughput may fluctuate with the changing dynamics of the network.

To find out why you are not getting the expected throughput from an AP:

- 1) Open the Efficiency screen. See Figure 10-8.

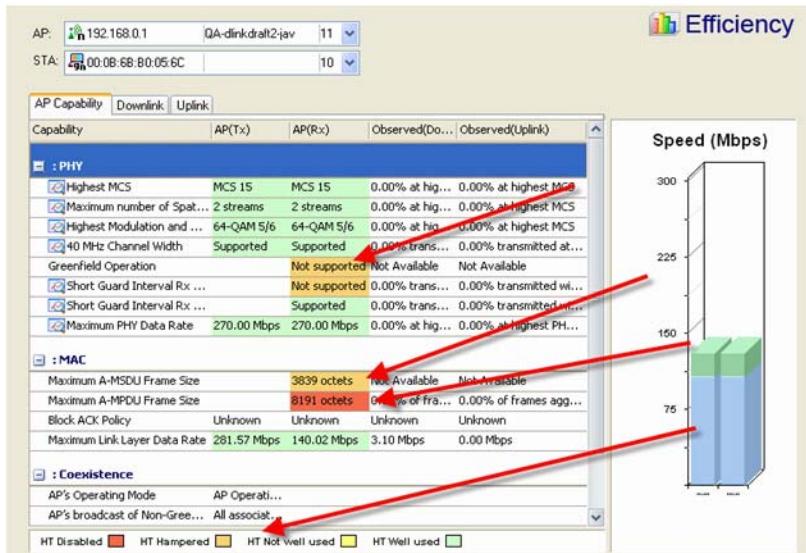


Figure 10-8: Viewing 802.11n network efficiency

The Efficiency tool enables you to analyze the transactions between APs and STAs. Along the bottom of the screen are color legends that tell you why expected throughput is not achieved. Based on this information, you can rectify the situation by enabling the settings on your 802.11n devices to take full advantage of 802.11n devices' HT capabilities. For more information, see "802.11n Efficiency" on page 256.

- 2) Open the Analysis screen.
- 3) Select an AP and a STA.
- 4) Select 20/40 Stats. See Figure 10-9.

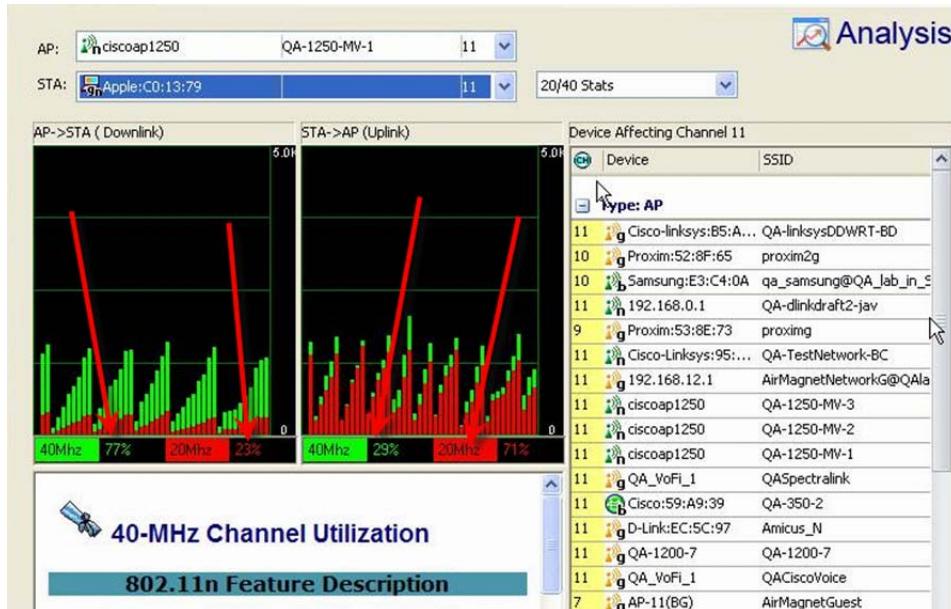


Figure 10-9: Viewing 20-/40-MHz channel usage

Figure 10-9 indicates the percentage of traffic being sent at 20 MHz and at 40 MHz. It can detect if utilization at higher MCS rate is low. It also indicate low signal-to-noise ratio in noisy RF environments or over greater distance between AP and STA.

What Is the Expected Device Throughput for an AP?

When installing an AP on your network, you may want to know the level of throughput you can expect from the AP before you put to work. This is where AirMagnet WiFi Analyzer's Device Throughput Calculator comes into play.

To test the expected device throughput of an AP:

- 5) Open AirMagnet WiFi Analyzer's Device Throughput Calculator screen.

- 6) Set the parameters you want to use on the AP and click Calculate.
- 7) Repeat Step 6, using different parameters. See Figure 10-10.

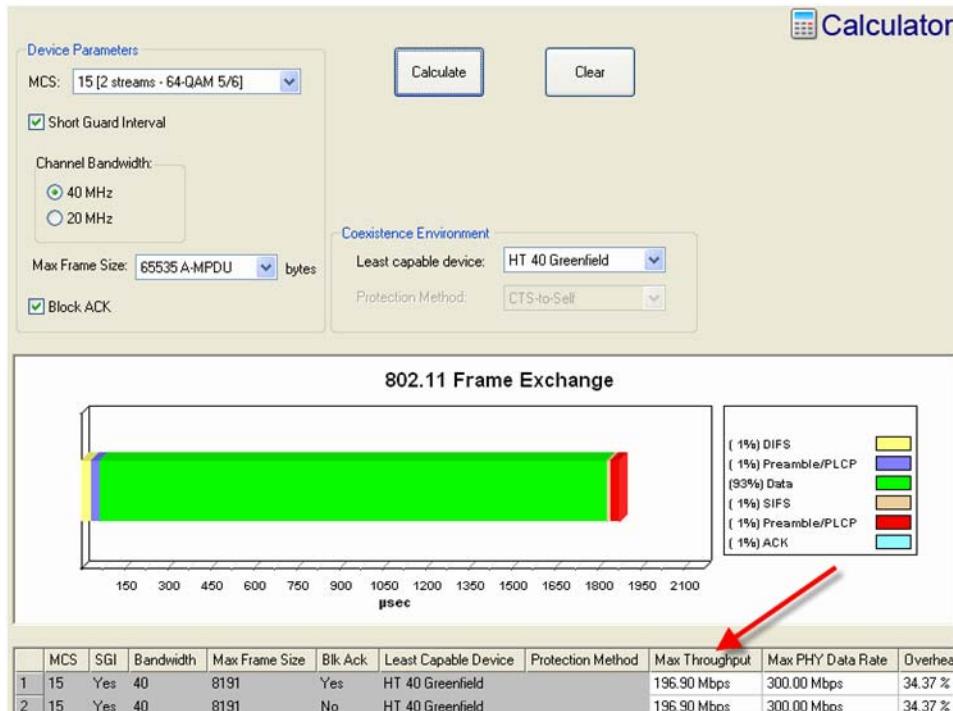


Figure 10-10: Testing device throughput

Each time you click Calculate, AirMagnet WiFi Analyzer will calculate the theoretical throughput level you can expect from an AP using the same parameters. This can help you set realistic expectations for a newly deployed AP because the calculations are based on parameters you (the user) specified on the AP. The Device Throughput Calculator also indicates the overhead incurred for supporting legacy devices.

What Should Be Taken into Consideration When Configuring New APs?

Before configuring new APs, you may want to make sure that all key 802.11n capabilities are properly configured on your APs before putting them on the network. AirMagnet WiFi Analyzer's Device Throughput Calculator screen lists all important parameters that must be taken into consideration when purchasing or installing APs.

To find out the important capabilities of 802.11n APs:

- 1) Open the Device Throughput Calculator screen.
- 2) Look through all the parameters on the Device Throughput Calculator screen, as highlighted in Figure 10-11.



Figure 10-11: Important 802.11 capabilities

All the fields highlighted in Figure 10-11 are considered very important for the 802.11n network and must be taken into consideration when purchasing or configuring 802.11n AP. They help you make informed decisions to maximize throughput of your 802.11n devices or networks.

What Change in Network Throughput Is Expected When Deploying New APs and/or STAs on the Network?

Your network throughput will certainly be affected each time new devices are added. Therefore, you may want to simulate the RF conditions when and after different devices (i.e., APs, STAs, etc.) are added to your network. The simulation results will tell you ahead of time what you should pursue and/or what you should avoid when installing new APs and STAs. You can do all this right from AirMagnet WiFi Analyzer's Network Throughput Simulator tool screen.

To simulate changes in network throughput:

- 1) From the WiFi Tools screen, click the WLAN Throughput Simulator tool.
- 2) Select the frequency band of interest by clicking the 2.4 GHz or 5 GHz radio button.
- 3) From the menubar, click Add Device and select an option from the drop-down menu.
- 4) Associate STAs with APs by clicking an STA and then the down arrow next to it to select an AP to associate with, as shown in Figure 10-12.

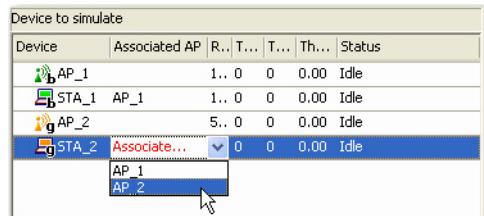


Figure 10-12: Associating station with AP

- 5) Repeat Step 3 to make sure that all APs and STAs are associated.

Note that every STA needs to be associated with an AP in order to run WLAN throughput simulation.

- 6) Click the Run button in the upper-right corner of the screen. The simulation starts and the results are shown on the screen. See Figure 10-13.

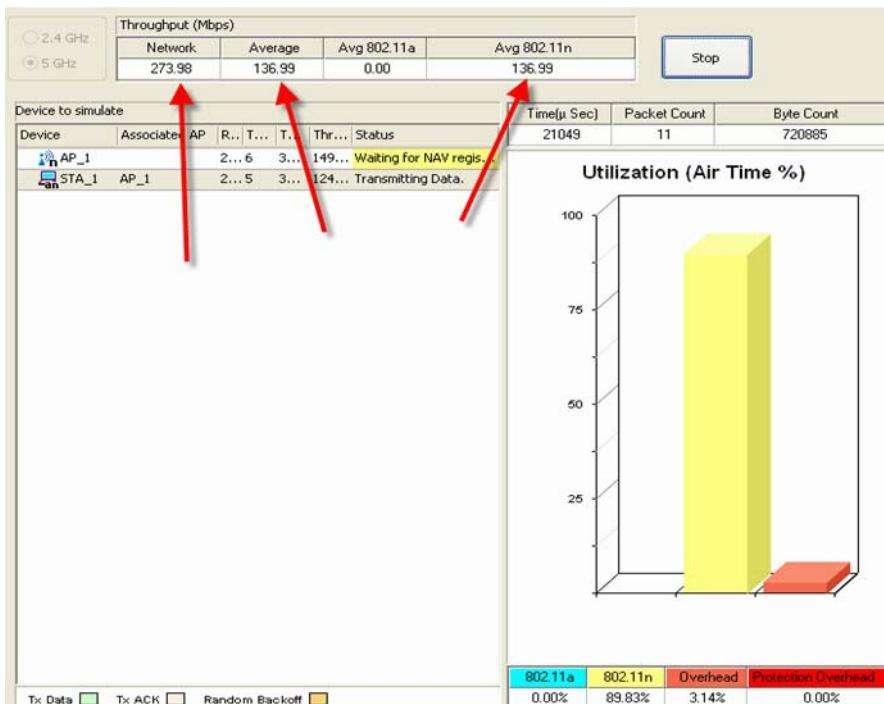


Figure 10-13: Viewing results of network throughput simulation

The Network Throughput Simulator allows you to simulate WLAN throughput under various user-defined conditions. You can simulate the impact on the network caused by addition of new APs and/or STAs by associating STAs with simulated APs or real APs that are installed on

the network. The Simulator will generate the results and make them available on the screen in no time, as shown in Figure 10-13.

How to Find Out the Network Throughput Between an AP and a STA?

Oftentimes, you may want to know the real-time network throughput between a certain AP and STA. AirMagnet WiFi Analyzer's Efficiency tool makes such information readily available on your desktop.

To find the real-time network throughput data between an AP and STA:

- 1) Open the WiFi Tools screen.
- 2) Click the Efficiency tool.
- 3) Select the AP and STA of interest.
- 4) Observe the live data on the screen. See Figure 10-14.

