WiFi Analyzer User Guide

Table of Contents

Introduction

Product Overview

AirMagnet WiFi Analyzer is the industry standard tool for mobile auditing and troubleshooting enterprise Wi-Fi networks. AirMagnet WiFi Analyzer helps IT staff quickly solve end-user issues while automatically detecting security threats and wireless network vulnerabilities. The solution enables network managers to easily test and diagnose dozens of common wireless performance issues including throughput issues, connectivity issues, device conflicts and signal multipath problems. AirMagnet WiFi Analyzer includes a full compliance reporting engine, which automatically maps collected network information to requirements for compliance with policy and industry regulations.

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 Wi-Fi across all industries.

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in a situation where they have to deal with an ever-increasing influx of network security and performance issues with outdated tools originally designed for the wired network.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 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.

Copyright

AirMagnet WiFi Analyzer Pro Technical Documentation.

AirMagnet, a NetAlly Brand

NetAlly
2075 Research Parkway
Colorado Springs, CO 80920

Compiled in the United States of America.

Version 11.3.2, Released 04/2020

Main Features

AirMagnet WiFi Analyzer is the industry's most popular mobile field tool for troubleshooting enterprise Wi-Fi 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

Automatically identify 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. You can also use the 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. You can designate your encryption and authentication methods then monitor your wireless LAN to check all devices for compliance with those policies and 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, it also provides a suite of active troubleshooting tools, available at your fingertips to help you quickly pinpoint network problems, such as RF interferences, traffic/infrastructure overloads, hardware failures, and connectivity issues. You can 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 Wi-Fi Interference Analysis

Interference can stem from a variety of sources including competition from other Wi-Fi 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 Wi-Fi 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

View real-time packet flows for any Wi-Fi 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 encyclopedic source for understanding the threats and performance issues at work in your Wi-Fi 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/ac Networks

Identify and classify all 802.11n/ac capable devices in the network (including differentiating between standards-compliant and pre-standard 802.11n devices).AirMagnet WiFi Analyzer supports monitoring for 20 MHz, 40 MHz and 80MHz channels and also detects and classifies higher data rates used by the 802.11n/ac devices. With AirMagnet WiFi Analyzer, you can classify and decode Non-HT (legacy), HT mixed format traffic as well as VHT traffic and identify backward compatibility issues with legacy 802.11a/b/g devices operating in the same environment. You can also locate 802.11n/ac rogue devices, which are often invisible to non-802.11n analyzers and decode new information elements/wireless frame types.

Generate Compliance Reports

Generate 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 Wi-Fi 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.

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 you the flexibility of walking about the physical premises to audit and troubleshoot enterprise Wi-Fi networks using a light-weight handheld solution. AirMagnet WiFi Analyzer is supported on the OQO Model 02/e2 UMPC.

Support for 802.11n/ac Wireless Networking Standard

AirMagnet WiFi Analyzer enables you to use the latest wireless networking standards, promising greater performance, more range, and improved reliability—the three most important elements of networking. With an AirMagnet-supported 802.11n wireless network

card, you can now monitor 802.11n/ac traffic on both 20, 40 and 80MHz channels, identify 802.11n/ac devices, and decode 802.11n/ac frames on the network.

802.11n/ac Tools

AirMagnet WiFi Analyzer comes with 802.11n and 802.11ac tools that allow you to analyze the performance of the wireless network—the next generation of wireless networking technologies that offer unprecedented network throughput, range, and stability. The following tools are designed to help you understand and troubleshoot the most common issues you may encounter:

- **Efficiency Tool**—The 802.11n and 802.11ac wireless network protocols 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 and 802.11ac networks.
- **Analysis Tool**—The Analysis Tool provides detailed explanation and analysis about the 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 you to add and configure up to fifty 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac 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. You just click to specify the parameters such as MCS index, SGI, bandwidth, maximum frame size, block ACK, least capable device, and/or protection mechanism used. AirMagnet will then 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 showing the percentage of DIFS, preamble/PLCP, Data, SIFS, preamble/PLCP, and ACK frames.

Integration with Windows Wireless Configuration

AirMagnet WiFi Analyzer allows you to take advantage of Windows wireless profiles that have been created in a Windows operating system and use them directly with AirMagnet WiFi Analyzer’s active tools (for example, Site Survey, Performance, Connect, Roaming, and so on.).

How-To Guide

AirMagnet WiFi Analyzer includes a Microsoft Office Assistant-like How-To guide that helps you 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.

Remote Troubleshooting

You can connect to remote systems to perform remote troubleshooting as follows:

- **Option 1:** this option involves setting a computer running AirMagnet WiFi PRO to Remote Operation Mode. Once a computer is set to this mode, you can enable a remote connection to it from your local computer running AirMagnet WiFi Analyzer PRO. The local computer switches to the remote adapter for data collection.
- **Option 2**: You can connect remotely to some models of AirMagnet SmartEdge Sensor.

System Requirements

***Note**: These are minimum system requirements. Packet capture and analysis rates depend on system performance. A higher performance system provides better results for packet capture and analysis.*

Laptop/Notebook/Tablet PC

- Operating Systems: Microsoft® Windows 8.1 Pro/Enterprise 64-bit, or Microsoft® Windows 10 64-bit.
- Intel® Core™ 2 Duo 2.00 GHz (NetAlly recommends Intel® Core™ i5 or higher).
- 4 GB memory or higher.
- 800 MB free hard disk space.
- An ExpressCard slot or USB port; or an AirMagnet supported internal WLAN adapter.
- Multiple slots in the PC when using multiple adapters. NetAlly recommends the use of its multi-adapter kit.
- AirMagnet-supported wireless network adapter(s).
- Optional spectrum adapter and license (required for viewing spectrum data and non Wi-Fi devices; AirMagnet WiFi Analyzer PRO only). Integration supported with AirMagnet Spectrum XT.

***Note:** Spectrum XT adapter is in the USB form-factor.*

Apple® MacBook® Pro

- Operating Systems: MAC OS X (Leopard™) running a supported Windows OS (as noted under Laptop/Notebook PC/Tablet PC section) using Boot Camp®.
- Intel® Core™ 2 Duo 2.00 GHz or higher recommended.

- 4 GB memory or higher.
- 800 MB free hard disk space.
- An internal Broadcom 802.11ac WLAN adapter (MacBook 2013 and 2014 models), an Atheros-based Airport Extreme 802.11n WLAN adapter, or a USB port (whichever applicable).
- Multiple slots in the PC when using multiple adapters. AirMagnet recommends the use of its multi-adapter kit.
- Optional spectrum adapter and license (required for viewing spectrum data and non Wi-Fi devices; AirMagnet WiFi Analyzer Pro only). Integration supported with AirMagnet Spectrum XT.

Note: *Spectrum XT adapter is in the USB form-factor.*

Supported Wi-Fi Adapters

AirMagnet WiFi Analyzer requires a supported Wi-Fi adapter be operating on the computer running the application in order to capture Wi-Fi data.

For a list of supported adapters, refer to https://www.netally.com/wp-content/uploads/2019/12/AMM-Preferred-Adapters.pdf

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.

.ecp — 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.

Technical Support

AllyCare Product Support

NetAlly's AllyCare is our comprehensive support and maintenance program that offers expanded coverage for the products.

For more information, visit https://www.netally.com/support/.

Contact Us

Call toll-free in North America: 1-844-TRU-ALLY (1-844-878-2559)

Visit https://www.netally.com/contact-us/ for additional phone numbers. Scroll down and select your region to complete a web form and have a NetAlly representative contact you.

Installation

Checking Product Package Contents

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

- Product CD.
- Software License Agreement.
- Read Me First.
- A software certificate bearing the serial number and serial key.
- If a support contract was purchased, a support contract with a support serial number and serial key.

In case any items are missing or damaged, contact your AirMagnet authorized reseller or AirMagnet Technical Support immediately. Refer to Technical Support

Preparing for Software Installation

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. Refer to "System Requirements" on page 10.

Before You Begin

Consider the following items before installing, launching and using the software:

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

Product Upgrades

If the computer 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 My AirMagnet account where you can access the software upgrade download. The product upgrade is 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.

You can view the status of your support contract under the Registered Products section of your My AirMagnet account. Refer to Product Registration . For information about support contracts, refer to Technical Support.

Software License

You are 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 computer 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

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

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

MAC Address Reset

Should you desire to reset the MAC address to a different computer or adapter, you can request a MAC address reset by choosing “Mac Address Reset” from your My AirMagnet account.

Backing-up the License File

We recommend 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 just browse to the file to install it.

Installing Product Software

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. From the Registered Products page of your My AirMagnet account, click 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. Refer to Software License Agreement.

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 can 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 to decode the upper layers of your capture files. You may choose to install this feature as part of product installation. For license information, refer to Upper-layer decode support feature license.

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**.

2. You must agree to the GNU Library General Public License to proceed with 3rd party decodes installation.

3. You can 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 can choose to install it from within the application in the* **Configuration dialog>Filter** *tab.*

Product Registration

We recommend that you create a My AirMagnet account and register your AirMagnet software. By registering your purchased software, you are entitled to a free My AirMagnet account with the following benefits:

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

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

https://airmagnet.netally.com/support/register_product/

Support Contract Activation

If you purchased a support contract for your product, you must 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 My AirMagnet 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.*

Launching the Application for the First Time

When you launch the application for the first time, you will need to 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.

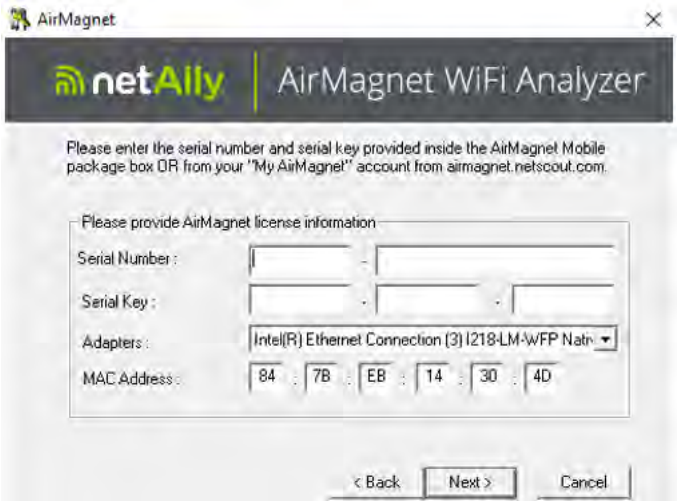
Bind the License to a MAC address

Choose to bind the license to one of two options:

- **The MAC address of the computer running the application**. If you chose this option, only that compute can run the application.
- **The MAC address of a removable Wi-Fi adapter**. To bind the license to a Wi-Fi adapter, it must be active on the computer running the application. Refer to Preparing for Software Installation. If you choose this option, that adapter must be attached to the computer running the application.

Supply the Serial Number and Serial Key

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



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

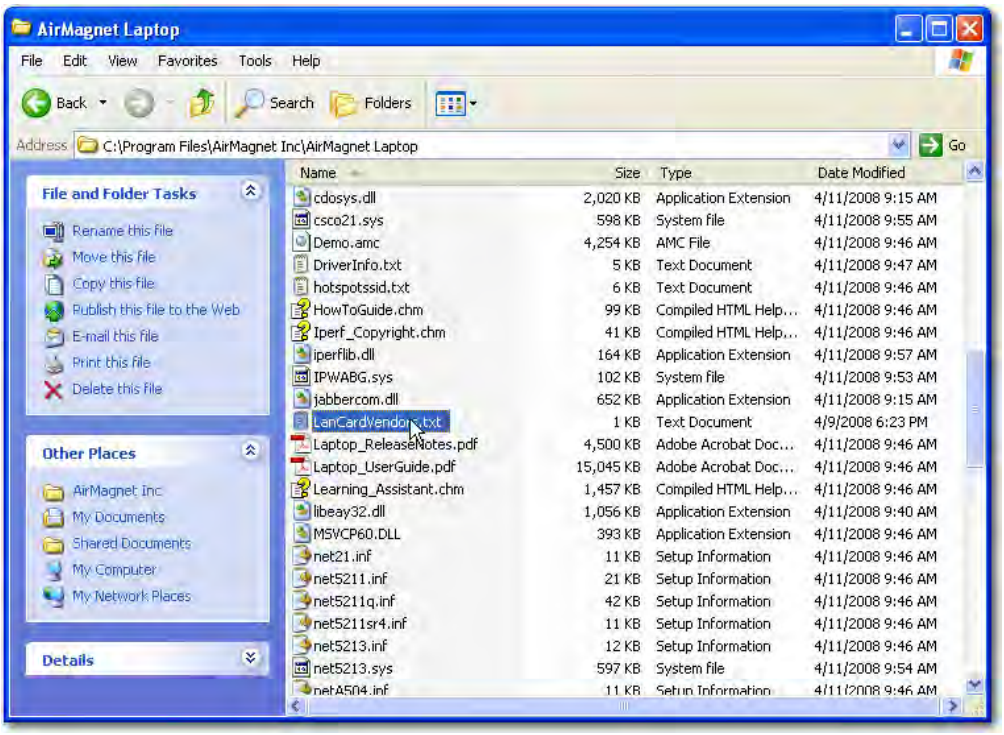
If you receive an error when attempting to install the software license, it may be for one of the following reasons:

- Your license does not support a newer version of the product. In this case, you can purchase a support contract that entitles you to run the newer software. Refer to Technical Support
- 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. Refer to Preparing for Software Installation

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.