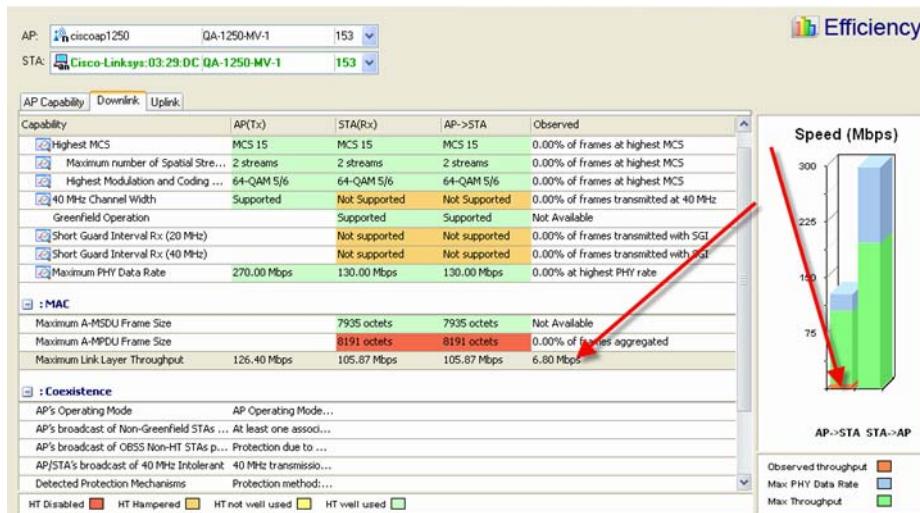


Figure 10-14: Viewing real-time AP-STA network throughput

As shown in Figure 10-14, the Efficiency screen provides comprehensive data about the throughput between a selected AP and STA in terms of Max PHY Data Rate, Max Link Layer Throughput, and Current Data Rate. It shows AP capabilities and uplink and downlink throughput statistics in the conversation between the AP and the STA.

Note: The Observed (Downlink) and Observed (Uplink) columns in Figure 10-14 show any of the following depending on the situation:

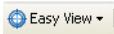
- When an AP-STA pair which is known to be associated by AirMagnet WiFi Analyzer, the Observed column contains metrics which are specific to the AP-STA association (i.e., only displays traffic measurements made between the combination of the AP and STA).
- When an AP-STA pair is not known to be associated, the Observed column contains metrics which are independent of any association (i.e., all outgoing [data] traffic metrics from the AP and STA are displayed).
- When an AP and “any” STA are selected, the APs outgoing (data) traffic metrics are used and the STA (and subsequently Uplink) metrics are zero (i.e., no traffic is indicated). In this case, the AP’s capability is compared against a “virtual” STA, which has parameters defined at the limit of the 802.11n specification.

How Can I Know If My 802.11n AP is Associated with Any Legacy Devices?

Even though 802.11n APs are backward compatible to legacy devices, care must be taken to make sure that protection mechanisms are used on the AP in order to minimize or avoid the potential negative impact that the 802.11n network may cause on legacy devices or networks. Towards that end, network administrators must know if their 802.11n APs are associating with legacy devices. And they can do this fairly easily using AirMagnet WiFi Analyzer.

To know if your 802.11n APs are associating with legacy devices?

- 1) From AirMagnet WiFi Analyzer, do one of the following:

- Open the Start screen, click  Easy View ▾, and select View by 802.11n from the drop-down menu. See Figure 10-15.

Type	Device	MAC	Operating Mode
.11:n			
STA	10 00:0E:8E:15:94:D6	00:0E:8E:15:94:D6	All STAs HT
AP	11 192.168.0.1	00:1B:11:62:A6:F0	One or more non-HT STAs associated
AP	11 Apple:FA:56:D7	00:19:E3:FA:56:D7	Non-HT STAs present
STA	10 Wistron Neweb:B0:0...	00:0B:6B:B0:0E:99	All STAs HT
STA	10 Wistron Neweb:B0:0...	00:0B:6B:B0:0E:74	All STAs HT
STA	10 Wistron Neweb:B0:0...	00:0B:6B:B0:0E:F8	All STAs HT
STA	10 Wistron Neweb:B0:0...	00:0B:6B:B0:0E:BC	All STAs HT
STA	10 Intel:BB:28:A5	00:13:E8:BB:28:A5	All STAs HT

Figure 10-15: 802.11n AP associated with legacy devices

- Open the Infrastructure screen, click AP List, and expand an 802.11n AP that has STAs associated to it. See Figure 10-16.

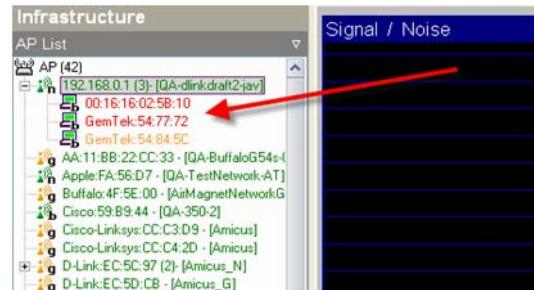


Figure 10-16: 802.11n AP associated with legacy STAs

How Much Overhead Does an 802.11n AP Use to Support Legacy Devices?

When 802.11n APs are installed within close proximity to legacy networks, the former must use (protection) overhead in order to minimize their impact on legacy devices. The Network Throughput Simulator enables you to easily find out the percentage of the frames that is used for overhead by 802.11n APs in an environment where they coexist with legacy devices.

To find out the overhead used by an 802.11n AP:

- 1) Open the WiFi Tool screen.
- 2) Click the Network Throughput Simulator, select 2.4 GHz or 5 GHz, and click Run. See Figure 10-17.

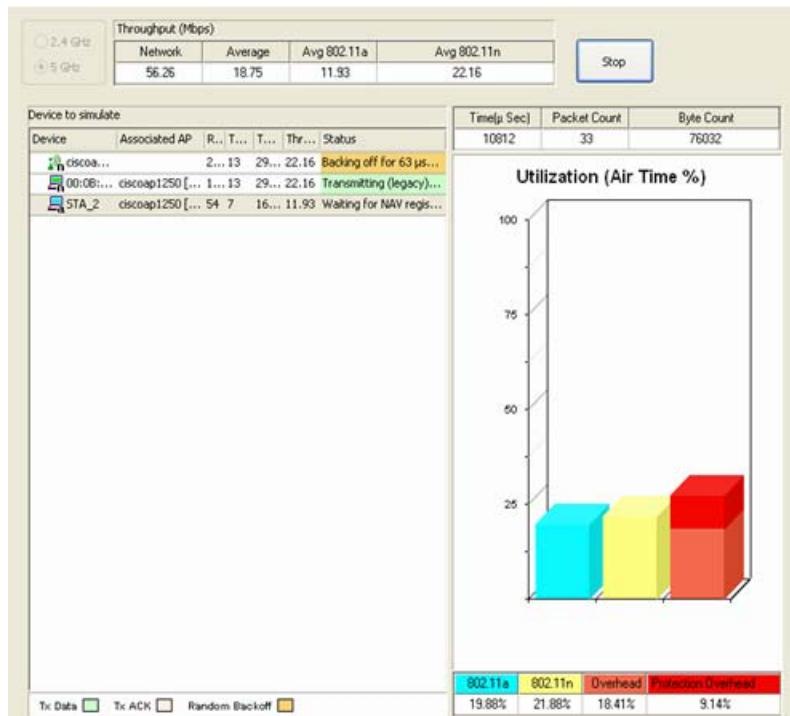


Figure 10-17: Overhead used in support of legacy devices

The Simulator allows you to simulate WLAN throughput under user-defined conditions. It allows you to visualize the overhead used by 802.11n APs in support of legacy devices as well as overhead used to protect 802.11n transmission from legacy devices.

How Will Associated Legacy Devices Decrease 802.11n Device Throughput?

The throughput of 802.11n devices will decrease in the presence of legacy devices. This is because that 802.11n devices have to use certain protection mechanisms in order to protect legacy devices from the potential detrimental effect that 802.11n transmissions may have on legacy devices. The Device Throughput Calculator provides instant feedback on how 802.11n device throughput will be affected with different least capable devices being used.

To find out how associated legacy devices decrease 802.11n device throughput:

- 3) Open the Device Throughput Calculator screen.
- 4) For (Coexistence Environment) Least Capable Device, select 802.11b and select a Protection Method.
- 5) Click Calculate.
- 6) Repeat Steps 3 through 4 to calculate the impact in various conditions. See Figure 10-18.

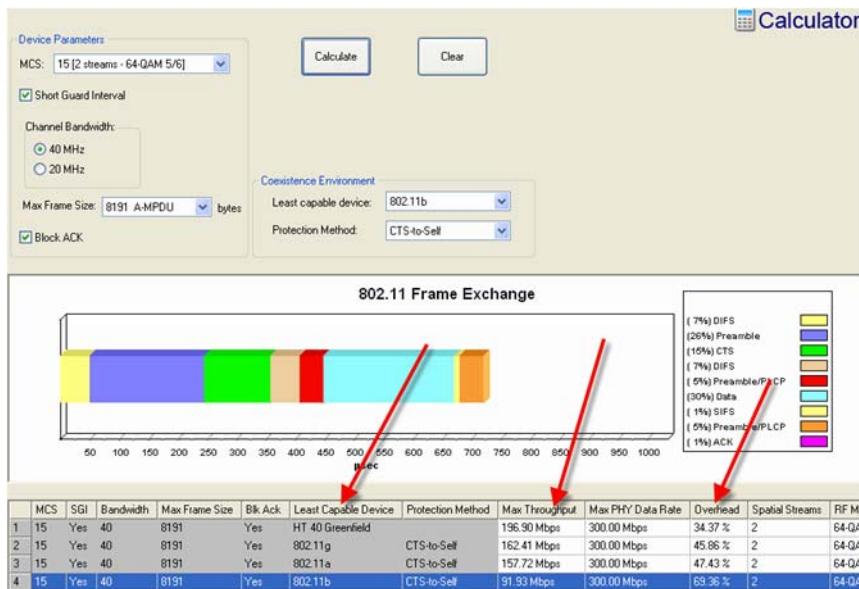


Figure 10-18: Impact of legacy device on 802.11n throughput

The Device Throughput Calculator tool screen allows you to calculate 802.11n device throughput, taking into consideration of those least capable devices on the network. It also shows the increase in overhead to accommodate for legacy devices.

How Many Legacy APs Can be Added to an 802.11n Network?

Despite the fact that the final ratification of the 802.11n protocol is around the corner, the reality facing the wireless networking professionals is that legacy networks and devices are not going to disappear overnight. 802.11n and legacy devices and networks may have to coexist for years to come. So network professionals must and should know how many legacy APs can be added to an 802.11n network, while still maintaining the latter's throughput up to a certain level. You can get this data easily using AirMagnet WiFi Analyzer's Network Throughput Simulator.

To find out how many legacy APs can be added to an 802.11n network?

- 1) Open the Network Throughput Simulator tool screen.
- 2) Select 2.4 GHz or 5 GHz, and click Run. See Figure 10-19.

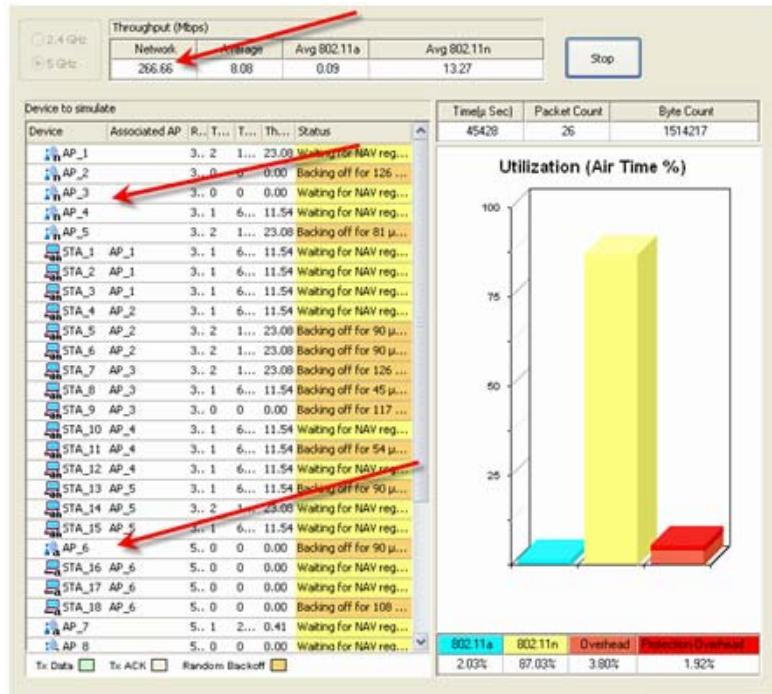


Figure 10-19: Determining number of legacy APs on 802.11n WLAN

The Network Throughput Simulator tool calculates the throughput values at both the node and network levels, taking into full consideration of least capable devices in the network. It also simulates the impact on the 802.11n network caused by the addition of legacy APs, which can be easily visualized as more and more legacy devices are being added.

How Will 802.11n STAs Affect an Existing 802.11a Network?

When 802.11n STAs are added to an 802.11a network, the overall throughput of the 802.11a network will increase, since they both support some of the latest 802.11 network technologies. This can be seen easily using the Network Throughput Simulator tool.

To find out the positive impact of 802.11n STAs on an existing 802.11g network:

- 1) Open the Network Throughput Simulator tool screen.
- 2) Run a few simulations by associating 802.11a stations with an 802.11g network and notice the network throughput. See Figure 10-20.

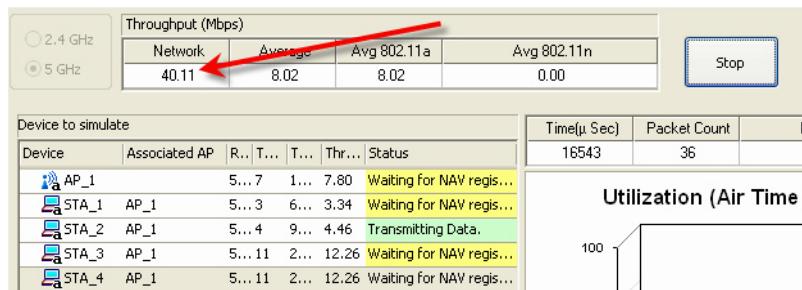


Figure 10-20: 802.11g network associated with 802.11a STAs

- 3) Run a few simulations by associating 802.11a/n stations with the same 802.11g network and notice the network throughput. See Figure 10-21.



Figure 10-21: 802.11g network associating with 802.11a/n STAs

As shown in Figure 10-20 and 10-21, the 802.11a network throughput was 40.11 Mbps when associating with 802.11a STAs. However, that number increased to 47.03 Mbps when association with 802.11n STAs. That's roughly an increase of 17%.

Chapter 11: Integration with Fluke INA

Chapter Summary

This chapter discusses some special issues involving the integration with Fluke INA. It covers the following topics:

- Fluke Networks OptiView Integrated Network Analyzer
- Installation and Licensing Procedures
- Software Usability, etc.

Fluke Networks OptiView® Integrated Network Analyzer

Fluke Networks' OptiView® Integrated Network Analyzer is a powerful, portable, all-in-one network analysis solution that provides the vision and capabilities to help you deploy new technologies and applications, manage and validate infrastructure changes, solve network and application performance issues, as well as secure the network from internal threats.

Today's networks may be more stable, but certainly not static. Management and users are constantly demanding new technologies, new services, and better performance which inevitably require infrastructure changes, deployment of new, emerging applications, and dealing with security issues. In the midst of all this, you need to control IT costs and minimize disruption to your organization. That means you need to be able to clearly see all aspects of your network to accurately assess the overall impact. The more your network changes, the more you will need to improve visibility and control.

The OptiView analyzer improves your visibility into your 10/100/1000 copper and optical networks through:

- Advanced discovery techniques – Automatically begins to discover devices on the network e.g., switches, routers, wireless controllers, VoIP devices. IT staff can immediately see

what's on the network and problems associated with those devices.

- Traffic analysis – Provides real-time statistics for traffic on the wire enabling the user to understand how the network resources are being used.
- Application traffic analysis – Automatically discovers all IPv4 and IPv6 protocols and sub protocols from layer 1 to 7, enabling IT staff to identify applications utilizing link bandwidth as well as top hosts and conversations.

You can expand the power of the OptiView Analyzer by adding visibility into your local 802.11abgn networks with AirMagnet® WiFi Analyzer PRO and Survey PRO products.

Figure 11-1 shows the Fluke Networks OptiView INA user interface showing AirMagnet WiFi Analyzer Start page.



Figure 11-1: AirMagnet WiFi Analyzer on Fluke OptiView

Software Installation

This section discusses the installation of AirMagnet WiFi Analyzer on Fluke Networks OptiView Integrated Network Analyzer. It specifies the wireless network adapters that are supported and the procedures for installing the software.

Supported Wireless Network Adapters

The integration of AirMagnet WiFi Analyzer with Fluke Networks OptiView Integrated Network Analyzer supports the following wireless network adapters:

- AirMagnet 802.11a/b/g/n Wireless PC card
- Fluke Networks 802.11 a/b/g
- Fluke Networks 802.11 a/b/g/n

Prior to installing AirMagnet WiFi Analyzer, make sure that either of the above supported wireless network adapters has already been installed and inserted in the card slot on the Fluke Networks OptiView INA. By default, the AirMagnet WiFi Analyzer installer automatically ties the software license file to the supported wireless network adapter used at the time of installation.

Software Usability

This section discusses the customizations of the AirMagnet WiFi Analyzer user interface that are specific to the integration with the Fluke Networks OptiView INA. The customizations are required in order to optimize the performance of AirMagnet WiFi Analyzer on the Fluke Networks OptiView INA.

Using Tap and Hold

This action is required on certain screens when the user wants to select an object (e.g., an entry on the Start screen) to bring up a pop-up menu, which provides a list of menus. It is equivalent to the right-click of an object on the screen of the AirMagnet application when it is running on a laptop PC. Figure 11-2 illustrates pop-up list menu when the user tap and hold on a entry on the Start screen.

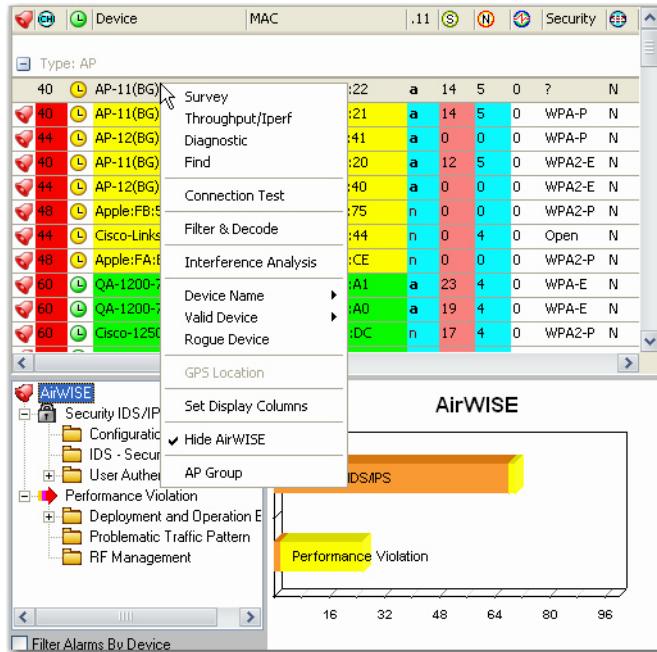


Figure 11-2: Using Tap and Hold to open the pop-up menu

Using the Full Screen/Restore Screen Button

Because of the size of the Fluke Networks OptiView INA, not all data can be shown on the user interface. This button is intended to give the user the flexibility to collapse or expand the left panel of the AirMagnet WiFi Analyzer user interface when desired. By default, the application shows both the left and right panels. The user can toggle between the screen options by clicking this button. Figures 11-3 and 11-4 show the two different screen options.

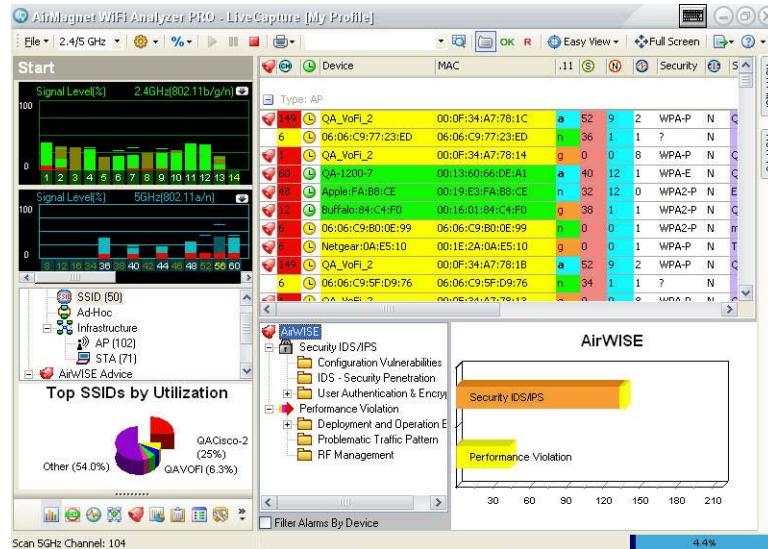


Figure 11-3: The regular user interface

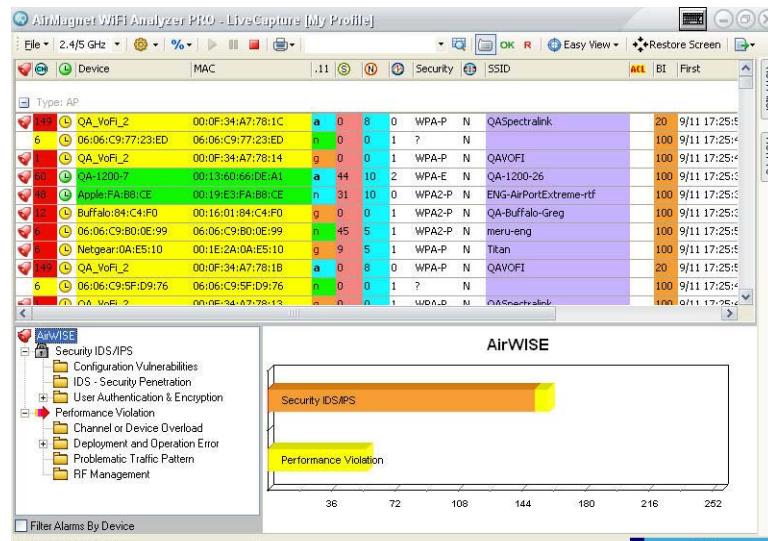


Figure 11-4: The full-screen user interface

Using the MyTTouch Soft Keyboard

The MyTTouch Soft Keyboard allows the user to make text entries in text boxes to search for items of interest on the screen. By default, this button is minimized and docked on the title bar in the upper-right corner of the user interface, as shown in Figures 11-3 and 11-4. The user can activate it by clicking the button. Figure 11-5 show the soft keyboard that is activated.

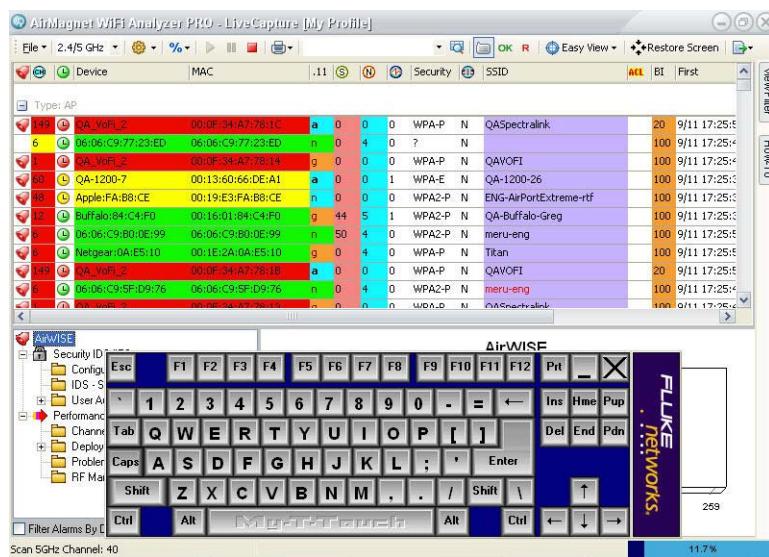


Figure 11-5: The activated soft keyboard

The user can restore the soft keyboard to its original state by clicking the X sign in its upper-right hand corner.