Updating Wireless Networking Device Vendor List

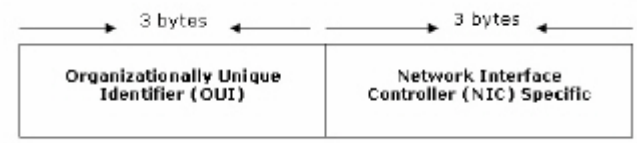
During the course of the AirMagnet WiFi Analyzer installation, a file named *LANCardVendors.txt* is automatically copied to the AirMagnet Wi-Fi folder.



The *LANCardVendors.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, that is, 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.



By default, MAC addresses of all existing wireless networking devices are already mapped with the names of their respective vendors. AirMagnet WiFi Analyzer’s Start screen 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 foran AirMagnet’s update.

To map MAC addresses with vendor names:

1. From your laptop PC, locate and open the *LANCardVendorsFile.txt* file.

2. 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.

Utilizing Multiple Wireless Adapters

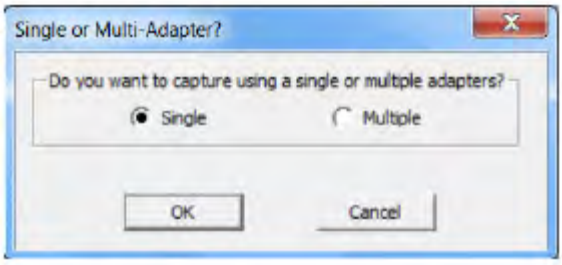
If the AirMagnet WiFi Analyzer computer has multiple AirMagnet-supported wireless adapters connected at the time you launch the application, you will be prompted to select the adapters that should be used by the process.

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

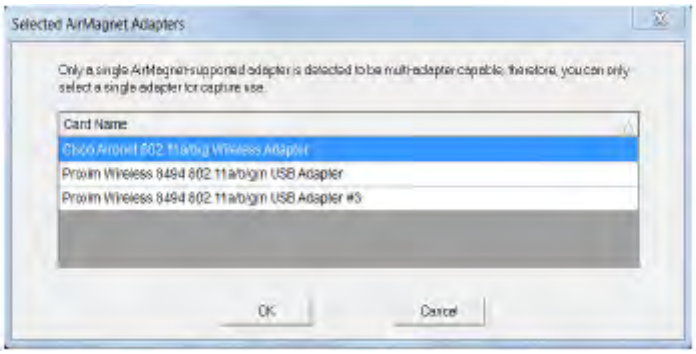
Refer to Configuring Channel Scan for information on Configuring Channel Scanning.

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

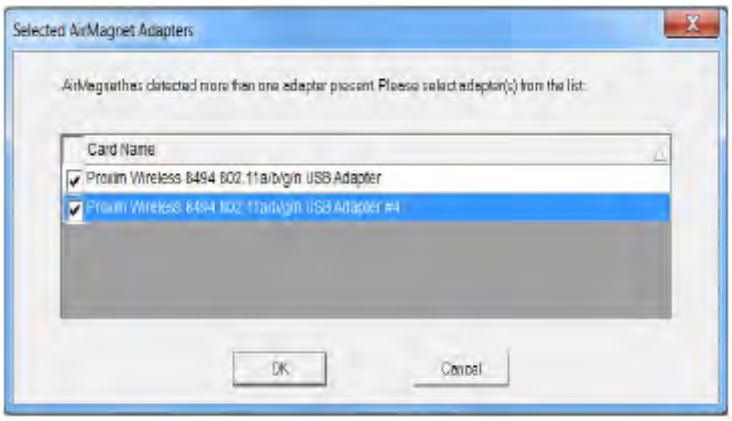
You can decide whether to use single or multi-adapter mode.



If you select single adapter mode, a dialog is presented to choose an adapter.

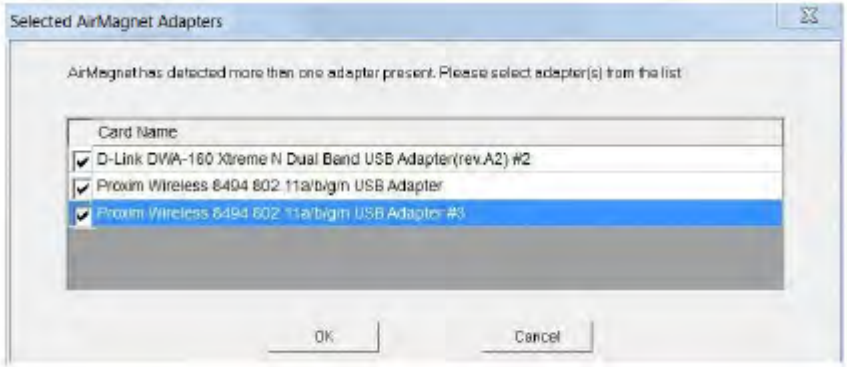


If you select multi-adapter mode, a dialog is presented to check the desired adapters.



When all adapters detected are multi-adapter capable:

You can specify use of up to three adapters at any given time. When running in multi-adapter mode, each active wireless adapter focuses on a single channel, allowing you to monitor all traffic on the selected channels simultaneously.

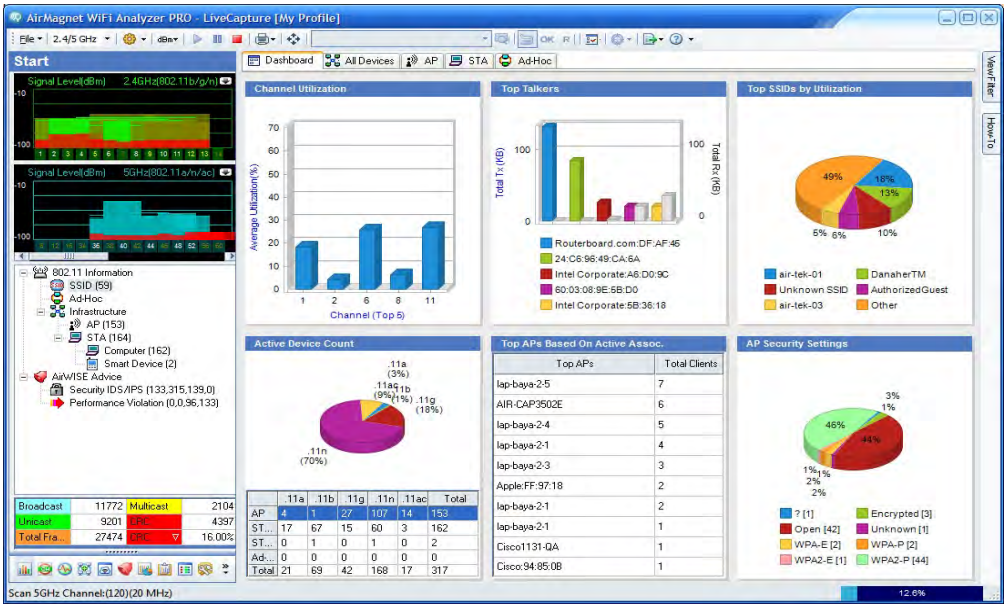


System Navigation

Launching AirMagnet WiFi Analyzer

From the desktop of your laptop PC, click **Start>All Programs>AirMagnet>AirMagnet WiFi Analyzer.**

The AirMagnet WiFi Analyzer's Start screen appears.



Major User Interface (UI) Components

The user interface consists of the primary major components as described in the following table:

Item	Description
Title Bar 	Located in the left part of the top of the screen, the title bar shows information about the application. When the application is operating in live capture mode, you will see "Live Capture" with the name of the current profile in parentheses, for example, [Sunnyvale, CA] in this case; if you are playing back an AirMagnet trace (*.amc*) file, you will see the name of the file and the progress of the file play-back in

	percentage. ***Note:*** *By default, WiFi Analyzer automatically names a trace (.amc) file by the date the file is saved, unless you change or rename it. For example, a trace file saved on Friday, February 29, 2008 is named "Friday, February 29, 2008.amc".*
Menu Bar 	Located right below the title bar, the menu bar contains tools and menus for operating the application. ***Note:*** *While some menus or tools apply to all major screens, some are available on certain screens only.*
Navigation Bar 	Located in the lower left-hand corner of the screen, right above the channel scan indicator, the navigation bar contains navigation buttons that allow you to navigate through the major screens of the application. Refer to here for more information.
Channel Scan indicator 	Located in the lower left-hand corner of the screen, right below the navigation bar, the channel scan indicator shows in real time the 802.11 radio frequency band and channels being scanned. The channels the application is configured to scan appear here in a revolving manner, determined by the frequency of the scans selected. However, if you set the application to scan one specific channel, then only that channel appears here. Also, you are focusing on a specific channel on the Channel screen, then only that channel appears here.
Buffer Status Indicator 	Located in the lower right-hand corner of the screen, directly opposite to the channel scan indicator, the buffer status indicator shows the status of the system buffer in percentage. Once it reaches 100%, the buffer will empty all

	data in it and start caching all over again as new data being captured. The same process repeats indefinitely as long as the application is running in live capture mode.
View Filter	Located along the upper right-hand edge of the screen, the View Filter allows you to select the type of data that are of the most interest or concern.
How-to-Guide	Located along the upper right-hand edge of the screen, immediately below the View Filter, the How-To Guide provides interactive online assistance that walks the user through some basic functions of the application.
Capture to Disk 	The 'disk' icon is shown in the lower right-most position of the application screen when the Capture to Disk function is enabled.

Navigation Bar

The Navigation Bar is located in the lower left-hand corner of the AirMagnet WiFi Analyzer user interface. It enables you to navigate to any of the major screens by clicking the corresponding navigation button. The figure below shows the default navigation bar.

As seen from the figure above, the navigation bar contains the following navigation buttons:

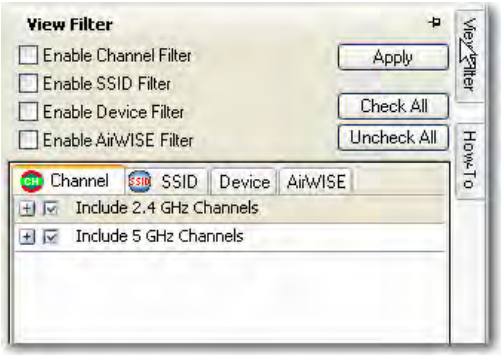
Navigation Button	Description
Start 	Opens the Start screen where you can have a quick overview of the state of your network.

Channel 	Opens the Channel screen where you can focus your attention on issues involving a specific channel.
Interference 	Opens the Interference screen where you can conduct detailed analysis of various sources of RF interference on your network.
Infrastructure 	Opens the Infrastructure screen where you can conduct detailed analysis about all devices detected on your network.
Roaming Analysis 	Opens the Roaming Analysis Screen, which allows you to troubleshoot roaming issues.
AirWISE 	Opens the AirWISE screen where you can focus your attention on analyzing various security and/or performance alarms that have been triggered on your network.
Top Traffic Analysis 	Opens the Top Traffic Analysis screen where you can visually analyze the most urgent issues in a specific category on your network.
Reports 	Opens the Reports screen where you can view various default network data reports as well as create custom report books.
Decodes 	Opens the Decodes screen where you can decode various packets that have been captured in the airwave in or around your network.
Wi-Fi Tools	Opens the Wi-Fi Tools screen which contains more than a dozen powerful, easy-to-use tools for troubleshooting and resolving network

WiFi Tools	issues.

View Filters

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



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

The View Filter pane contains four tabs: Channel, SSID, Device, and AirWise, each representing a specific type of filters. You can 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, that is, 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 (refer to Configuring Channel Scan Settings) 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

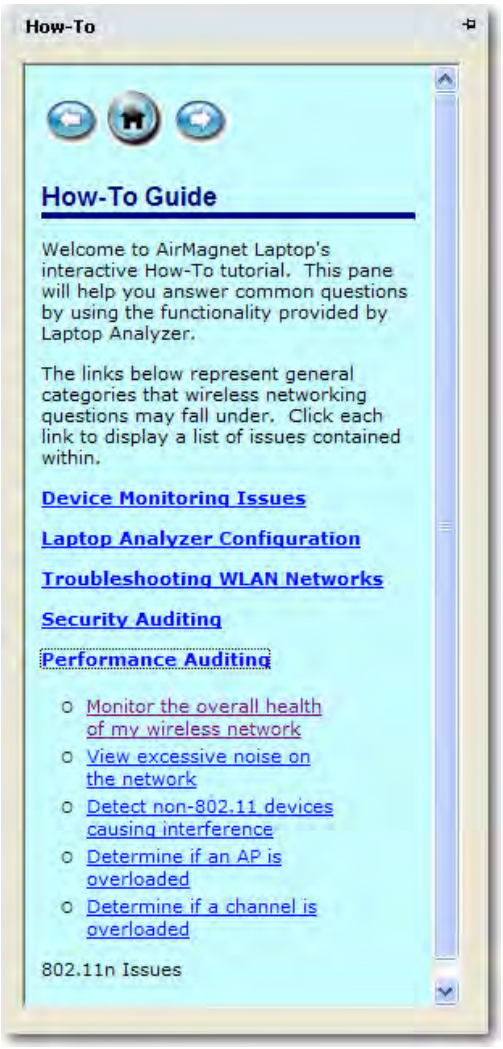
The AirWISE filter allows you to specify alarms to be shown onscreen based on the level of severity you specify. This way, you can focus your attention more on alarms that are of great interest to you.