Miscellaneous UI Changes

When integrated with Fluke Networks OptiView INA, certain options on AirMagnet WiFi Analyzer user interface may have been optimized to accommodate for the screen resolution of the device.

Chapter 12: Analyzing WiFi Roaming

Viewing Wireless Roaming

Users can access the Roaming Detail screen by clicking the **Roaming Analysis** button located in the Navigation Bar.

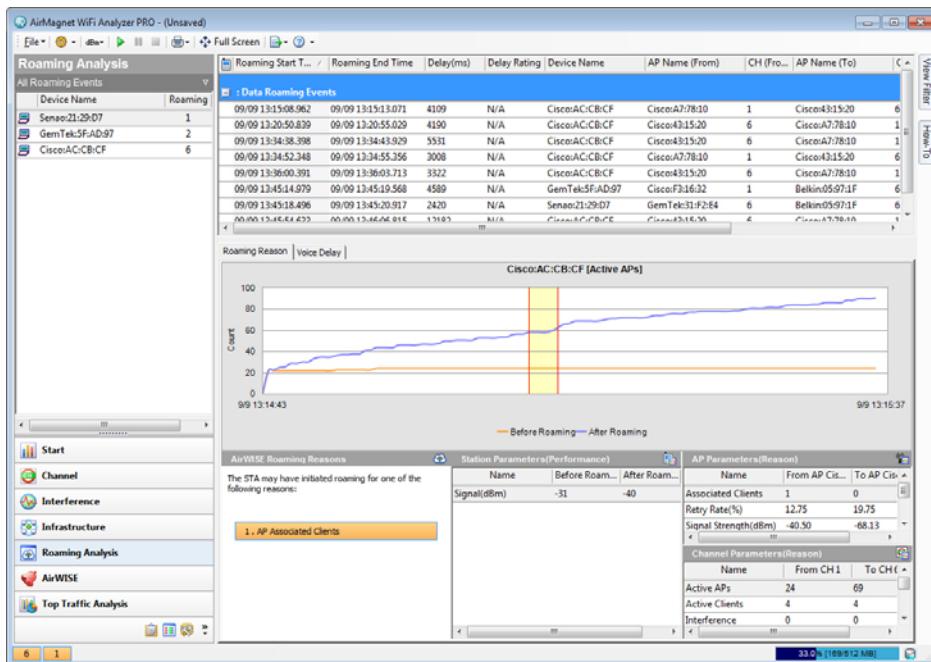


Figure 12-1: Roaming Details

As seen in Figure 12-1, the Roaming Analysis screen is divided into two major panes: the Device Listing (on the left) and the Roaming Details section (on the right). These regions are described in more detail in the following sections.

Device Listing

By default, the Device Listing pane displays all devices that experienced roaming instances while the application was actively scanning. This listing can include standard wireless stations as well as VoFi phones, depending on the devices present in the environment. See Figure 12-2.

Roaming Analysis	
All Roaming Events	
Device Name	Roaming
Sena:21:29:D7	1
GemTek:5F:AD:97	2
Cisco:AC:CB:CF	6

Figure 12-2: Device Listing Pane

As shown above, the information is laid out in a table that provides additional details about each device, as described in Table 12-1.

Table 12-1: Device Listing Data

Column	Description
(Icon)	The first column simply displays an icon that corresponds to the type of device detected.
Device Name / Channel	By default, this column displays the specified name of the device. If no name has been entered, the name is generated using a combination of the device vendor name and the last six digits of its MAC address. Note that when viewing roaming by channel, this column simply indicates the channel number.
Roaming	This field allows the user to quickly assess the number of instances a given device or channel experienced roaming. Larger numbers could indicate that a device is experiencing connection issues and may require additional analysis, as described in “Analyzing Roaming Details” on page 383.

Table 12-1: Device Listing Data

Column	Description
Roaming In/Out	These columns are only present when viewing the Device Listing by AP or Channel. The number provided for Roaming In indicates the total number of times that devices were found to roam to the AP or Channel indicated, whereas the Out column represents the number of times devices roamed away. Channels or APs that have a large number of devices roaming away from them may be indicative of insufficient signal coverage in that area.

The columns present in the table may vary depending on the view option selected in the Roaming Event Filter, described below.

Roaming Event Filter

In order to easily assess the data of interest, users can adjust the information displayed in the Device Listing by using the drop-down filter provided at the top of the pane. See Figure 12-3.

**Figure 12-3: Filter Options**

Note that since the columns provided vary depending on the selection made, the user can tailor the display to provide exactly the data required:

- **All Roaming Events** – The default option, this selection provides a broad overview of all devices experiencing

roaming and the number of instances detected. This listing can include both standard wireless stations as well as VoFi phones.

- **List by Station** – This option displays only wireless stations, thereby filtering out phones. This can be useful for environments where voice traffic is already considered sufficient for the needs of the users present but data traffic appears to be suffering.
- **List by Phone** – The opposite of List by Station, this filter ignores instances of data roaming and allows the user to focus entirely on VoFi phone roaming.
- **List by AP** – This selection lists all APs that experienced devices roaming either to or away from them as well as the number of instances detected for each. APs that have a large number of roams could be overloaded, indicating that additional infrastructure may be needed in the region.
- **List by Channel** – The final filter allows the user to view the roaming instances divided up into the individual channels detected. As with the List by AP selection, the user can view the number of roams both to and away from each channel; large numbers of roams away from a channel could indicate that there is too much interference present at that particular frequency range.

Roaming Pie Chart

The lower portion of the Device Listing provides a pie chart display of the Voice Delay present in the VoFi roaming instances detected. This value measures the time that passes between the last packet transmitted via the initial AP and the first packet transmitted via the new AP (i.e., the AP to which the phone roamed). Voice Delay is a major indicator of the quality of a VoFi conversation; higher delay can cause lags in the communication between the two phones, and ultimately may result in dropped calls.

Analyzing Roaming Details

The majority of the Roaming Analysis screen is occupied by the Roaming Details pane, which provides detailed data based on the user's selections in the Device Listing. After the user has made a selection from the left-hand pane (by clicking a device or channel of interest), the information in the Roaming Details section refreshes to reflect data specific to the selection made. See Figure 12-4.

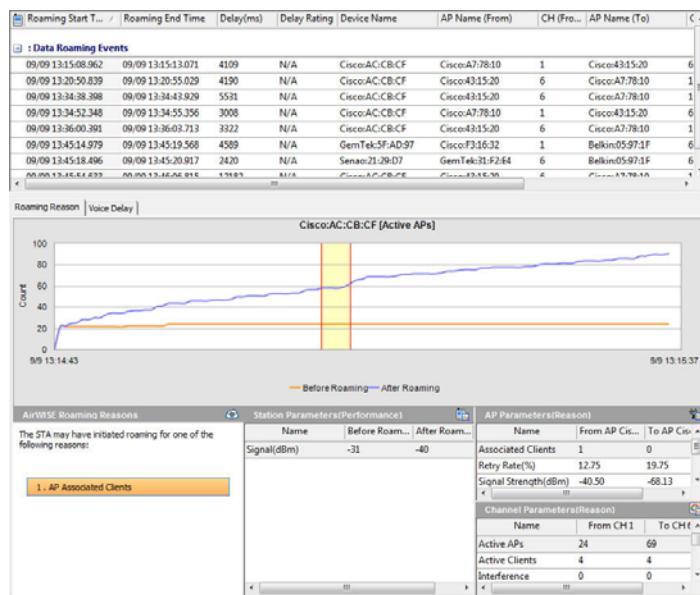


Figure 12-4: Detailed Roaming Data

Due to the amount of information available, the Roaming Details pane is divided up into three major sections: the Roaming Instance Table (across the top), Roaming Reasons (the first tab selected from the bottom), and Voice Delay Information (the second tab). Each of these is described in greater detail in the following sections.

Roaming Instance Table

The top portion of the pane contains a table that displays all instances of roaming detected for the device selected. Depending on the device, these instances could be either Data or Voice Roaming Events. To view roaming data for a specific event, simply click the desired selection in the table and the other portions of the screen will refresh accordingly. See Figure 12-5.

Roaming Start T...	Roaming End Time	Delay(ms)	Delay Rating	Device Name	AP Name (From)	CH (Fro...	AP Name (To)	C
: Data Roaming Events								
09/09 13:15:08.962	09/09 13:15:13.071	4109	N/A	CiscoAC:CB:CF	Cisco:A7:7B:10	1	Cisco:43:15:20	6
09/09 13:20:50.839	09/09 13:20:55.029	4190	N/A	CiscoAC:CB:CF	Cisco:43:15:20	6	Cisco:A7:7B:10	1
09/09 13:34:38.398	09/09 13:34:43.929	5531	N/A	CiscoAC:CB:CF	Cisco:43:15:20	6	Cisco:A7:7B:10	1
09/09 13:24:52.348	09/09 13:24:55.266	3008	N/A	CiscoAC:CB:CF	Cisco:A7:7B:10	1	Cisco:43:15:20	6
09/09 13:36:00.391	09/09 13:36:03.713	3322	N/A	CiscoAC:CB:CF	Cisco:43:15:20	6	Cisco:A7:7B:10	1
09/09 13:45:14.979	09/09 13:45:19.568	4589	N/A	GemTek:5F:AD:97	Cisco:F3:16:32	1	Belkin:05:97:1F	6
09/09 13:45:18.496	09/09 13:45:20.917	2420	N/A	Sennar:21:29:07	GemTel:31:F2:E4	6	Belkin:05:97:1F	6
09/09 13:45:41.433	09/09 13:46:06.816	13193	N/A	CiscoAC:CB:CE	Cisco:43:15:20	6	Cisco:A7:7B:10	1

Figure 12-5: Roaming Table Selection

The columns in the table contain a variety of various data for both VoFi and data roaming instances, as described in Table 12-2.

Table 12-2: Roaming Instance Table Columns

Column	Description
(Icon)	The icons in the first column indicate the type of device associated with each event; data roams are indicated by a computer icon, whereas VoFi roams display a phone.
Roaming Start/End Time	The times at which the device started and finished the roaming process.
Delay (ms)	The delay measured from the time at which the last packet was transmitted to the original AP to the time at which the first packet was transmitted to the new AP.

Table 12-2: Roaming Instance Table Columns

Column	Description
Rating	The icons provided in the Rating column indicate whether the device's wireless service improved as a result of the roam. This is calculated based on the delay value; by default, a delay longer than 500ms indicates a bad roam, as the device took too long to establish a new connection and could have interrupted any calls or data transactions that were processing at the time of the roam. <i>Note: The Rating column only applies to VoFi calls; data roams will simply display "N/A".</i>
Device Name	The name of the roaming device.
AP Name (From/To)	These columns indicate the names of the APs involved in the roam (i.e., both the original AP and the one to which the device roamed).
CH (From/To)	These columns display the original channel (before roaming) and the final one (after roaming).
Signal (From/To)	These columns display the signal strength detected both before and after the roam.
MOS (From/To)	These fields provide the MOS score for the call both prior to and after roaming. <i>Note: The MOS columns pertain only to VoFi calls and will display "N/A" for data instances.</i>

Determining the Roaming Cause

By default, when the user first navigates to the Roaming Analysis screen, the Roaming Reason tab is displayed. This selection provides a variety of different sub-panes that help the user identify the reason for the selected roam.

Roaming Reasons

Selecting the Roaming Reason tab in the bottom-left portion of the screen allows the user to identify the potential reasons for the selected roaming instance. This changes the Roaming Chart, Delay, and Decodes portions of the screen. See Figure 12-6.

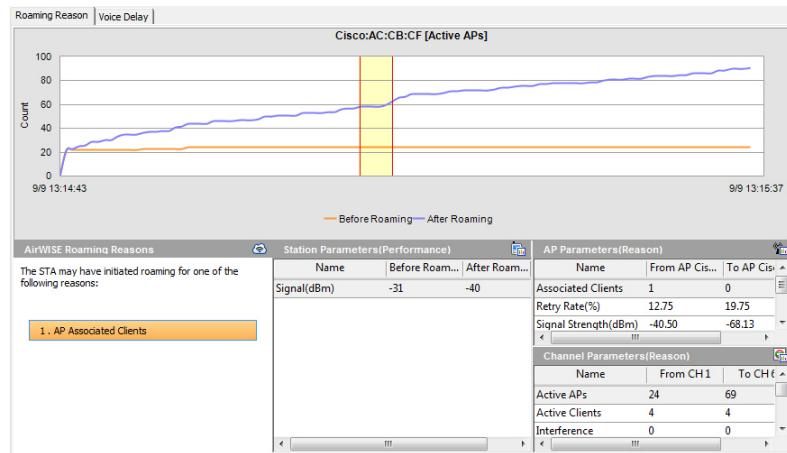


Figure 12-6: Roaming Reason Display

The Roaming Reasons pane in the lower-left lists possible reasons behind the instance of roaming. Clicking these reasons will adjust the chart display to highlight data that can help diagnose the roam.