To use the View Filter:

1. From the upper right-hand edge of the screen, click the **View Filter** button. The View Filter pane extends out.
2. Click the (left-pointing) push-pin to dock the View Filter pane to the right-hand side of the screen.
3. Use the options on the screen to narrow down the data to be displayed on the screen.
4. Click the (downward-pointing) push pin to close the View Filter pane.

How-To Guide

Located in the upper right-hand edge of the screen, the How-To guide provides the user context-sensitive assistance, especially new users, of AirMagnet WiFi Analyzer to get give a jump start on using the application. The illustration below shows the main page of the How-To guide.

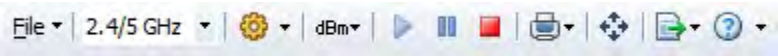


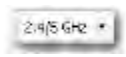
To use the How-To guide:

1. Click **How-To** in the upper right-hand edge of the screen.
2. Click the push-pin to dock the How-To guide pane to the right-hand side of the screen.
3. Click any link of interest to expand it.
4. Click the entry of interest to learn how to use it.
5. When you are done, click the push-pin to close the How-To guide.

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.



Item	Description
File menu 	The File menu provides the following command options: • **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. Refer to Open above. • **Save As**: Saves the file currently opened on the screen using a different file name or format. • **Configure**: Opens the AirMagnet Configuration 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 an AirMagnet sensor. • **Disconnect**: Disconnects the application from a laptop PC running in Remote Analyzer Mode or 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.
Band 	Select one of the following 802.11 band options for the bands you wish to scan. The options available correspond to the active Wi-Fi adapter's 802.11 protocol specification (a/b/g/n/ac). • 2.4 GHz (for 802.11b/g/n channels) • 5 GHz (for 802.11a/n/ac channels) • 2.4/5 GHz (for 802.11a/b/g/n/ac)

	• 4.9 GHz
Configure 	The Configure button contains two options in its drop-down menu: **Configure...** and **Policy Management...**. ***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.*
Toggle Percentage or dBm 	This button allows you to show data onscreen either by percentage or by dBm.
Live capture 	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. **Note:** *Pause Live Capture applies only to the Decodes screen.*
View Reports 	The View Reports button allows you to view reports based on data on the current screen and to set up your printer settings.
Full Screen 	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.
Dashboard 	The Dashboard Selection button allows you to customize the dashboard by selecting from a list of available charts and tables.
Easy View 	The Easy View button allows you to open a drop-down menu that contains the pre-configured viewing options for you to choose from.
Import /	The Import-Export button allows you to import or export an ACL as well

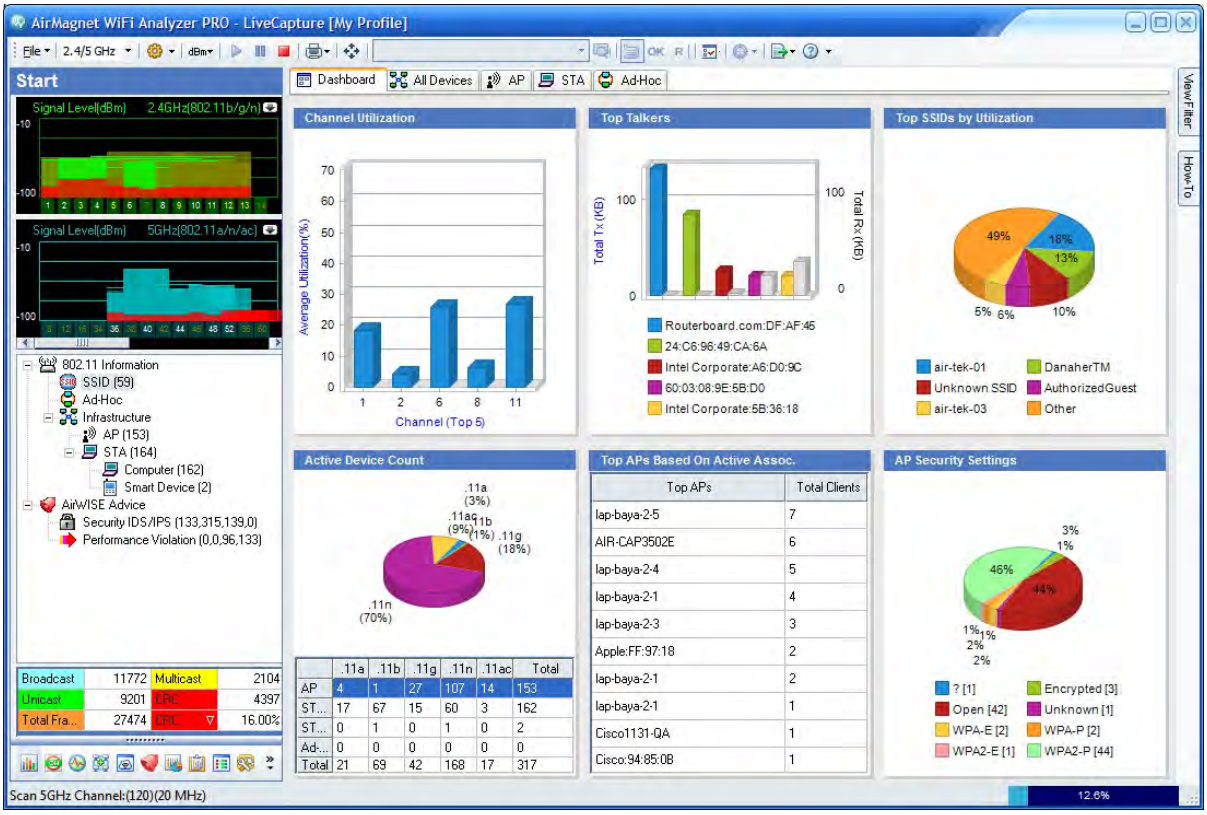
Export 	as some important data captured by the application.
Help 	The Help button contains three options in its drop-down menu: • Contents: opens AirMagnet WiFi Analyzer's online Help. • About: Opens the About AirMagnet dialog box which contains important information about this product. • Check Update: Checks the availability of software update.

Start Screen

About the 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 on your wireless LAN environment. You can get to the Start screen when you launch the program or, if you are on another screen, by clicking 

from the **Navigation Bar**. The figure below shows AirMagnet WiFi Analyzer's Start screen.



By default, AirMagnet WiFi Analyzer starts in live capture mode, as indicated by **Live Capture** on its title bar. From the Start screen, you can easily drill down to any specific channel, a WLAN component (for example, an access point or client station), or a security or performance alarm for further information or analysis.

WiFi Dashboard

AirMagnet WiFi Analyzer's usability-focused dashboard interface allows you to get a quick overview of the traffic in the wireless environment. By default, the Start screen displays the dashboard interface to provide a comprehensive look at traffic. It presents a quick snapshot of the overall health of your network without the need to dig for details. You can still dig for details by clicking on the desired statistic. The high-level statistics summary available are:

- Channel Utilization
- Channel Wi-Fi Interference
- Top Talkers
- 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

You can access the dashboard at any time by clicking the Dashboard tab located at the top of the Start screen.

By clicking the various charts in the dashboard, you can navigate to the respective screens of AirMagnet WiFi Analyzer's user interface. You can customize the charts provided using the Dashboard Selection button from the toolbar.

Start Screen Menu Bar

The menu bar on the Start screen (refer to the image below) contains some tools that are found only on the Start screen, in addition to all the commonly used menu and tool options. This section explains the tools that are specific to the Start screen only.

The menu bar on the Start screen provides the following tools that are found only on the Start screen. They are represented by icons shown towards the left-hand side of the menu bar (marked inside the red rectangle). You can learn the name of any of these tools from the tip screen that automatically pops up when you mouse over any of them.

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. Just 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 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 are grouped based on their media types: 802.11a devices show up first, then 11b, 11g, 11n, 11ac. 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 (that is, AP, STA, or Ad-Hoc).
- **View by 802.11n and ac**—This option allows you to view only 802.11n and 802.11ac devices currently active.

  Note: *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 appears 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.

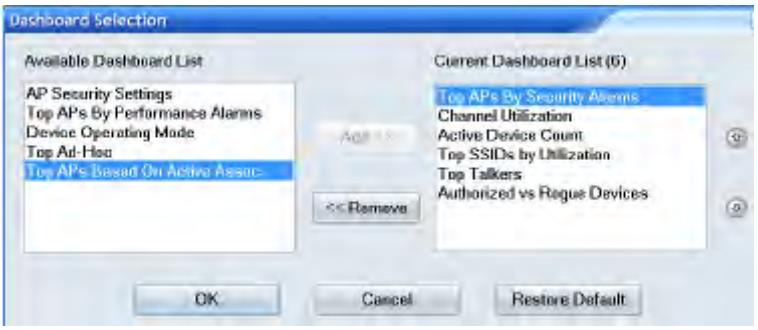
OK/R(ogue) Buttons

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. Just 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 Button

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. Y change the selection of currently shown high-level statistics by using the add-remove dialog. There is also a **Restore Default** button to restore the selection to a default list of items.



Dashboard Add Remove Buttons

Bubble Help Button

Bubble help provides tool tip information when enabled. The button appears enclosed inside a square box when enabled.

Full Screen Button

Full Screen enables you to toggle back and forth between a full screen view and partial screen view of each of the tabbed screens.

Start Screen Right-Click Menus

The Start screen, as its suggests, provides a starting point for identifying and solving your wireless network issues. It is loaded with a great amount of data AirMagnet WiFi Analyzer has captured since each session starts. To help fully understand and take advantage of the rich features shown on this screen, several parts of the Start screen is equipped with right-click menus that allow you to jump to action right away.

This following explains the parts of the Start screen that are equipped with a right-click menu and the contents of each of these right-click menus.

RF Signal Meter

This right-click menu contains options for setting or resetting the high-water mark in the RF signal meter. All you have to do is to right-click anywhere in the signal meter and select an option from the pop-up menu.

This right-click menu offers the following options:

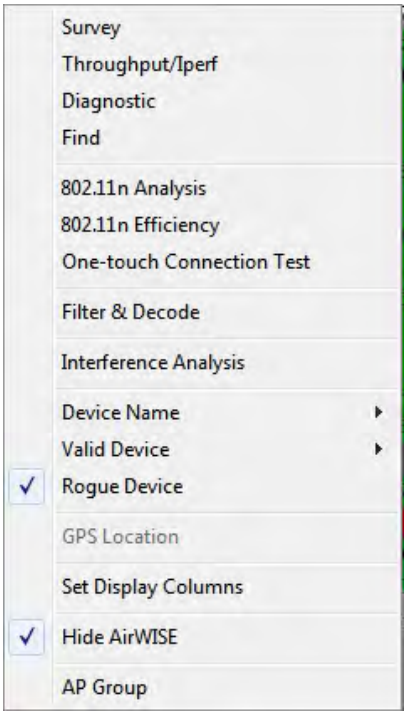
- **Set High Water Mark** - Opens **High Water Mark Setting** dialog box where you select a resetting frequency.

- **Never Reset** - Enables AirMagnet WiFi Analyzer never to reset the high water mark.
- **Auto Reset with 5 sec.** - Enables AirMagnet WiFi Analyzer to reset the high water mark every five seconds.
- **Auto Reset with 10 sec.** - Enables AirMagnet WiFi Analyzer to reset the high water mark every 10 seconds.
- **Reset Now** - Resets the high water mark the moment you click this option.

Live Network Data Pane

This right-click menu contains tools for solving issues related to the devices displayed on the Start screen. Some allows you to work directly from the Start screen while others enable you to easily navigate to other screens with a click of the button.