The type of chart displayed will vary depending on the selection made in the panes across the bottom of the screen. As shown above, when the user clicks one of the links in the Roaming Reasons pane, the chart refreshes accordingly. However, the chart will also update depending on the selection made in the Phone Parameters, AP Parameters, or Channel Parameters panes.

When a selection is made in either of the parameter panes, the chart displays an arrow indicating the call performance before and after the roam.

Each of the parameter panes display data in three basic columns:

- **Before Roam**—The data displayed in the first column corresponds to the call experience prior to the roaming instance.
- **After Roam**—The second column displays data as detected after the roam has completed.
- **Rating**—The final column displays a thumbs-up icon if the category (e.g., MOS, Retry Rate, Jitter, etc.) improved after the roam finished; a thumbs-down will appear if the category suffered as a result of the roam.

This data can help the user identify problems with the user experience during the call process. For example, the roam shown in Figure 2-41 experiences improvements in Retry Rate and CRC Errors (as displayed in the Phone Parameters), but Jitter appears to have increased significantly as a result of the roam. This could indicate that the user would consequently experience added difficulty in maintaining a conversation.

Device Parameters

Immediately to the right of the Roaming Reasons pane, the Device Parameters field will vary depending on the type of roaming instance selected; instances of data roaming will simply display the retry rates, CRC errors, and signal level both before and after the roam. For a VoFi roam, these details will be supplemented by MOS and Jitter information. See Figure 12-7.

Name	Before Roam...	After Roam...
Signal(dBm)	-31	-40

Figure 12-7: Station/Phone Parameters

AP Parameters

When troubleshooting repeated instances of wireless roaming, it can be helpful to identify just how much traffic the APs in the region are handling. The AP Parameters field provides this information, identifying the number of calls and clients serviced by both APs involved in the instance of roaming selected (e.g., the original and final APs). See Figure 12-8.

Name	From AP Cis...	To AP Cis...
Associated Clients	1	0
Retry Rate(%)	12.75	19.75
Signal Strength(dBm)	-40.50	-68.13

Figure 12-8: AP Parameters

As shown above, users can also view the retry rate, signal strength, and utilization before and after the roam. This information can be helpful in identifying whether the roam was justified or not; if the original AP had a low signal level just before the roam, it may be that the station or phone was simply moving away from that region and needed to locate a closer source of wireless connectivity.

Channel Parameters

The Channel Parameters field provides a quick overview of the channels involved in the roam, allowing the user to identify whether a crowded or blocked channel is the root cause. See Figure 12-9.

Name	From CH1	To CH6
Active APs	24	69
Active Clients	4	4
Interference	0	0

Figure 12-9: Channel Parameters

By identifying the number of APs and clients present on the selected channel, users can see whether there were simply too many active devices in the environment at the time of the roam. A large number of wireless clients can cause interference, which could result in poor connection quality. In a similar manner, high levels of noise and utilization could result in reduced bandwidth available for the client's connection.

Voice Delay

The Voice Delay tab will only be available if an instance of VoFi roaming is selected, as its information does not apply to standard data roaming.

The Voice Delay tab provides users with an overview of all data pertaining to VoFi roaming, making it perfect for troubleshooting localized instances of excessive roams. The following sections detail each section of information provided on this tab.

Packet Chart

After the desired selection has been made in the Roaming Table, the Packet Chart will update to display a detailed chart of the frames transmitted and received during the conversation both before and after the instance of roaming.

The chart highlights the selected roaming instance in red, with the color-coded packet displays on either side of the gap. Users can check or uncheck options as desired in the color legend in order to view the frames detected during the call. See [Figure 12-10](#).

The Frame Flow Chart display is divided into two sections; frames collected before roaming was initiated are displayed along the upper portion of the chart, whereas the frames gathered after the roam are displayed in the lower portion.



Figure 12-10: Packet Chart

Delay Analysis

The Delay Analysis section displays the duration of the delays detected during roaming, including the time taken to select a new AP, associate, and resume the conversation. See Figure 12-11.

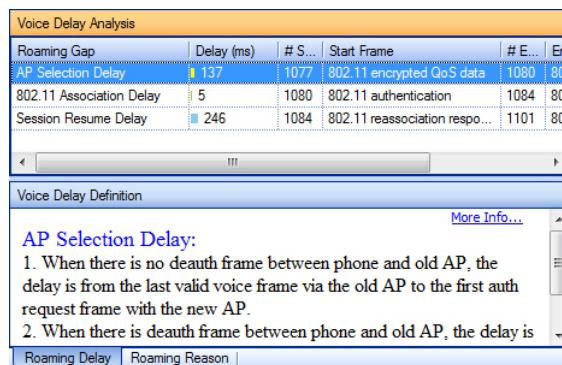


Figure 12-11: Voice Delay Details

The Voice Delay Analysis (upper) portion of the pane breaks the total delay during the roam into (up to) 5 components, as described below:

- **AP Selection Delay**—The time taken to select an AP that will provide a better call experience.
- **802.11 Association Delay**—The time that elapsed during the association process to the new AP.
- **802.1x Authentication Delay**—The time required for authentication to 802.1x-enabled networks.
- **Key Exchange Delay**—The delay experienced during 802.1x key exchanges.

- **Session Resume Delay** – The time between the successful authentication and the subsequent transmitted voice frame.

Selecting a specific delay option from the Delay Analysis table adjusts the Packet Chart to display frames specific to the selection made.

The lower portion of the window displays advanced details about the delay selected. Users can scroll through this information for specific data regarding how the delay is identified or click **More Info...** for additional details. See [Figure 12-12](#).

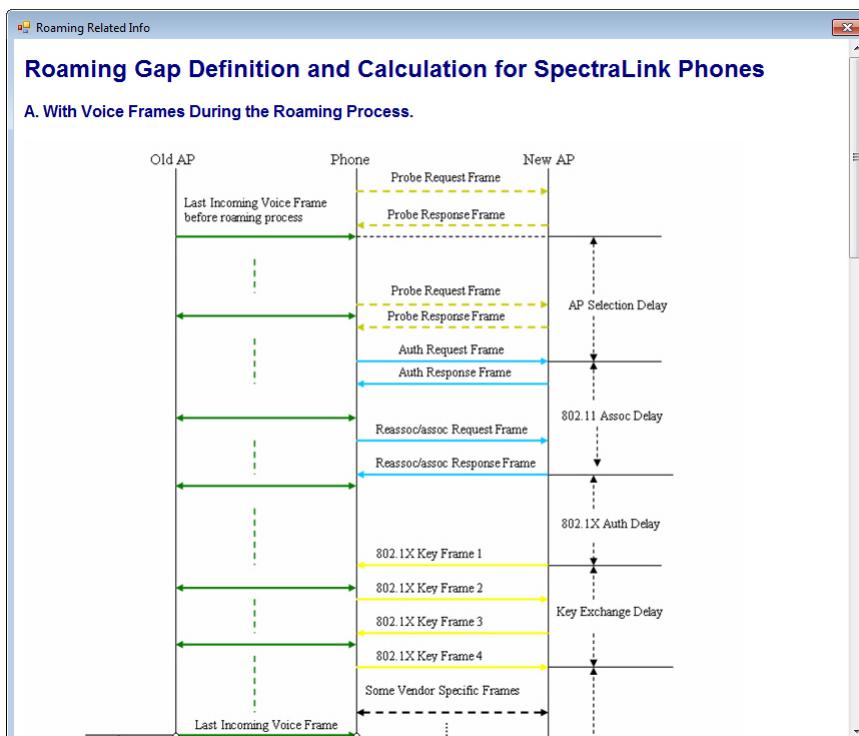


Figure 12-12: Additional Information on Selected Roaming Instance

Packet Decodes

The Decode Table and Tree can be used to help identify the packets transmitted before and after the roaming process. Selecting a specific packet will display its summary in the Decode Tree.

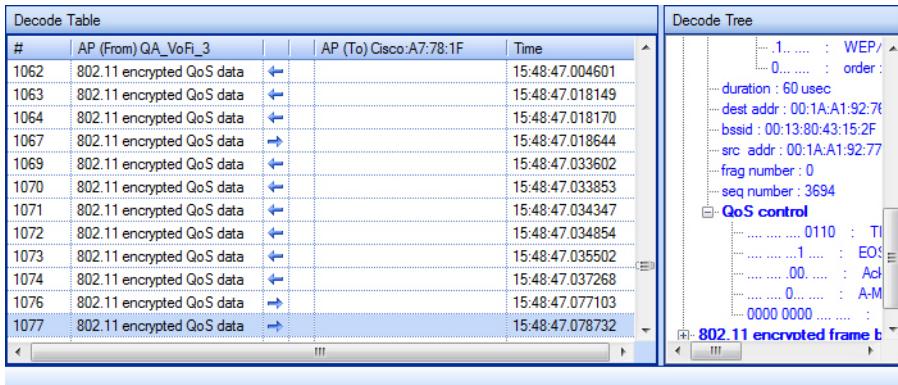


Figure 12-13: Roaming Decodes

Table 12-3 describes the columns found in the Decode Table.

Table 12-3: Decode Table Columns

Field	Description
#	The frame's number in the roaming transaction.
AP (From)	The AP from which the phone roamed.
[Arrows]	The arrows detail the direction in which each frame is moving, e.g., the arrow pointing right indicates that the frame was sent from the phone to the destination AP. An arrow pointing left indicates that the frame was transmitted from the destination AP to the phone.
AP (To)	The AP to which the phone roamed.
Time	The time at which the frame was sent.

Appendix A: Abbreviations & Acronyms

This section lists the abbreviations and acronyms used in this document. The full forms of these terms are also given. The definitions of these terms are provided in [Appendix B, "Glossary"](#).

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
ACK	Acknowledgement frame
ACL	Access Control List
ACU	Cisco Aironet Client Utility
AES	Advanced Encryption Standard
AirWISE	AirMagnet Wireless System Expert
AP	Access Point
Auth.	Authentication
BI	Beacon Interval
BSSID	Basic Service Set Identifier
CAD	Computer-Aided Design
CCI	Cross-Channel Interference
CCKM	Cisco Centralized Key Management
CF	Compact Flash
CH	Channel
CRC	Cyclic Redundancy Check (Frame)
Ctrl	Control (Frame)
CTS	Clear to Send

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
dBm	Decibels referenced to 1 milliwatt
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
Diag.	Diagnostics (Tool)
DNS	Domain Name System
DoS	Denial of Service. See DoS attack
DTIM	Delivery Traffic Indication Message
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexile Authentication via Secure Tunneling
EAP-TLS	Extensible Authentication Protocol with Transport Layer Security
FCC	Federal Communications Commission
Frag.	Fragmentation
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineering
IP	Internet Protocol
IPSec (VPN)	IP Security
IT	Information Technology
IV	Initialization Vector
L2TP (VPN)	Layer 2 Tunneling Protocol
LAN	Local Area Network
LEAP	Light EAP, Cisco LEAP

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
MAC	Media Access Control
Mgmt	Management (Frame)
MIC	Message Integrity Code
PCF	Point Coordinated Function
PEAP	Protected Extensible Authentication Protocol
Perf.	Performance (Tool)
Ping	Packet Internet Groper
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RF	Radio Frequency
RTS	Request to Send
RTT	Round Trip Time
S. Dist	Signal Distribution (Tool)
S/N	Signal/Noise (ratio)
SSID	Service Set Identity
SSH (VPN)	Secure Shell Protocol
STA	Station
STD	Standard Deviation
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
Tx	Transmission
VoIP	Voice over IP

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired-Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

Appendix B: Glossary

802.11

An IEEE local area network specification that defines the wireless network access link layer. It includes the 802.11 media access control (MAC) sublayer of the Data Link Layer and two sublayers of the Physical (PHY) layer – a frequency-hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. See 802.11a, 802.11b, 802.11e, 802.11g, and 802.11i.

802.11a

A supplement to the IEEE 802.11 wireless LAN (WLAN) specification which defines transmission through the PHY layer based on orthogonal frequency division multiplexing (OFDM), at a frequency of 5 GHz and data rates up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification which defines transmission through the PHY layer based on direct-sequence spread-spectrum (DSSS), at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11e

A supplement to the IEEE 802.11 WLAN specification that defines a set of quality of service (QoS) enhancements for WLAN applications. It enables real-time audio and video streams to be given a higher priority over regular data. This standard is considered critical for delay-sensitive applications such as Voice over Wireless IP and Streaming Multimedia.

802.11g

A supplement to the IEEE 802.11 WLAN specification that defines transmission through the PHY layer based on orthogonal frequency division multiplexing (OFDM), at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11i

An IEEE standard security protocol for the 802.11 wireless network which was developed to replace the original WEP protocol. It provides sophisticated authentication using a variety of protocols (e.g., 802.11x, EAP, and RADIUS) and strong security with the AES-CCMP encryption protocol. Also known as WPA2.

802.11X

The primary IEEE 802.11 standard for port-based network access control. Based on the Extensible Authentication Protocol (EAP), 802.11X provides an authentication framework that supports a variety of methods for authenticating and authorizing network access for both wired and wireless users.

Access Control List (ACL)

A list of known wireless devices kept by a network router or switch to control the access to and from a network.

Acknowledgement (ACK)

According to the TCP/IP protocol, ACK packets are used to acknowledge the receipt of packets. ACKs are widely used on 802.11 networks to provide reliable data transmission over unreliable media.

Advanced Encryption Standard (AES)

One of the Federal Information Processing Standards (FIPS), AES specifies a symmetric encryption algorithm for protecting sensitive information transmitted over public networks. Refer to FIPS Publication 197.

Ad Hoc Mode

A wireless network mode by which wireless networked devices can communicate directly with each other without using an AP or wired network. Also known as peer-to-peer mode or Independent Basic Service Set (IBSS).

Access Point (AP)

A hardware device that links or bridges wireless stations to a wired network. APs serve to centralize all wireless stations on a LAN in a so-called “infrastructure” mode. They are commonly used in large office buildings or public places like airports to form one wireless local area network (WLAN) that covers a large area. Each AP typically supports 255 wireless stations. Also known as wireless access point or WAP.

AirMagnet Wireless System Expert (AirWISE)

AirMagnet’s patent-pending wireless network analytical engine which automatically notifies IT and network professionals of WLAN status involving network security, performance, and configuration in real-time and provides context-sensitive, case-specific analyses and advice.

Association

The relationship or communication established between a wireless station (e.g., a laptop PC) and a wireless AP in which the station receives services from the AP.

Authentication

Any security measure adopted to establish the validity of a transmission, message, or originator, or a process for verifying a party’s authorization to receive certain information.

Bandwidth

In computer networking, the data rate supported by a network connection or interface. Bandwidth represents the overall capacity of the connection. The greater the capacity, the greater the performance, though the overall network performance may also be affected by factors such as latency, usage, etc.

Beacon

In wireless networking, a packet sent by one networked device to the other networked devices, informing them of its presence and readiness.

Beacon Interval

The length of time the transmitting device can wait before it re-sends a beacon. When sending a beacon, a wirelessly networked device will include a beacon interval which tells the networked receiving devices how long they can wait in low-power mode before waking up to handle the beacon. Beacon interval is usually measured in milliseconds (ms).

Bridge Mode

In a wireless network, the bridge mode allows two WAPs (wireless access points) to associate with each to join multiple LANs. While some wireless bridges support only a single point-to-point connection to another AP, others support point-to-multipoint connections to several APs. The AP bridging capability (if available) can be enabled or disabled through a configuration option. While operating in bridge mode, wireless APs consume a substantial amount of bandwidth. Wireless stations in a bridged 802.11 network generally share the same bandwidth as the bridge devices. Therefore, they tend to perform slower than otherwise.

Broadcast

The process of sending the same data to all stations on the network. See multicast and unicast.

Basic Service Set Identifier (BSSID)

The unique identifier for an AP in a Basic Service Set (BSS) network. It is the 48-bit MAC address of the radio inside an AP that serves the stations within the BSS.

Channel

A radio frequency or band of frequencies assigned to a specific country or region of the world by an international agreement. For instance, 802.11b is made up of 14 unlicensed channels (i.e., Channels 1-14) in the 2.4 GHz band (i.e., from 2412 MHz to 2484 MHz in 5 MHz steps).

Cisco Centralized Key Management (CCKM)

An encryption key management scheme defined by Cisco which makes it possible for wireless devices to roam fast and secure within the control domain of a WLAN. CCKM includes protection against common attack vectors such as spoofing, replay attacks, or man-in-the-middle attacks. It works when an 802.1x with EAP authentication scheme is in place, provided that the client device supports it.

CiscoWorks Wireless LAN Solution Engine (WLSE)

An important component of the Cisco SWAN framework that provides capabilities for managing the WLAN, including making configuration changes, generating reports, collecting radio monitoring and management information, and performing device discovery.

Clear to Send (CTS)

An RS-232 signal sent from the receiving station to the transmitting station, indicating that it is ready to accept data.

Co-Channel Interference

A term that refers to the interference from two or more APs operating on the same radio channel.

Compact Flash (CF)

A type of flash memory. Compact flash cards are commonly used in digital cameras for storing pictures, but are also used in PDAs and music players. There are two types of CF cards: Type I and Type II. The former is 3.3 mm thick and the latter 5 mm.

Computer-Aided Design (CAD)

A Drawing created using a software application that assists in precision drawing. CAD applications are widely used in art, architecture, engineering, and manufacturing drawings.

Crash

Any critical failure in a computer, network device or software application that runs on such devices. When a crash occurs, a computer may freeze or hang indefinitely. A crash could occur without warning. The user may have to power down and then restart the computer or network device in order to recover from a crash.

Cyclical Redundancy Checking (CRC)

An error-checking technique used to ensure the accuracy of data transmitted over the network. Each transmitted message is broken down into predetermined lengths which are then divided by a fixed divisor. The remainder of the calculation is appended onto and sent with the message. Upon receiving the message, the receiving station recalculates the remainder. An error is detected when it does not match the transmitted remainder.

Distributed Coordination Function (DCF)

A Media Access Control (MAC) technique used to manage data transmission over a medium in a WLAN. It allows a wireless node to listen to its surrounding nodes to determine if they are transmitting before transmitting itself. See PCF.

Data Encryption Standard (DES)

An encryption method originally developed by IBM and certified by the United States government for transmitting non-classified data. It uses an algorithm for private-key encryption by which the sender and recipient use the same private key. The key consists of 56 bits of data that are transformed and combined with each 64-bit block of the data to be sent.

Data Integrity

The validity of data transmitted over a network. It calls for measures to ensure that the contents of data are not tampered with and altered. The most common approach is to use a one-way hash function that combines all the bytes in the message with a secret key and produces a message digest that is impossible to reverse. Integrity checking is a key component of data security.

Decibels compared to one milliwatt (dBm)

In wireless networking, a device's transmit or receive powers are measured in decibel strength compared to one milliwatt of power. The higher the dBm value, the greater the device's transmit or receive power.

Delivery Traffic Indication Message (DTIM)

A signal transmitted as part of a beacon by an AP to a station in power-save mode, alerting the device that a packet is waiting for delivery.

Domain Name System (DNS)

The name-address resolution system which automatically converts Internet domain and host names to IP addresses. DNS eliminates the manual task of updating hosts files in a network. Also known as Domain Name Service, Domain Name Server.

Dynamic Host Configuration Protocol (DHCP)

A software application that automatically assigns IP addresses to stations logging on to a TCP/IP network. DHCP software typically runs on network servers and is also found on network devices, e.g., ISDN routers, modem routers, etc. that allow multiple users access to the Internet. DHCP relieve network professionals the burden of having to manually assign IP addresses.

Encryption

The reversible transformation of data from the original to a difficult-to-interpret format (the encrypted) as a way to protect their confidentiality, integrity and sometimes authenticity. It involves the use of an encryption algorithm and one or more encryption keys.

Ethernet

A standard used for connecting computers together to form a local area network (LAN).

Extensible Authentication Protocol (EAP)

A protocol that is used as a framework and transport for other authentication protocols. EAP uses its own start and end messages, but can also carry any number of third-party messages between a station and an AP in a wireless network.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)

An enhancement to LEAP by Cisco that provides an encrypted tunnel for transmitting pre-shared keys known as "Protected Access Credential" (PAC) keys. PAC keys can be continuously refreshed to prevent dictionary attacks. EAP-FAST provides secure access to a wireless network.

Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)

A wireless network security protocol created by Microsoft and accepted by IETF. Refer to *RFC 2716: PPP EAP TLS Authentication Protocol*.

Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS)

A proprietary protocol developed by Funk Software and Certicom and supported by Agere Systems, Proxim, and Avaya. It is being considered by the IETF as a new standard for wireless networks.

Federal Communications Commission (FCC)

A United States federal government agency that regulates communications in the country.

Frame

In communications, a fixed block of data transmitted as a single entity over the network.

FTP

Standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet.

Global Positioning System (GPS)

A satellite-based radio navigation system operated by the United States Department of Defense. It is used for identifying locations on the Planet. By triangulation of signals from three satellites, a receiving device can pinpoint its location anywhere on earth to within 20 meters horizontally.

Hot spot

In wireless networking, a specific location within an AP's range where the general public can use the network service, usually, for a fee.

HTTP

Networking protocol for data distribution for the World Wide Web.

Infrastructure Mode

A wireless network setup in which all stations communicate with the network or with each other via an AP. Infrastructure mode is typical of an enterprise wireless network.

Institute of Electrical and Electronic Engineers (IEEE)

A non-profit engineering organization in the United States that develops, reviews, and promotes standards within the electronics and computer industries.

Interference

In wireless networking, the disturbance that results when radio signals from different APs collide in the airwave.

Internet Protocol (IP) address

A 32-bit unique string of numerical characters used to identify a networked computer, printer, or any other device.

Jitter

Radio signal fluctuation observed in traffic between AP and station on a wireless network.

Lightweight Extensible Authentication Protocol (LEAP)

A proprietary protocol for secure access to WLANs developed by Cisco.

Local Area Network (LAN)

A short-distance network that joins a group of computers together, usually within the same building. Using a network hub as a wiring point, data can be sent from one computer to another over the network.

Media

In wireless networking, the term refers to the types of 802.11 media used on wireless networking devices, i.e., 802.11a, 802.11b, and 802.11g.

Media Access Control (MAC) address

A unique, 48-bit number assigned to each IP network adapter. It is written in a sequence of 12 hexadecimal digits (e.g., 46:2F:0B:19:11:CB). Each MAC address is uniquely set by the network device manufacturer and is sometimes called the device's "physical addresses". The first six hexadecimal digits of an MAC address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number.

Multicast

The process of sending a single message to multiple destinations simultaneously. It is a one-to-many transmission similar to broadcasting, except that multicasting means transmission to specific groups, whereas broadcasting implies sending to everybody. Multicasting can save considerable bandwidth when sending large

volumes of data because the bulk of the data is transmitted once from the source through major backbones and are multiplied, or distributed out, at switching points closer to the recipients. In a unicast system, the data is replicated entirely to each recipient. Compare unicast. See diagram.

Network Adapter

A hardware device that interfaces a station (e.g., a computer) to a network. Modern network adapter hardware comes in many forms, such as PCI Ethernet cards, PCMCIA devices, or USB devices. Some laptop computers even come with integrated wireless network adapters pre-installed on them in the form of circuit chips. Operating systems support network adapters through a piece of software known as “device driver”, which enables application software to communicate with the adapter. Some network adapters are software packages that simulate the function of a network adapter. Also known as wireless network card, WiFi card.

Noise

In wireless networking, any radio signal that does not convey useful information. See to signal-to-noise ratio (S/N or SNR).

Ping

In wireless networking, an application that is used to send a packet over the Internet to verify the connectivity of a remote node. If the packet bounces back, it means that the remote device is connected.

Point Coordinated Function (PCF)

A Media Access Control (MAC) technique used in WLANs, in which a wireless node relies on an AP as a central node to communicate with another node. The AP listens to make sure that the airwaves are clear (i.e., no other data traffic) before allowing the node to transmit.

Protected Extensible Authentication Protocol (PEAP)

A proprietary protocol jointly developed by Microsoft, Cisco, and RSA Security.