Note: *The options available depends on the media type of the device selected. For example an 802.11n device provides the 802.11n Efficiency option whereas an 802.11ac device provides the 802.11ac Efficiency option.*



This right-click menu provides options as described in the following table and bullet items:

Option	Description
Survey	Opens the **WiFi Tools>RF>Site Survey** screen.
Throughput / Iperf	Opens the **WiFi Tools>Additional Tools>Throughput / Iperf** screen.
Diagnostic	Opens the **WiFi Tools>Connection>Diagnostic**.
Find	Opens the **WiFi Tools>Additional Tools>Find**.
802.11n / ac Analysis	Opens either **802.11n or 802.11ac Tools>Analysis** depending on the devices

	media type.
802.11n/ac Efficiency	Opens either **802.11n or 802.11ac Tools>Efficiency** depending on the devices media type.
One-touch Connection Test	Opens the **WiFi Tools>Connection>One-touch Connection Test**.
Filter & Decode	Opens the **Decodes** screen.
Interference Analysis	Opens the **Interference** screen.
Device Name	Opens a pop-up menu which contains options for managing the way devices are displayed or identified on the screen.
Valid Device	Opens a pop-up menu which allows you to assign the selected (highlighted) device to an ACL group.
Rogue Device	Enables you to change a device's ACL status from valid device to rogue device.
GPS Location	Opens up the **AP GPS Location** screen where you can specify APs' GPS parameters, such as latitude, longitude, altitude, and antenna height,etc. ***Note:*** *You must check the Enable GPS Port option and complete GPS configuration in order to have this option available.* **Set Display Column** - Brings up the Field Chooser dialog box which allows you to decide what data (columns) are to be displayed on the Start screen. **Show/Hide AirWISE** - Allows you to

	show or hide the AirWISE pane at the bottom of the Start screen. **AP Group** - Brings up the AirMagnet Configuration>AP Grouping screen.

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 (refer to Device Data) while Dashboard is a high-level summary of your WLAN health.

RF Signal Meter

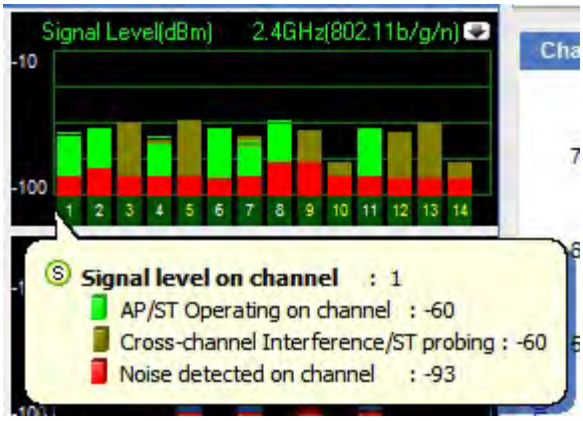
The upper-left part of the Start screen is the RF Signal Meter, which provides an overview of RF signal quality on all available channels, each represented by a bar. The bars implement a high watermark feature that shows the highest historical RF signal level each channel has reached within a user-specified interval (configurable under the General tab of the AirMagnet Configuration dialog box).

This part of the screen consists of two sections: the upper part shows the 2.4-GHz band and all available 802.11b/g/n channels while the lower part the 5-GHz band and all available 802.11a/n/ac channels.

Note: *Keep in mind that the channels available on the two bands are different and that the number of available channels for the same band may also differ among countries/regions of the world, depending on the regulatory rules in place in the locale where AirMagnet WiFi Analyzer is used.*

RF Signal Quality Codes

As seen from the screen, the channel bars are color-coded; the colors (green, brown, and red) change dynamically to reflect the real-time fluctuation in RF signal quality on the network. To find out RF environment conditions on the channel, you can mouse over any channel of interest. A tip screen will pop up momentarily, briefly describing the conditions on the selected channel.



For 2.4-GHz (802.11b/g/n) channels, RF signal quality is color-coded as follows:

- **Green:** Indicates 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,you should take action 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 can high packet error rates and disrupt wireless transmission, resulting in poor network performance or unstable network connectivity.

For the 5-GHz 802.11a/n/ac 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.

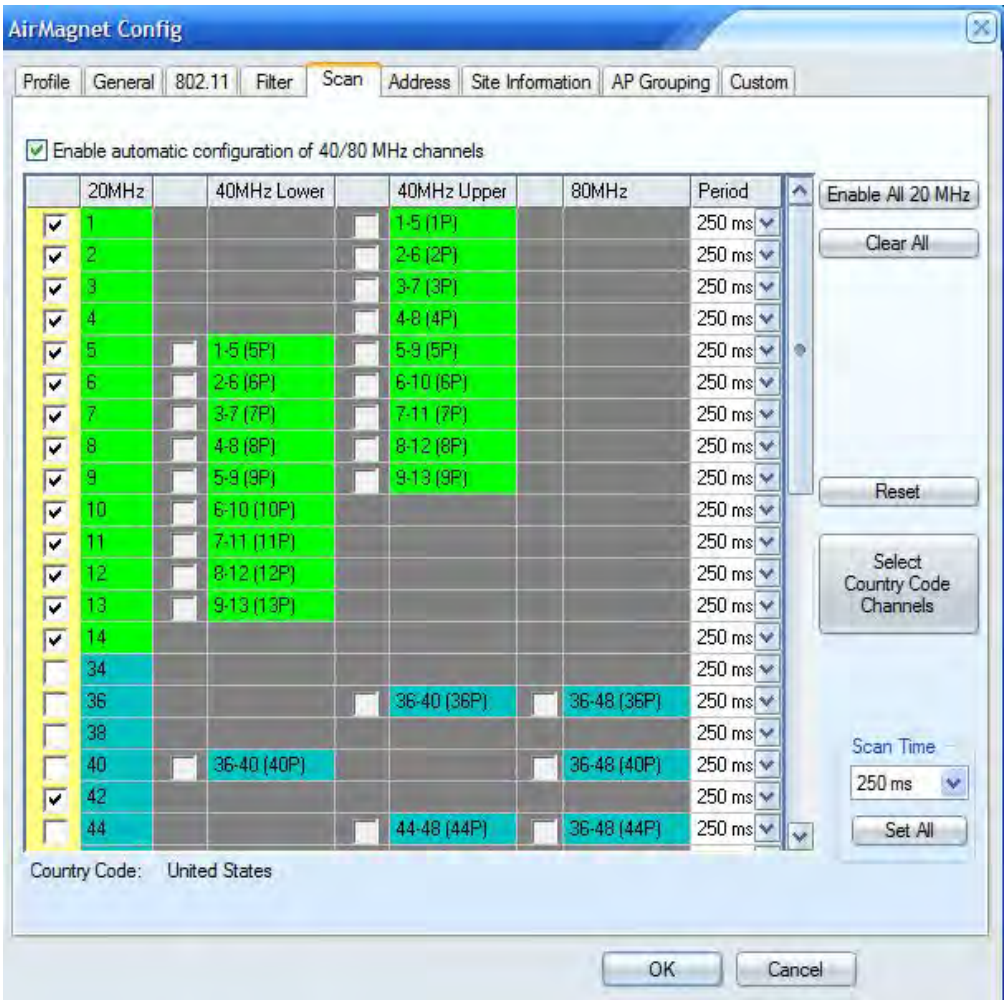
Expanding the RF Signal Meter

By default, the RF signal meter pane is contracted, only showing the consolidated RF data for each channel. You can expand the upper or lower part of the RF signal meter, one at a time, by clicking  (Expand) in the upper-right corner of each section of the signal meter. The expanded RF signal meter displays signal strength, noise level, signal-to-noise ratio, and interference score on each channel using separate graphs.

Restore the RF signal meter to its original state by clicking  (Contract) in the upper-right corner of the expanded signal meter screen.

Tips:

- 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 you are interested in 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 from **AirMagnet Configuration>Scan dialog box.** This enables AirMagnet WiFi Analyzer to focus on capturing traffic on known active channels while still keeping an eye on those unassigned channels for rogue APs and stations.
- Double-clicking a channel in the signal meter takes you directly to the Channel screen where you can conduct focused analysis about data on that channel.

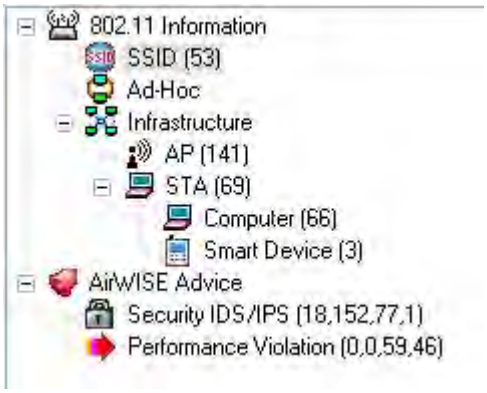


Data Summary

Below the RF signal meter is the network data summary. It presents a summary of some key network information:

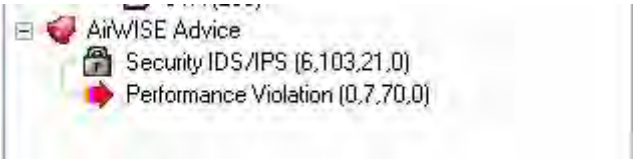
802.11 Information

It categorizes all the network components or devices detected on your wireless network and shows the total number of components or devices in each category. Notice that the Station (STA) count distinguishes between Computer(s) and Smart Device(s).



AirWISE Advice

It categorizes all the alarms detected on your WLAN into two groups: security and performance. There are four sets of digits for each category, representing different levels of severity. The digits, from left to right, represent number of alarms that are Critical, Urgent, Warning, or Informational.



Frame Count

In the lower-left corner of the Start screen is a tabulation of all frames AirMagnet WiFi Analyzer has captured on your wireless network.

The frames are categorized into the following groups:

- **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.

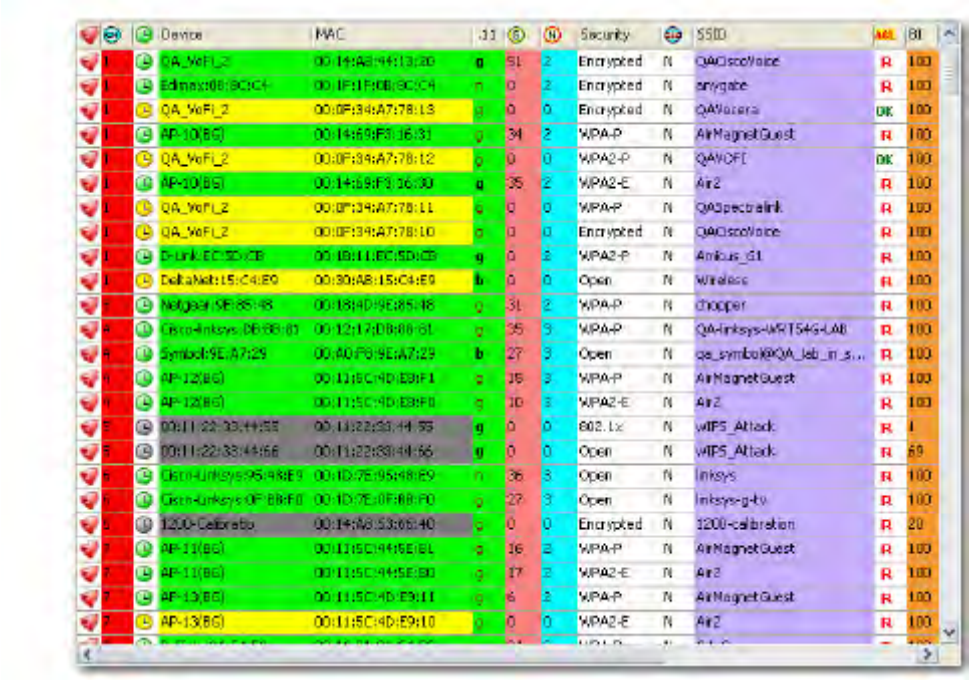
- **Unicast:** Unicast is a term used to describe communication where data are sent from one point to another point. There are only one sender and one receiver.
- **CRC:** Cyclic Redundancy Checks are used to verify packet information and reduce the potential for errors.

Tip: In order to display this part of the screen, you must select the Show Frame Statistics option in the AirMagnet Configuration>General dialog box.

Note: *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. Just 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 include 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.



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. (Refer to WiFi Dashboard).

All Devices

The devices are organized into three categories, as indicated by the collapsible sections: APs, Ad-Hocs, and STAs. 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 49 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, Tx Channel Width, Rx Channel Width, SGI, First Seen Time, and Last Updated Time.

Sort the data by any category just by clicking the title of that column, for example, 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.

Note: *"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 activates the AirWISE screen, which shows all alarms detected from that device; double-clicking in any other column takes you directly to the Infrastructure screen.

Item	Description
Type	Shows the category of the device which can be one of the following: • 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: • Red = Alarms are detected on the channel. • Yellow = No alarm is detected on the channel.
Active Time for	Displays the current status of the device. The icon is color-coded to display

Device	how long the device has been active: • 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. Refer to Configuring AP Grouping for more information.
Device	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: • 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).
.11 (802.11)	Type of 802.11 media,that is, 802.11b or 802.11g, the device is using. • Green = 802.11b • Orange = 802.11g • Blue = 802.11a • Green/Blue = 2.4 GHz 802.11n/5 GHz 802.11n • Purple = 5 GHz 802.11ac
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	Displays the interference score of the channel.

Score	
Security Mechanisms	Indicates the security mechanisms used on the device: • WPA-P = WPA-Personal. • WPA-E = WPA-Enterprise. • WPA2-P = WPA2-Personal. • WPA2-E = WPA2-Enterprise. • VPN = PPTP, IPsec, Secure Shell, and so on. • Open = no security mechanism in place. • Encrypted = packets are encrypted, but the specific encryption mechanism is not known. • ? = Security mechanism is unknown. Devices using multiple SSIDs will display the security settings for each SSID implemented, separated by commas.
TKIP/MIC	Shows TKIP/MIC security settings: • Y = Enabled. • N = Disabled. • U = Unknown. Devices using multiple SSIDs will display the security settings for each SSID implemented, separated by commas.
Bridge Mode	• Y = Bridge Mode. • N = Non-Bridge Mode.
SSID	Displays the SSID of the device.
ACL Status	Shows the ACL status of the device. ***Note:*** *When AirMagnet WiFi Analyzer is launched for the first time upon installation, all devices detected are shown as U (Unknown). You must change the ACL status of all the devices one by one. Do this 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 all devices are marked R (Rogue), all devices will show up as U (Unknown) if you restart the application after exiting it.*

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: • 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.
Last	Displays the time the last packet was received.
Cell Power	Shows the power level at which the AP is transmitting in dBm.
Note:	***The following are applicable to View by 802.11n only.***
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: • PCO active in the BSS. • PCO inactive.
Greenfield Supported	Indicates whether Greenfield transmission is supported, which can be either of the following: • 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.
HT Protection	Indicates the HT protection 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: • 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) • Y = Use protection due to OBSS. • N = No protection due to OBSS.
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 Reduced Interframe Space (RIFS) mode for 802.11n devices as either permitted or prohibited.
Tx STBC	(Tx STBC Supported) Indicates whether Tx STBC is supported, which can be either of the following: • Y = Supported. • N = Not supported.
Rx STBC	(Rx STBC Supported) Indicates the state of Rx STBC support, which can be one of the following:

	• 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: • Y = Yes. • N = No.
SM Power Save	Displays SM Power Save.
Dual Beacon	Indicates whether Dual Beacon is used: • Y = Secondary beacon is transmitted by AP. • N = No secondary beacon is used.
Dual CTS Protection	Indicates wether Dual CTS Protection is required: • Y = Required. • N = Not required.
L-SIG TxOP Full Support	Indicates whether L-SIG TxOP is supported: • Y = All HT STAs support LSIG TxOP Protection. • N = One or more HT STAs do not support LSIG TxOP Protection.
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. (Refer to 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. (Refer to 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. (Refer to WiFi Dashboard).

Live Network Data Pane

The upper right-hand side of the Start screen is the live network data pane that displays comprehensive data about all wireless devices detected on your WLAN. The main part of this section is a table that can display more than 30 types of device data, one in each column of the table.

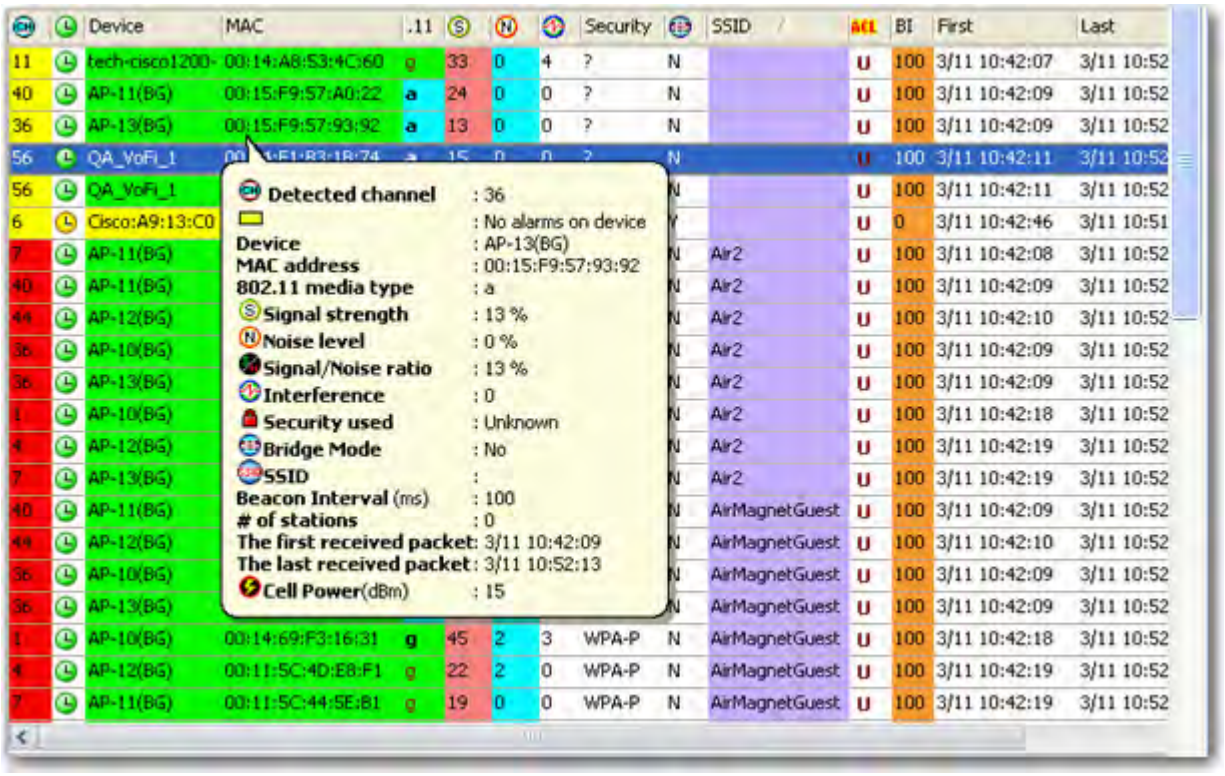
Tips:

The following are some tips to help you effectively use this part of the Start screen.

- The devices are organized into three categories: APs, Ad-Hocs, and STAs. You can choose to show or hide any category of devices by clicking the "+" or '-' sign at the beginning of that section.
- You learn the meaning of the data in any column by mousing over the title of that column --the tip screen that pops up will provide a brief description about the data.

Note: *You must enable Bubble Help to take advantage of this feature.*

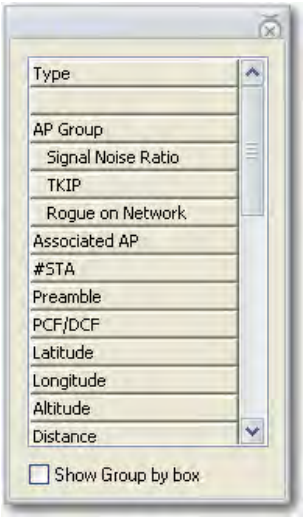
- You can review various data about a device on the screen by mousing over any field in the table. Again, you must enable Bubble Help in order to take advantage of this feature.



- Sort the data by any category by clicking the title of that column, for example, SSID.
- Use the horizontal scroll bar at the bottom of the table to view data that may be hidden from the screen.
- Choose or change the types of data to be displayed in this part of the screen.

To select data for screen display:

1. Right-click anywhere in the table and select “Set Display Columns” from the pop-up menu. The **Field Chooser** dialog appears.



2. The boxes in the Field Chooser dialog represent potential column headings; drag-and-drop them 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 column from the table.
4. Check the **Show group by box** option to display the different data type in a stacking order.
5. Close the dialog box when done.

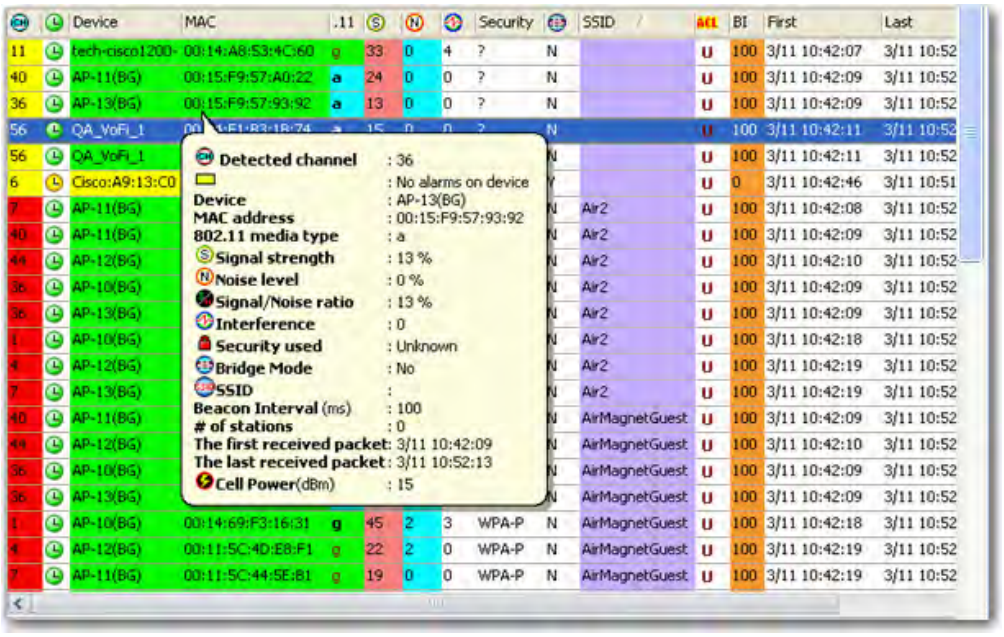
Locating a Wireless Device from the Start Screen

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 brings up AirMagnet’s **Find Tool**, which allows you to physically locate the device. For instructions on how to use the **Find Tool**, refer to Locating Rogue Devices.

Using Bubble Help

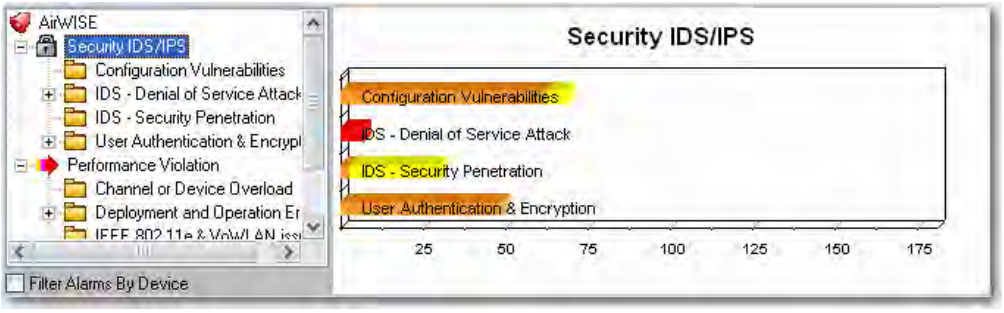
The  (Show/Hide Bubble Help) button allows you to enable or disable the bubble help, which is a context-sensitive tip screen that is only available for the Signal Meter, 802.11 Information and AirWISE Advice, and Device Data sections of the Start screen. It provides helpful information these parts of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



AirWISE Details

Below the device data section is the AirWISE section, which presents detailed information about all the network alarms that have been triggered. This part of the screen is made up of (left and right) two parts. On the left are the security and performance alarms, each being further broken down in various sub-categories. On the right is a bar chart that displays the number of alarms in the selected category.



Note: *In the lower left-hand corner of this section is the Filter Alarms by Device check box. Normally, the AirWISE pane displays information about all the alarms triggered by all the devices (that is, APs, STAs, or Ad Hoc) displayed on the screen. However, if the Filter Alarms by Device is checked, the AirWISE pane section will only display information about the device, whether it is an AP, station, or ad hoc station, you select from the live traffic data pane above.*

Tips:

- In order to display the AirWISE pane, you must select the **Show AirWISE** option in the Configuring General System Parameters dialog box.

- You can hide the AirWISE pane from the Start screen by right-clicking it and then clicking **Hide AirWISE** from the pop-up menu.

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, that is, 802.11a/b/g/n/ac. 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.

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

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
802.11ac	5	200 – 250	1 Gbps	~90	TBD

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 WiFi Analyzer currently provides the only WLAN analysis software that is capable of monitoring the 4.9-GHz band.

Note: *The 4.9-GHz feature only functions with 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.

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/ac 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.

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, and so on.)	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, refer to Saving Captured Data.