Request to Send (RTS)

A message sent by a networked station to the associated AP or station, seeking permission to transmit data.

Roaming

In wireless networking, the ability of a wireless device (station) to maintain network connection when it is being moved between different cells covered by different APs.

Service Set Identifier (SSID)

A unique name that identifies a wireless network or a network subset. It is used by every device connected to the network or that part of the network to identify itself as part of the family when accessing the network or verifying the origin of a data packet it is transmitting.

Signal

In wireless networking, any electrical pulse or frequency that carries meaningful data in the airwave.

Signal-to-Noise Ratio (S/N or SNR)

The ratio of the amplitude of a signal to the amplitude of background noise (interference) that mixes in with it measured in decibels. It measures the clarity of a signal in a wireless transmission channel. The greater the ratio, as indicated by a larger number, the less the noise and the better the signal quality. A SNR of 0 (zero) means that noise and signal levels are the same, which is the lowest value it can go.

Station (STA)

In wireless networking, any device with a MAC address and a physical layer (PHY) interface to the wireless medium that comply with the IEEE 802.11 standard, e.g., a laptop, PDA, etc.

Temporal Key Integrity Protocol (TKIP)

A security protocol defined in IEEE 802.11i specifications for WLANs. It was designed to replace WEP without replacing legacy hardware. Like WEP, TKIP uses a key scheme based on RC4 except that it encrypts every data packet sent using its own unique encryption key. TKIP also hashes the IV values that are sent in the current release of WEP, meaning that the IVs are also encrypted and are not as easy to sniff out of the air.

TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus addressing other security issues with WEP. This increases the complexity of decoding the keys by reducing the amount of data available to the cracker, that has been encrypted using a particular key.

A wireless encryption protocol that mends the known security loopholes in the WEP protocol for existing 802.11b devices. TKIP comes with a 128-bit encryption key, a 48-bit initialization vector (IV), a message integrity code (MIC), and initialization vector sequencing rules to offer better protection than WEP does.

Traceroute

An IP networking utility that is used to identify the path in real time from the transmitting station to the remote host being contacted. It can discover the IP addresses of all the routers in between.

Transport Layer Security (TLS)

An authentication and encryption protocol for private transmission over the Internet. It provides mutual authentication with non repudiation, encryption, algorithm negotiation, secure key derivation, and message integrity checking. As the successor to the Secure Socket Layer (SSL) protocol, TLS has been adapted for use in WLANs and is widely used in IEEE 802.11x authentication.

Tunnel Transport Layer Security (TTLS)

A subprotocol of the Extensible Authentication Protocol (EAP) developed by Funk Software, Inc. for 802.11x authentication. It uses a combination of certificates and password challenge and response as a means of authentication. TTLS supports authentication methods defined by EAP, as well as the older Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft CHAP (MS-CHAP), and MS-CHAPV2.

Unicast

The process of sending duplicates of the same message to multiple destinations on the network. In unicast, even though multiple users might request the same data from the same server at the same time, duplicate data streams are transmitted, one to each destination. Compare multicast. See diagram.

Voice over IP (VoIP)

A technology used to carry telephone voice signals as IP packets over the Internet or a dedicated IP network, in compliance with International Telecommunications Union Standardization Sector (ITU-T) specification H.323. It enables a router to transmit telephone calls and faxes over the Internet with no loss in functionality, reliability, or voice quality. Also known as IP telephony or Internet telephony.

Wired-Equivalent Privacy (WEP)

A security protocol within the IEEE 802.11 standard that provides a WLAN with a *minimum* level of security and privacy comparable to that of a typical wired LAN. WEP encrypts data transmitted over the WLAN to protect vulnerable connection between APs and stations. However, since WEP regulates WLAN access based on a device's MAC address which is relatively easy to be sniffed out and stolen, it offers limited security to a WLAN.

Wireless LAN (WLAN)

A local area network (LAN) to which wireless users (stations) can connect and communicate via high-frequency radio waves rather than copper wires.

WiFi Protected Access (WPA)

A security protocol for the IEEE 802.11 standard designed to overcome the security vulnerabilities of WEP. The technology is intended to work with existing wireless devices that are WEP-enabled, but offers two important enhancements over WEP: enhanced data encryption through TKIP and user authentication through EAP. TKIP complies with only a subset of the IEEE 802.11i protocol and is designed to work in older WEP-enabled devices by updating their firmware to WPA.

WPA2, on the other hand, offers full support for the 802.11i standard. In addition to TKIP, it supports AES-CCMP encryption protocol which is based on the very secure AES national standard cipher combined with sophisticated cryptographic techniques and is specifically designed for WLANs.

Appendix C: Third-Party Copyrights

Iperf Copyright

Copyright (c) 1999-2006, The Board of Trustees of the University of Illinois
All Rights Reserved.

Iperf performance test

Mark Gates

Ajay Tirumala

Jim Ferguson

Jon Dugan

Feng Qin

Kevin Gibbs

John Estabrook

National Laboratory for Applied Network Research

National Center for Supercomputing Applications

University of Illinois at Urbana-Champaign

<http://www.ncsa.uiuc.edu>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software (Iperf) and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimers.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.
- Neither the names of the University of Illinois, NCSA, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTRIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

D. Young Copyright

Copyright (c) 2003, 2004 David Young. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 The name of David Young may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY DAVID YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL DAVID YOUNG BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

A. Onoe & S. Leffler Copyright

Copyright (c) 2001 Atsushi Onoe

Copyright (c) 2002-2005 Sam Leffler, Errno Consulting

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions * are met:

- 1 Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

S. Leffler Copyright

Copyright (c) 2002-2005 Sam Leffler, Errno Consulting

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B. Paul Copyright

Copyright (c) 1997, 1998, 1999

Bill Paul <wpaul@ctr.columbia.edu>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by Bill Paul.
- 4 Neither the name of the author nor the names of any co-contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY Bill Paul AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL Bill Paul OR THE VOICES IN HIS HEAD BE LIABLE FOR

ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

AppendixD: Upper-layer decode support license

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for your
libraries, too.

When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and
charge for this service if you wish), that you receive source code or
can get it if you want it, that you can change the software or use
pieces of it in new free programs; and that you know you can do
these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES

ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
See the GNU

Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

Index

Symbols

.pcap 316
#STA 70, 74

Numerics

02.11n-related issues 347
2.4 GHz vs. 5 GHz 82
2.4-GHz 90
2.4-GHz (802.11b/g/n) channels 63
2.4-GHz channels 90
20- and 40-MHz channels 65
20 MHz 84, 96
20/40 MHz Statistics 261
20-MHz 353
2nd Channel 75
3rd party decodes 21, 135, 201
4.9-GHz band 342
4.9-GHz spectrum 81, 342
40 GHz Intolerant 76
40 MHz Tolerant 350
40-MHz 353
40-MHz transmissions 203
40-MHz wide band 65
5-GHz 802.11a/g/n channels 64
5-GHz channels 90
802.11 72
802.11 a/b/g 79
802.11 media band 96
802.11 protocols 111
802.11 settings 161
802.11 standards 82
802.11 wireless networking standards 80
802.11-based wireless local area networks 1
802.11d 109
802.11h 109
802.11n capabilities 361
802.11n network 369
802.11n network efficiency 255
802.11n network issues 255
802.11n Networks 7

802.11n protocol 369
802.11n tools 9, 256
802.11n transmissions 368
802.1x process 287

A

access control list 161
access recently opened files 322
accuracy 286
ACL 161, 235
ACL group 235
ACL Status 74
acquisition of IP addresses 289
active support contract 17
Active Time for Device 71
add an SSID group 241
add new alarm notification 227
add site information 211
adding reports 332
address book 161
address books 161
address table 207
Ad-Hoc 66
administration responsibility 161
Advanced 61
Advanced Driver Settings 191
Advanced Features 8
Advanced Iperf Properties 301
AirMagnet 802.11n Learning Assistant 352
AirMagnet Reporter 315
AirMagnet Wireless System Expert 1
AirWISE 2, 7, 47, 79
AirWISE Advice 67
AirWISE Community 45
AirWISE expert engine 219
AirWISE filter 51
AirWISE Screen 112
AirWISE screen 49, 67, 70, 109, 304
Alarm Information 116
Alarm Severity and Color Codes 114
Alarm Status 109

Alert 108, 116
alias 207
Altitude 74
amc 316
Americas 82
A-MPDU 261
Analysis 256, 260
analysis 1
Analysis tool 353
AP 66
AP (Rx) 259
AP (TX) 259
AP Capability 258
AP Details 116
AP Grouping 212
AP grouping rules 213
AP->STA 259
appearance 216
archiving 315, 327
assets 207
assign a notification 250
Associated AP 74, 268
association process 285, 286
Atheros chipset 35
Australia 82
authentication 246, 285
authentication mechanism 187
Authentication Mechanisms 187
Authentication Types 245
Author 332
authorized reseller 16
Automatic Configuration of 40 MHz Channels 203
Automatically 2
Average 104

B

backup license file 19
backward compatibility 257
backward compatible 365
Basel II 125, 128
Basel II Accord 125
basic 47
beep 252
BI 70, 74

Bind to Host 303
Block ACK 270
Bluetooth devices 100
boilerplate 162
Book properties 335
Book Title 332
breakage 290
Bridge Mode 70, 73
broadcast 67
Bubble Help 78, 351
buffer 80
Buffer Length 302
Byte Count 268
bytes 86

C

Cahnnel Throughput 84
calculating 262
calibrate wireless LAN card 197
cap 316
Capability 259
capture filters 161
Capture to disk 166
case-specific 2
Cell Power 75
cell size 273
center frequency 355
Channel 71
Channel Bandwidth 270
Channel Data Graphical Display 87
Channel Data Summary 86
Channel filter 51
channel interference summary 96
Channel Occupancy 88
channel occupancy 90
channel scan list 65, 161
channel scan settings 161, 201
Channel screen 49, 83
Channel Screen Control Buttons 87
channel throughput 84
Channel Utilization 84
channel utilization 84
Chart Data Tabulation 123
China 82
Classic Tree View 113

- client configuration utility program 285
Client Port 302
client service 289
close proximity 367
coexist 369
coexist with legacy devices 367
Coexistence 257
color-coded 63, 111
comma-separated-value 322
Company Info 332
Compatibility 302
Compiling a Report Book 330
Compliance Charts 124
compliance charts 120
Compliance Reports 129
compliance reports 7
Compliance Reports Disclaimer 129
Conducting a Roaming Test 294
Conducting RF Data Survey 281
Conducting roaming tests. 255
Conducting Signal Distribution Test 277
Conducting site survey 255
configuration settings 161
Configure 162
configure 219, 244
configure advanced driver settings 191
configure channel scan settings 203
configure filter settings 199
configure LEAP 190
configure policies 245
configure signal coverage test settings 273
configure Signal Distribution tool settings 276
configure survey logging options 280
configure WEP settings 189
Configuring 802.11 Settings 185
Configuring General Settings 167
congested network 354
connection problem 285
Connection Test 285
connection troubleshooting 1
Connections between Devices 109
connectivity problems 287
context-sensitive 2
Control Frames 108
Control frames 116
cordless phones 63, 100
Cover Page 332
Coverage 272
Coverage tool 272
create an address book 208, 209
Creating a new system profile 162
Critical 67, 114
cross-channel interference 63
csv file 324
Custom 216
Custom Books 329
Custom Reports 333
customize 65
Customizing 219

D

- Data Analysis 116
Data Frames 108, 116
Data Selector 88
database applications 322
Decode screen 50
Decode Screen Parameters 130
Decodes Screen 129
Decodes screen 129
Decoding 47
default alarms settings 219
Default Books 329
default gateway 289
default notifications 250
default profile 161
Default Reports 333
delete alarm notification 234
delete an SSID group 244
Department of Defense (DoD) Directive Number 8100.2 125
Department of Defense Directive 8100.2 125
Device 72, 268
Device Charts 120
Device filter 51
device information 322
device throughput 255
Device Throughput Calculator 256, 268, 359, 361
Device to Simulate 268

device-centric 117
diagnose 285
Diagnostic 284
Diagnostic tool 285
diagnostics 1
diagnostics screen 286
digits 67
Distance 74
DNS server 289
DOD 8100.2 125
Downlink 258
download 296
Dual Beacon 76, 351
Dual CTS Protection 76, 351