Accessing Data Reports

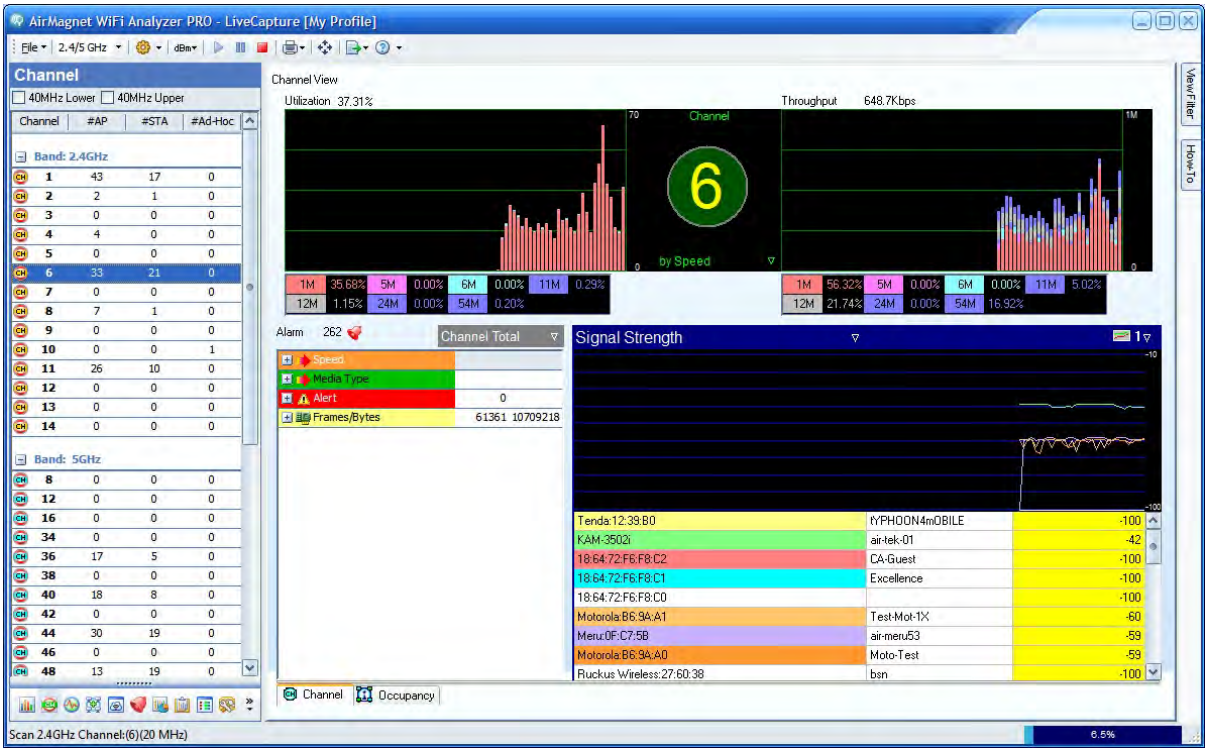
The integrated AirMagnet Reporter automatically converts all on-screen data into reports. The content of the reports are screen-specific, making them easy to view, analyze, share, and archive. You can find detailed instructions on how to use the Reporter in the Report Pane.

Channel Screen

About the Channel Screen

The Channel screen lets you focus on issues involving various wireless devices on a selected channel. You can navigate to the Channel screen at any time by clicking Channel

on the navigation bar.



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. Channels are listed based on the Band setting selected on the toolbar (2.4 GHz, 5 GHz or both).

Channels are scanned based on the Channel settings in the **Config>Scan** tab. Refer to Configuring Channel Scan. These settings can be temporarily overwritten by the option described below. The Channel settings are restored once you navigate away from the channel screen.

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.

As each channel is scanned, the channel number is displayed in the Status bar at the bottom of the user interface.

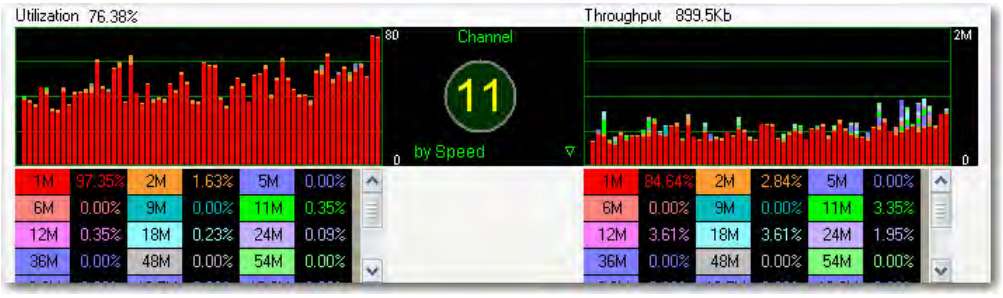
If a channel includes Upper or Lower 40 MHz, the status bar will include this information as the channel is scanned.

For a channel that includes Upper or Lower 40 MHz, channel scanning may be further defined using the check boxes at the top of the Channel Selection pane. The check boxes enable you to focus on HT packets being scanned as described in the following bullet points:

- **Lower 40 MHz** — If selected, the 40-MHz lower channel is shown. Packets are scanned in the 40 MHz lower channel and in the 20 MHz channel.
- **Upper 40 MHz** —If selected, the 40-MHz upper channel is shown. Packets are scanned in the 40 MHz upper channel and in the 20 MHz channel.
- **80 MHz** — If using a supported 802.11ac adapter, you may choose to scan packets in the 80 MHz channel.

Click a channel listing in the Channel Selection pane and its details are displayed on Channel screen to the right of the Channel Selection pane.

You can switch from one channel to another by clicking a channel listing in the Channel Selection pane. Once a channel is selected, AirMagnet WiFi Analyzer locks 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.



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 utilization graphs above. If the entire graph is red, virtually all packets on your network are being transmitted at 1 Mbps.

Link Speed and Media Type

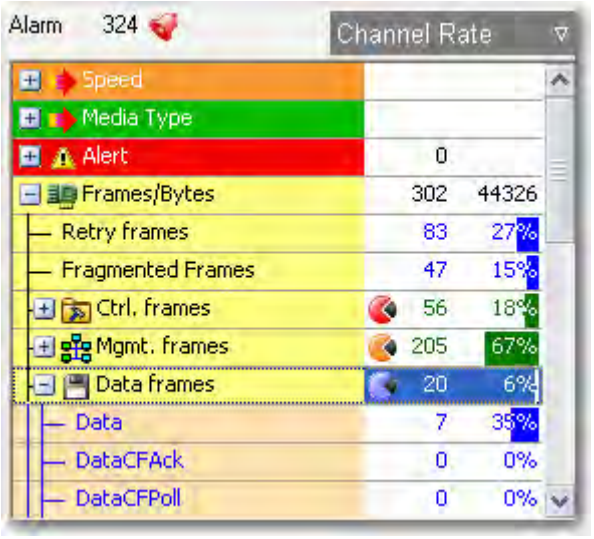
When you are using 802.11g, a/g, or a/b/g/n/ac for your media type, a filter appears below the channel number, allowing you to toggle the data display between link speed and media type. Both link speed and media type are color-coded. Selecting by Speed displays the different rates at which data are being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

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 displays the number of alarms triggered on the channel. Clicking takes you to the AirWISE screen, where a detailed explanation about the alarm(s) and expert advice.

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.



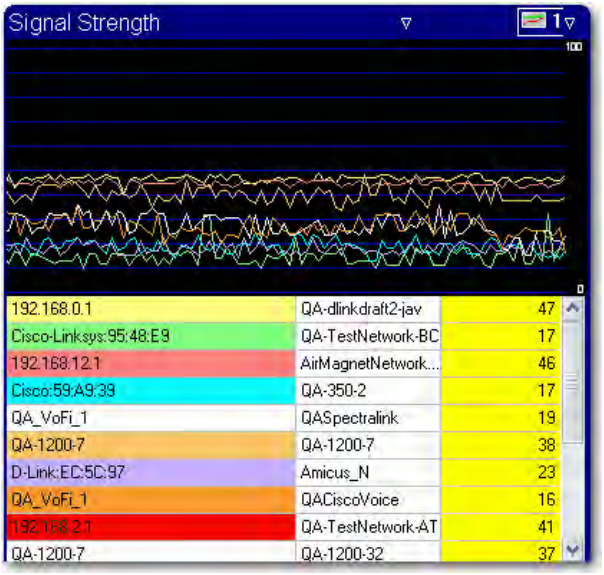
Button	Description
	Summarizes link speed of the channel.

	Summarizes the types of media discovered on the channel.
	Lists frame error code information.
	Divides frame and byte counts into retry frames, fragmented frames, control frames, management frames, data frames, and CRC error frames, and so on.
	Summarizes control frames/bytes.
	Summarizes management frames/bytes.
	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

This part of the Channel screen displays the various types of network data as a line charts. 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.



This figure 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 the 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.

Variations of the Channel Screen

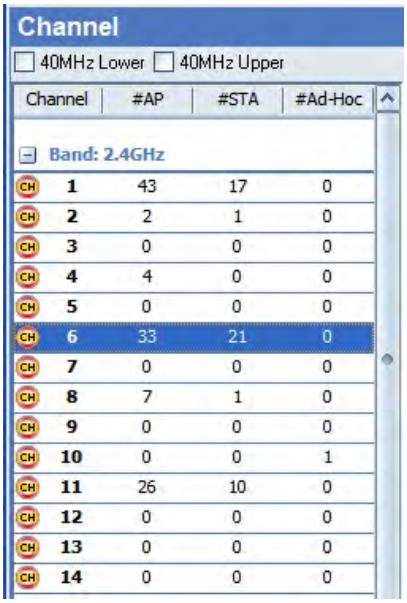
The Channel screen comes in two variations: Channel and Occupancy. The former is used for analyzing RF conditions on a selected channel whereas the latter is for analyzing the state of channel occupancy or usage by media band. You can switch between the two by clicking the **Channel** or **Occupancy** tab at the bottom of the screen.

Analyzing RF Conditions by Channel

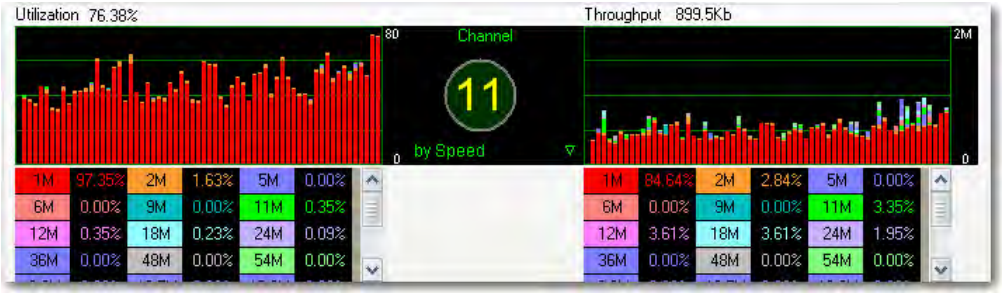
By default, the Channel tab is automatically selected when the Channel screen opens. This version of the Channel screen allows you to view and analyze in great detail the huge amount of RF data captured on each channel of the wireless network. Not only does it provides a head count of each type of device on each channel, but also allows you to focus on one particular channel at a time for in-depth analysis.

The screen consists of the following sections:

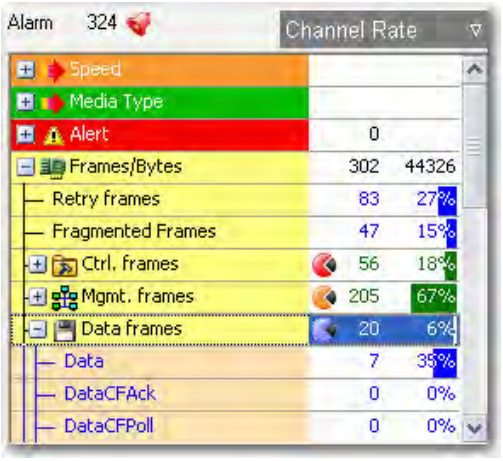
- **Device Count by Channel** - This part of the screen displays all available channels by media band (that is, 2.4 GHz vs. 5GHz) and the number of wireless devices in each of the three device categories (that is, AP, STA, and Ad Hoc) on each channel.



- **Channel Utilization and Throughput** - This part of the screen shows real-time utilization (left) and throughput (right) statistics of the selected channel. The number in the middle indicates the channel you are currently focusing on. You can display data by speed (default) or by media band by clicking the down arrow and select the desired option from the drop-down list menu.

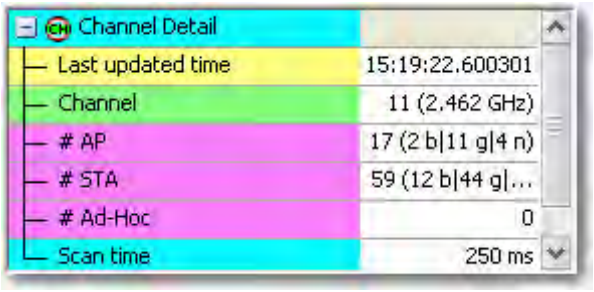


- **Channel RF Data Analysis** - This part of the screen provides detailed data analysis in the four categories (speed, media type, alert, and frames/bytes), each of which can then be further divided into another of subcategories. You can view the statistics either by Channel Total (default) or Channel rate by clicking the down arrow in the upper-right corner of this part of the screen and select either one. The number in the upper-left corner of this part of the screen indicates the total number of alarms that have been detected on the current channel.



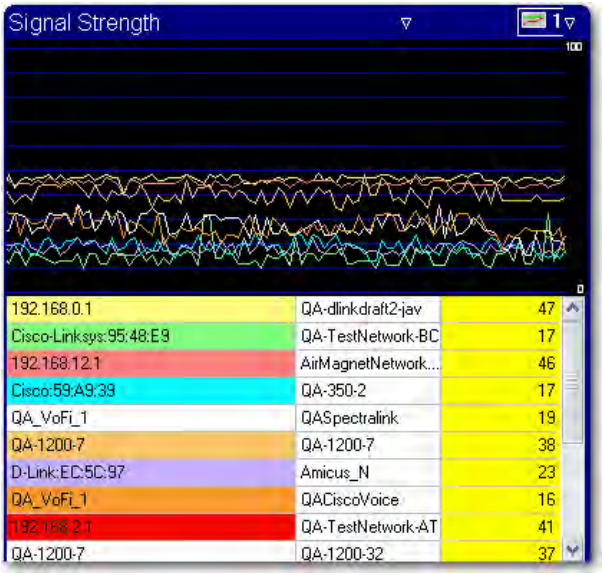
- **Channel Detail** - This part of the screen displays some key statistics about the current channel.

Note: *You may need a larger screen display or increase your screen resolution in order to show this part of the Channel screen.*



- **Data Graphs** - This part of the screen allows you to display 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.

Note: *The bottom of this part of the screen displays information related to the type of data that is being selected from the data filter above. The default graph (Signal Strength) displays the devices on the channel; these devices are graphed on the screen. The colors for each device correspond to the color their lines will be graphed in above. If any of the devices have a value of zero on the far right, their graphs will not appear.*

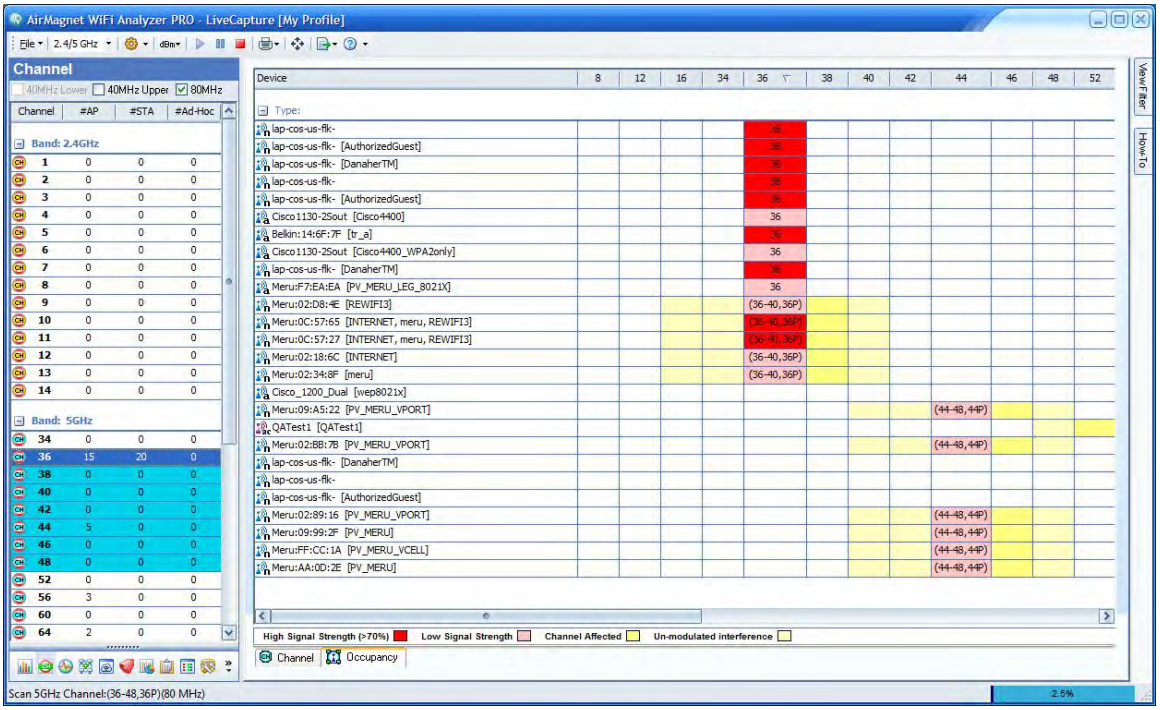


Analyzing Channel Occupancy by Frequency Band

The Channel Occupancy screen provides 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 and 80 MHz channels, the channel range is indicated followed by the primary channel (P). For example (44-48, 44P) indicates 40 MHz channel with primary on channel 44.
- The device’s modulated spectrum usage, as indicated by the yellow cells in its row; and the device’s unmodulated spectrum usage, as indicated by the light yellow cells in its row.



The example screen above displays the following information about the first 5 devices listed:

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

You can also view the following information about the 7th and 8th devices listed:

- These devices are operating on 40 MHz (Lower), channel 11.
- The modulated interference extends two additional cells on either side of the center frequency, as compared to the 20 MHz devices discussed above.
- The unmodulated interference extends all the way to channel 1.
- There is a 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).

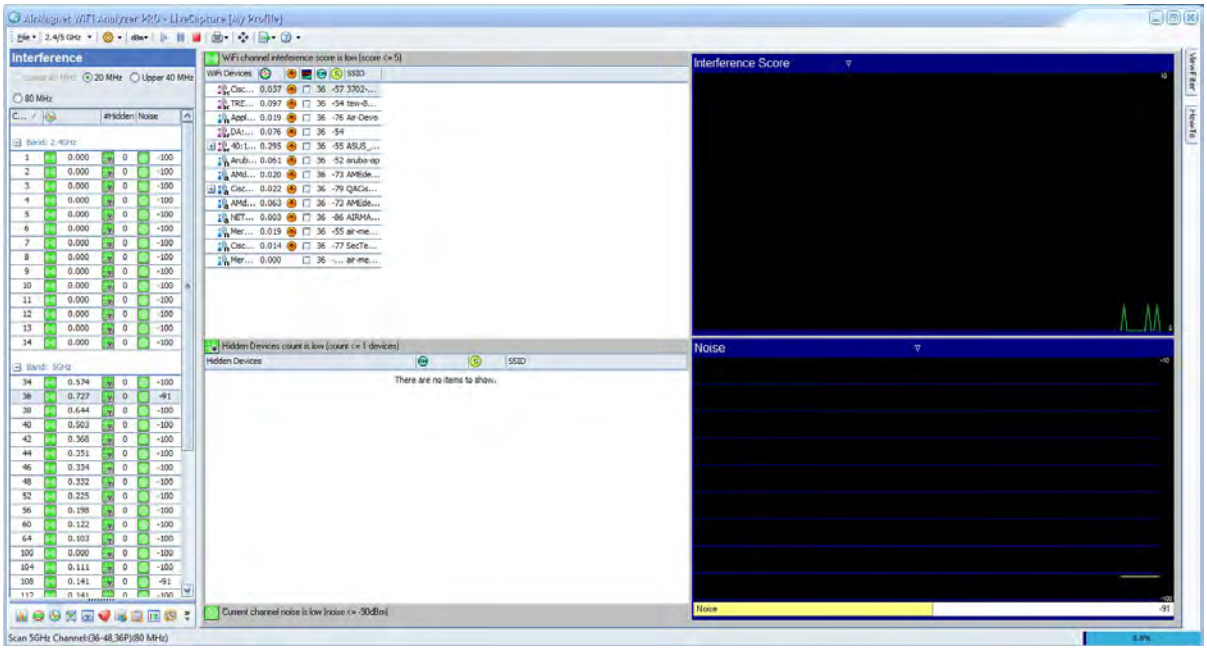
Note: *The 2.4-GHz and 5-GHz channel occupancy differs from each other, in the fact that the 5-GHz channels are spaced 20 MHz apart, as compared to 5 MHz for the 2.4-GHz channels. Thus, devices will take up less cells in the 5-GHz view than the 2.4-GHz view.*

Interference Screen

About the Interference Screen

The Interference screen allows you to view and analyze RF signal interference on a given channel. You can navigate to the Interference screen by clicking 

on the navigation bar. The following figure shows the Interference screen.



The Interference screen enables 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.

Note: *A channel's interference score is calculated based entirely on standard Wi-Fi 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.*

Interference Scores

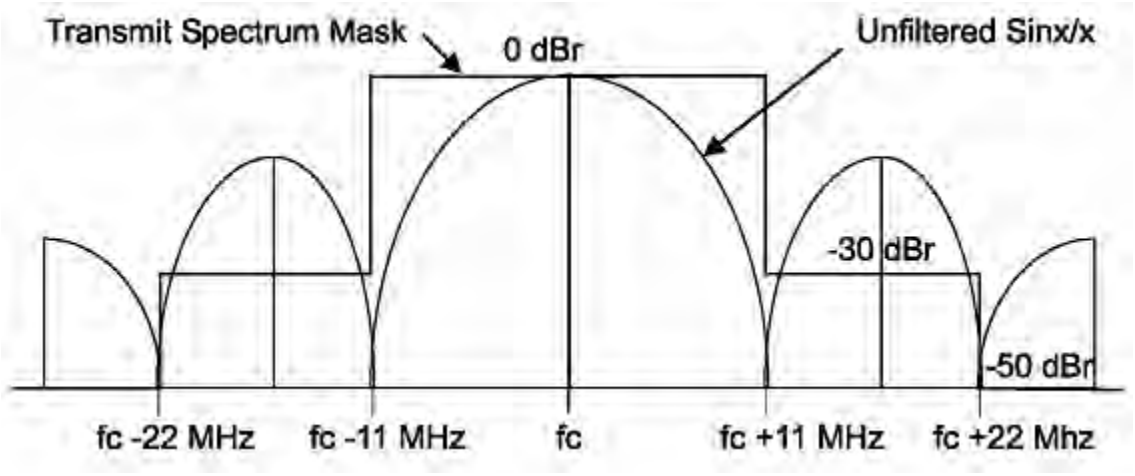
A channel's interference score is calculated based entirely on standard Wi-Fi devices. Each device operating on the selected channel or on adjacent channels will generate interference on the channel you are focusing on. The displayed interference score adds up the interference caused by all these devices 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 Spectrum Analyzer integration), the displayed interference represents the total of all standard interference generated on the selected channel by 802.11 devices (APs, Wi-Fi devices, wireless stations, and so on). Any non-802.11 interference shows 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 (that is, objects or devices that are causing this noise), you can purchase AirMagnet Spectrum Analyzer and integrate it with AirMagnet WiFi Analyzer. Refer to AirMagnet Spectrum Analyzer Integration.

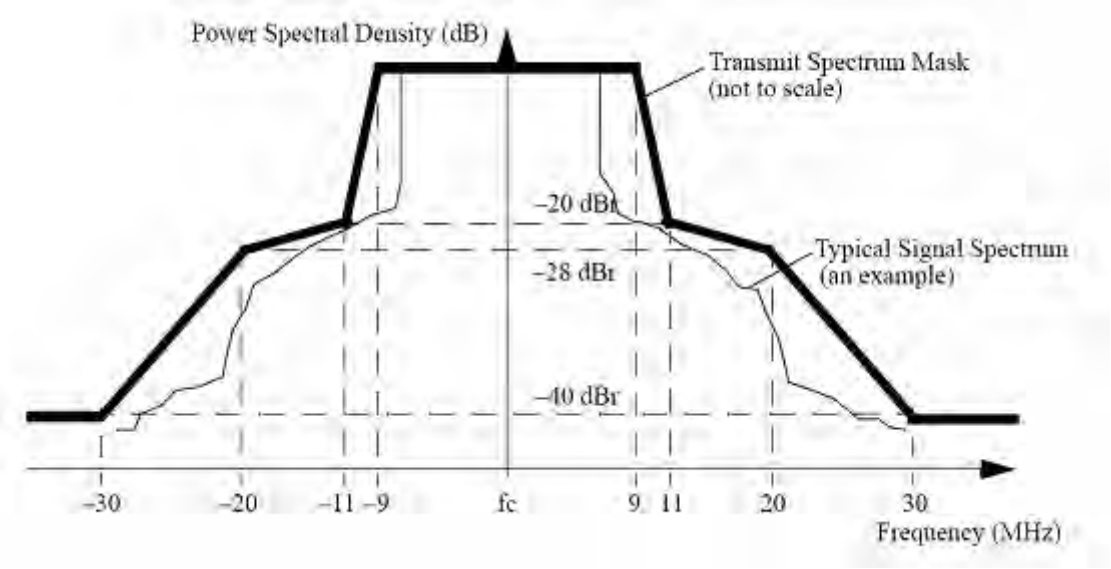
Interference Calculations

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.