E

EAP-FAST 187
Easy View 57, 60
easy-to-follow screens 244
edit existing alarm notification 231
editing an address book 210
Efficiency 256
Efficiency screen 352
Efficiency tool 256, 351, 358, 364
Email 230
emission powers 82, 201
Enable non-stop (wraparound) capture 166
enterprise technology 1
epc 316
equalize 197
Erase 114
Ethereal 316
Ethernet 1
EU CRD/CAD3 128
EU-CRD 125
Europe 82
European Union (EU) Capital Requirements Directive 125
event alarms 219
Event Log 169
event log options 169
Excel 282, 322
existing file 317
expanded signal meter screen 65
Expert Advice 114, 116

export 161, 315, 327
export a profile 164
export file names 161
export operation 323
Exporting a System Profile 164
Exporting Data 122
Extended Channels 205

F

Failure Analysis Tool 9
features 349
Federal Information Security Management Act 126
file formats 316
file path 317
Filter 199
filter options 198
filter settings 161
final ratification 369
Find 295
Find in This View 137
Find tool 77, 304
First 74
FISMA 126
Fluke 373
frame communication 57
frame types 200
Frames 108, 116
frequency 201
frequency spectrum 64
FTP Tool 291
Full Screen 376

G

General settings 166
general system settings 161
geographical location 82
GPS 295
GPS device 310
GPS Log 310
GPS tool 310
Gramm-Leach Bliley Act 126
Graph Option 123
Graph Options 88

Greenfield Supported 75, 351
guest 246

H

hardware failures 285
Health Insurance Portability and Accountability Act 126
hidden devices 97, 99
HIPAA 126
historical RF data 318
Hong Kong 82
host computer 322
Host-Based EAP 187
How-To Guide 10
How-To guide 52
HT Disabled 259
HT Not Well Used 259
HT Well Used 259
HTTP Tool 292

I

ICMP messages 290
IEEE 351
impact 370
import 165
Importing a System Profile 165
increment 197
Informational 67
Infrastructure Data Graphs 106
Infrastructure Data Pie Chart 108
Infrastructure Data Summary Report 107
Infrastructure screen 49, 66, 70, 104, 366
install Iperf 296
Installing 15
Integration with Windows Wireless Configuration 30
Interference 90
Interference Score 72
interference score 90, 92
interference score graph 99
interference scores 96
Interferers 103
internal database 207
Iperf 255, 296

ISO 27001 127
ISO/IEC 27001
2005 127

IT 1

J

Japan 82
Jitter 295, 306
Jitter tool 307

K

key functions 47
knowledge 244
known active channels 65
Korea 82

L

LANCardVendorsFile.txt 27
Laptop Analyzer CD 15
Last 70, 75
Latitude 74
Launching 47
Launching AirMagnet Laptop 48
layered policy structure 221
LDPC 76, 350
LEAP 187
Least Capable Device 271
least capable devices 368, 370
legacy 802.11 networks 257
legacy APs 370
legacy devices 365, 368
legacy devices and networks 369
legacy networks 367
levels of severity 67
license file 15
Link Speed 86
Live Capture 57
live capture 321
live capture mode 57
Load Statistics on Open Capture File 318
locate a rogue device 304
locate rogue devices 304
location 310
locations 282

log files 315, 327
Longitude 74
Lower 40 MHz 84, 95, 203
L-SIG TxOP Full Support 76

M

MAC 257
MAC Address 72
MAC address 70, 285, 286, 304
MAC address-alias pairs 207
MAC addresses 207
MAC-vendor name mappings 28
Main Features 5
Main Title 332
major 47
malicious 202
manage 219
Management Frames 108, 116
Managing Alarm List 114
mandatory 349
manual groups 214
Max 104
Max Frame Size 270
Max Hold 104
Max Segment Size 302
MCS 261, 270
measure roaming connectivity 293
measure site RF signal coverag 274
Measuring RF jitter 255
Measuring WLAN coverage 255
Media 86
Media Type 79, 86
media type 70
Medium Access Control layer 257
Microsoft Core XML 24
Microsoft Wireless LAN API 24
microwave ovens 63
microwaves, 100
misconfiguration 202
misconfigured WLAN devices 202
mismatched configurations 285
mobile application 1
mobile user base 1
modulated 94, 98, 355
modulated spectrum 94

modulated spectrum usage 89
modulation types 92
monitor 347
monitoring 1
multicast 67
My Profile 161
MyTTouch Soft Keyboard 378

N

Navigation Bar 48
Navigation Bar and Buttons 49
navigation buttons 48
navigation controls 47
neighbor 246
network data reports 328
network infrastructure 57
Network Infrastructure Color Codes 106
network performance analysis 296
network policies 219, 221
network policies and alarms 225
Network Policy Hierarchy 113
network professionals 2
network security 1, 112
network security and performance issues 1
network settings 244
Network Throughput Simulator 367, 369
Network Tree Structure 105
node and network levels 370
Noise 72
noise 63, 70
noise floor 197
noise level 64, 81, 97
non-802.11 interference 91
Non-Greenfield STA Present 75
Non-Greenfield STAs Present 350
Non-HT OBSS 75, 350
notification configuration 249
notification options 227, 250
Notification Wizard 219, 249
novice users 244

O

Observed (Downlink) 259, 260, 365
Observed (Uplink) 259, 260, 365

OBSS Non-HT STAs Present 350
Occupancy 88, 355
occupancy 88
occupied and/or unoccupied channels 355
One-tou connection test tools 287
operating frequencies 80
Operating Mode 75, 350
optimal channel 354
optional 349
organizational summary 66
other 246
OUIs 27
Output Format 303
overall 47
overhead 367
overview 272

P

P Group 71
Pacific Rim 82
Packet Capture 165
Packet Capture Filters 198
Packet Count 268
packet frames 130
Packet Frames Summary 67
Page over Internet 231
Page over Phone 230
Parallel Streams 302
path 281
Payment Card Industry Data Security Standard 127
PCF/DCF 70, 74
PCO 75, 351
Peer-AP-Peer Connections 110
Peer-to-Peer Connections 110
percentage 81
percentage of the frames 367
performance status 112
Performing WLAN diagnostics 255
PHY 256
PHY Data Rate 261
physical layer 256
pie chart 66, 108
Ping 287
Ping tool 289

Play Sound 231
plot 282
policies 161
Policy Management Procedures 253
Policy Management Screen 220
Policy Reference Guide 16
policy rule 221
policy structure 253
Policy Tree 220, 221
policy violations 219
Policy Wizard 219, 244, 245
pre- or post-installation 272
Preamble 70, 74
preamble 285
pre-configured 187, 201, 225
pre-configured network policies 225
Previewing Data 321
Previewing data 315
primary channel 85
Primary/Secondary Channels 350
print 315, 327
Print MSS 304
probe discovery 285
Product Overview 1
product package 15
Product Package Contents 15
Product Registration 27
profile 163, 164, 211
prohibited channels 202
protect legacy devices 368
protection 367
protection mechanisms 368
Protection Method 271
public safety 344

R

Radio Channel Allocation 82
radio frequencies 82, 201
radio operating frequencies 79
Rate 268
Read Me First 15
re-association 285
Recent Files 321
recently opened files 315
Registering 15, 16

- regulated channels 202
regulatory requirements 202
regulatory rules 202
remove a filter 200
Report Book Detail 331
report book. 332
Report Properties 336
Report Type 334
Reports screen 328
Representative File 303
Reset 252
resolve 347
restore 252
Restore Screen 376
resume 321
RF channels 285
RF Interference 90
RF signal quality 57
RF Spectrum Interferer 103
RF Spectrum Interferers 103
RIFS Mode 76, 350
Roaming 283, 285
roaming 273
roaming control option 283
Roaming Criteria 283
Roaming Option 282
Roaming tool 293
Roaming tool screen 293
rogue AP 202
rogue APs 202
Rogue APs and clients 252
rogue APs and stations 65
rogue device 305
Rogue in Network 74
routing path 290
run the AirMagnet Traceroute utility 290
Rx Ch Width 75
Rx Channel Width 351
Rx STBC 76, 351
- S**
Sarbanes-Oxley 128
Sarbanes-Oxley Act 127
save 315, 327
save data 317
- scan frequency 65
Scan time 204
screen options 47
screens 48
scrolling list 130
Search Text 339
secondary channel 85
security 70
security and performance management 1
security and performance policies 219, 244
security and performance status 57
Security Mechanisms 73
session 323
session name 323
Setting up Authentication 244
Setting up SSID Groups 244
Setting up Vendor List 244
Setup Vendor List 246
SGI 75, 350
sharing 315, 327
Short Guard Interval 270
Short Guard Interval (SGI) 261
Signal 72
signal 70
signal coverage 282
Signal Distribution 272
signal distribution patterns 276
Signal Distribution tool 276
Signal Meter 62
signal meter 64
signal Multipath 276
signal quality 63
Signal Quality Codes 63
signal strength 64, 81, 197
Signal-to-Noise Ratio 72
signal-to-noise ratio 64, 70, 81
simulated WLAN data 266
Simulator 262
Singapore 82
Site Information 210
site information 161
Site Survey 272
site survey 161, 278
site survey and audit 1
Site Survey utility 279
Skin 217

- SM Power Save 76, 351
SMS via Email 230
Sniffer 316
software installation 15
sound 252
Spain 82
spectral distance 94
spectral properties 94
Spectrum Analyzer 100, 102
Spectrum Analyzer Adapter 102
Spectrum Analyzer graph 104
Spectrum Analyzer Integration 100
spectrum graph 101
spectrum usage 355
Speed 86, 108, 116
spreadsheets 322
SSID 66, 70, 73, 235, 304
SSID filter 51
SSID groups 241
SSIDs, 285
STA 66
STA->AP 259
Start scree 366
Start screen 48, 49, 59, 349
Station Detail 116
station probing 63
Status 268
structured policy configuration 219
Subtitle 332
summarized information 57
supported 351
Supported Wi-Fi Cards 14
survey file 281
Switching media type 80
SysLog 231
System Address Book 207
system configuration 161
system profile 161, 162
System Requirements 10
system requirements 10
- T**
- Table of Contents 332
tabulate 282
tabulation 67
- Taiwan 82
tap and hold 375
TCP 297, 298
TCP No Delay 303
TCP Window Size 302
technical support 15
Testing signal distribution 255
theoretical throughput level 360
third-party software 282
Throughput 267, 268
throughput 357
throughput between a certain AP and STA 364
Throughput/Iperf 295, 356
Time (usec) 268
TK & MIC 70
TKIP/MIC 73
toolbar 53, 60
tools 48
Tools screen 50
Top Traffic Analysis screen 118
Trace utility 290
Tracing network device 255
transmission rates 285
transmit spectrum masks 92
troubleshoot 347
Troubleshooting link connection 255
Tx Channel Width 350
Tx channel width 75
Tx Data Bytes 268
Tx Packets 268
Tx STBC 76, 351
Type of Service 303
- U**
- UDP 297, 299
UDP Bandwidth 302
unicast 67
unidentified RF signals 63
Unit of Measurement 81
un-modulated 94, 98, 355
unused channels 65
up- and downlink throughput 357
Uplink 258
Upper 40 MHz 84, 96, 203

Upper-layer decode support 21, 135, 201, 417
Urgent 67
use multiple capture files 166
User Guide 16
utility 244

V

value 320
Vendor List 247, 248
vendors 248
View by 802.11n 60, 349, 366
View by AirWISE Category 113
View by Channel 60
View by Device 60
View by Device/Channel 113
View by Media Type 60
View by Node Type 60
View by SSID 60
View by Time 113
View Filter 50, 51
View Reports 83, 328
violation 202
Visio 282
Vista 10, 30
VLAN 212

W

Warning 67
Web cameras 63
WEP 187
WEP keys 285
What's New 10
Wi-Fi 1
WiFi Analyzer Express and WiFi Analyzer

PRO 2
Windows event log 169
Windows Vista 35
Windows wireless profiles 10
Windows XP 30
Windows XP operating system 31
wired networks 1
wireless adapters 14
wireless cameras 100
wireless card 80
wireless devices 207
wireless LAN card driver 191
Wireless LAN Card RF Calibration 192
wireless LAN infrastructure 66
wireless network adapters 283
WLAN 1
WLAN event management and analysis 219
WLAN health 47
WLAN management duties 255
WLAN network management tools 255
WLAN nodes 47
WLAN policies 161
WLAN structural components 107
WLAN throughout 255
WLAN Throughput Simulator 256, 262, 362
world-mode 202
Worldwide 82
worldwide 201
WPA configuration and support 191

X

XP 10