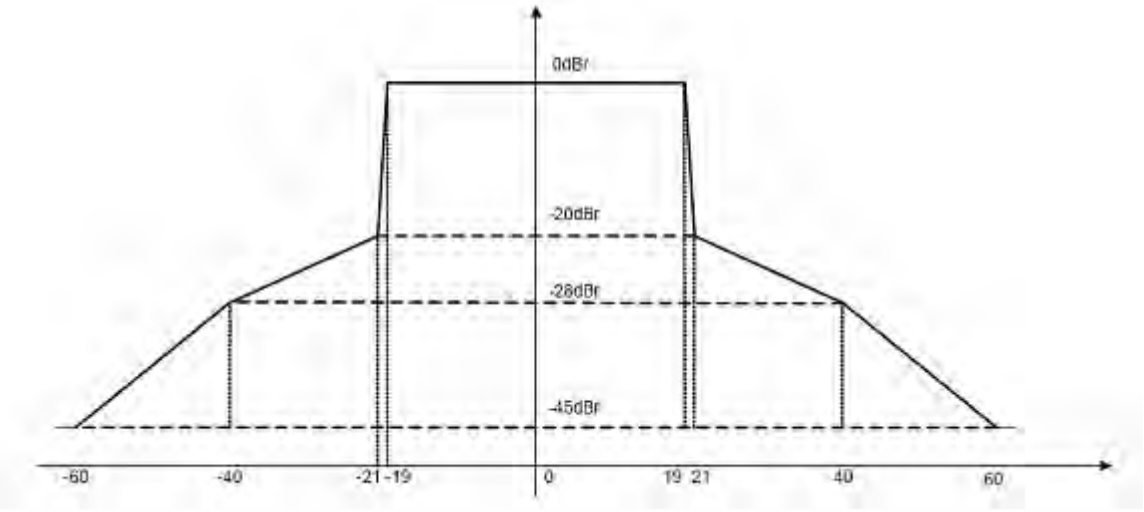
The following transmit spectrum masks are defined in the 802.11 standard (and/or its amendments):



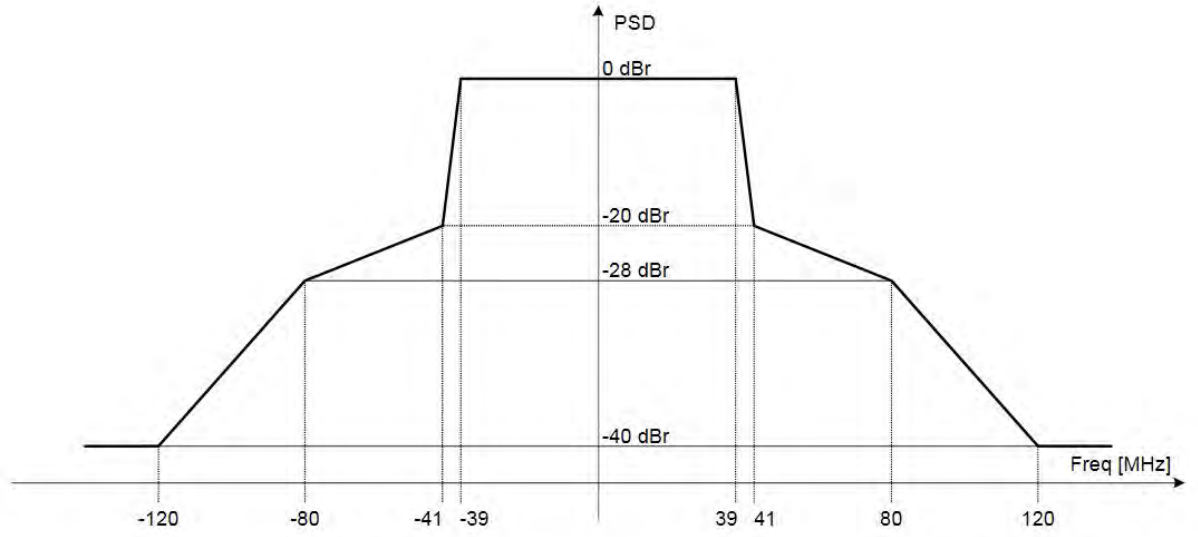
Transmit Spectrum Mask for 802.11b



Transmit Spectrum Mask for 802.11a/g (20 MHz)



Transmit Spectrum Mask for 802.11n (40 MHz)



Transmit Spectrum Mask for 802.11ac (80 MHz)

As illustrated in the figures above, 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:

- The “spectral distance” between the channel of interest and a device’s operating channel (including each of the channel’s widths).
- Whether or not the interference from a device (to a channel) is caused by modulated spectrum (that is, within the device’s operating channel width), or by the “bleed over” outside the modulated portion of the transmission(s).
- The RSSI (signal strength) of the device.
- 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. Refer to the Interference Screen.

Interference Statistics by Channel

The left-hand portion of the Interference screen shows interference statistics by channel. It provides a brief overview of the overall state of interference on each available channel, enabling you to easily and quickly identify the channel or channels that require attention.

Based on the channel selected and adapter capability (802.11a/b/g/n/ac), the radio buttons at the top (Lower 40 MHz, 20 MHz, Upper 40 MHz and 80 Mhz) enable you to focus on the desired channel width.

This part of the screen contains four data columns (from left to right):

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

Note: *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.

Note: *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. The table below provides a list of the color thresholds for each column.

Data Type	Color Codes and Interference		
Interference	0-5	5.01-20	20.01 or above
Number of Hidden Devices	0-1	2-5	6 or above
Number of Noise-Causing Sources	0-1	2-5	6 or above

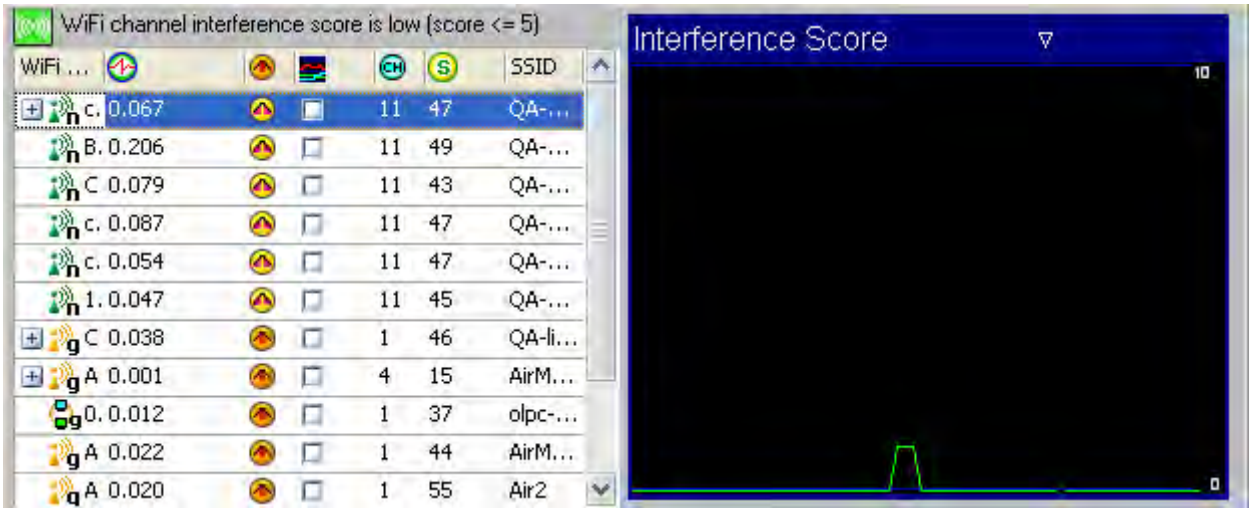
- **The third column** - Displays the number of hidden devices detected on the corresponding channels. Hidden devices can cause interference and traffic collisions within your network, thereby slowing down general network operations (for more details regarding hidden devices, refer to Hidden Station Detected).
- **The fourth column** - Displays the number of non-802.11 interfering devices detected; these devices are displayed in the "Hidden Devices" pane on the right.

Note: *The #Interferers column will only contain information if you have integrated AirMagnet Spectrum Analyzer and are using a AirMagnet Spectrum Analyzer card.*

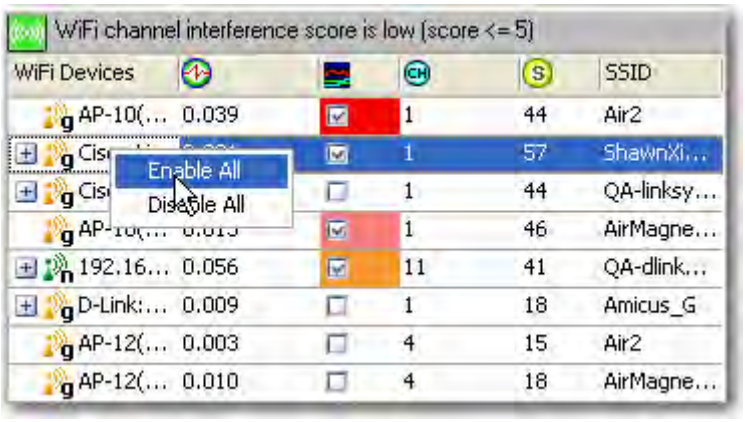
When a particular channel is selected, all areas in the right-hand side of the Interference screen are updated to show interference- or noise-causing devices that are detected on that channel. Refer to the Interference Analysis pane.

Channel Interference

The channel interference 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, 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.



Use the check boxes in the middle column of the table to select the devices to be graphed on the Interference Score graph. 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.

Note: *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.*

Channel Hidden Devices

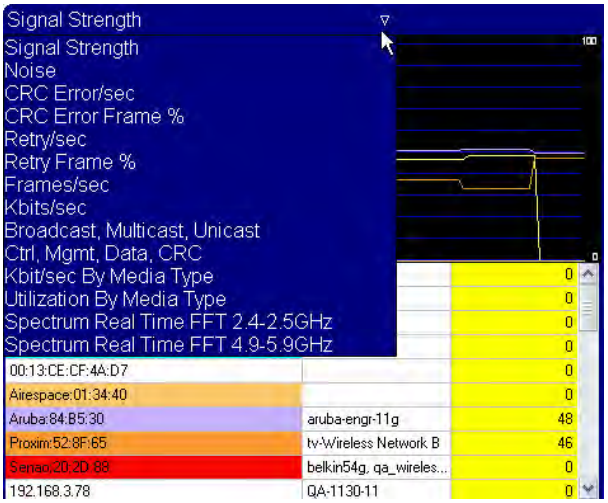
The Hidden Devices pane is located right below the Wi-Fi interference devices pane. It displays all hidden devices, if any, that are detected on your network. It provides information such as device name, channel, signal strength, and SSID of each hidden devices

being detected. The message across the top of this section tells you about the total number of hidden devices detected on the channel.

Hidden devices are a problem that happens when or where two wireless devices (for example, stations) cannot see each other directly (often due to distance between them). Since they are unaware of each other, they may try to access the same AP between them at the same time, causing network collisions. This would cause both stations to re-transmit their packets, thus creating delays network traffic. For more information on hidden devices, refer to the "Hidden Station Detected" AirWISE alarm.

Channel Data Graph

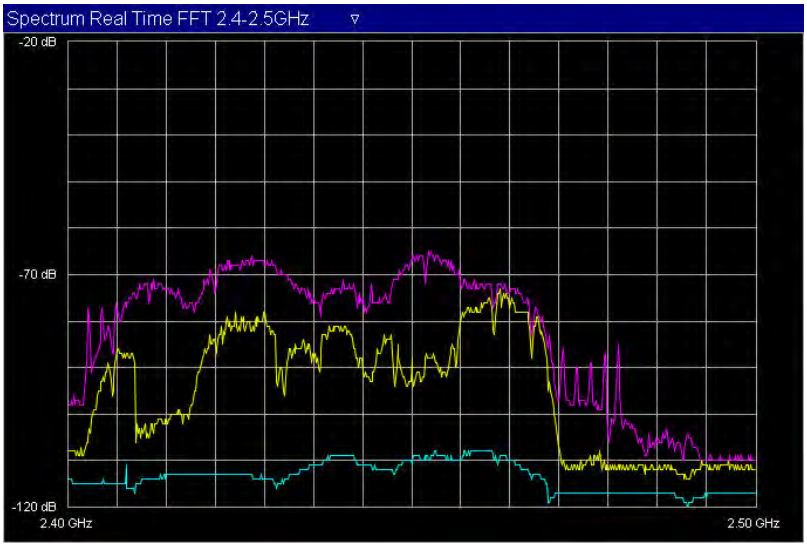
This part of the screen allows you to display the various types of data about the selected channel in the form of line charts. Across the top this screen is a filter that provides up more than a dozen types of data for you to choose from for the graph. It is very similar to the graph pane on the Channel screen.



Note: *The bottom of this part of the screen displays information related to the type of data that is being selected from the data filter above. The colors for each device correspond to the color their lines will be graphed in above. If any of the devices have a value of zero on the far right, their graphs will not appear.*

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, and so on. When such devices are detected, AirMagnet WiFi Analyzer sends out the “Non-802.11 Interfering Source Detected” alarm. The integration also makes available the spectrum graph selection in the graph pane.



To enable AirMagnet Spectrum Analyzer:

1. From the main menu, click **Configure** and select the **General** tab.
2. Check **Enable Spectrum Analyzer**.
3. Click **OK** to finish.

Note: *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 shows 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.

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

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 and ac devices).

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. The following table 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.

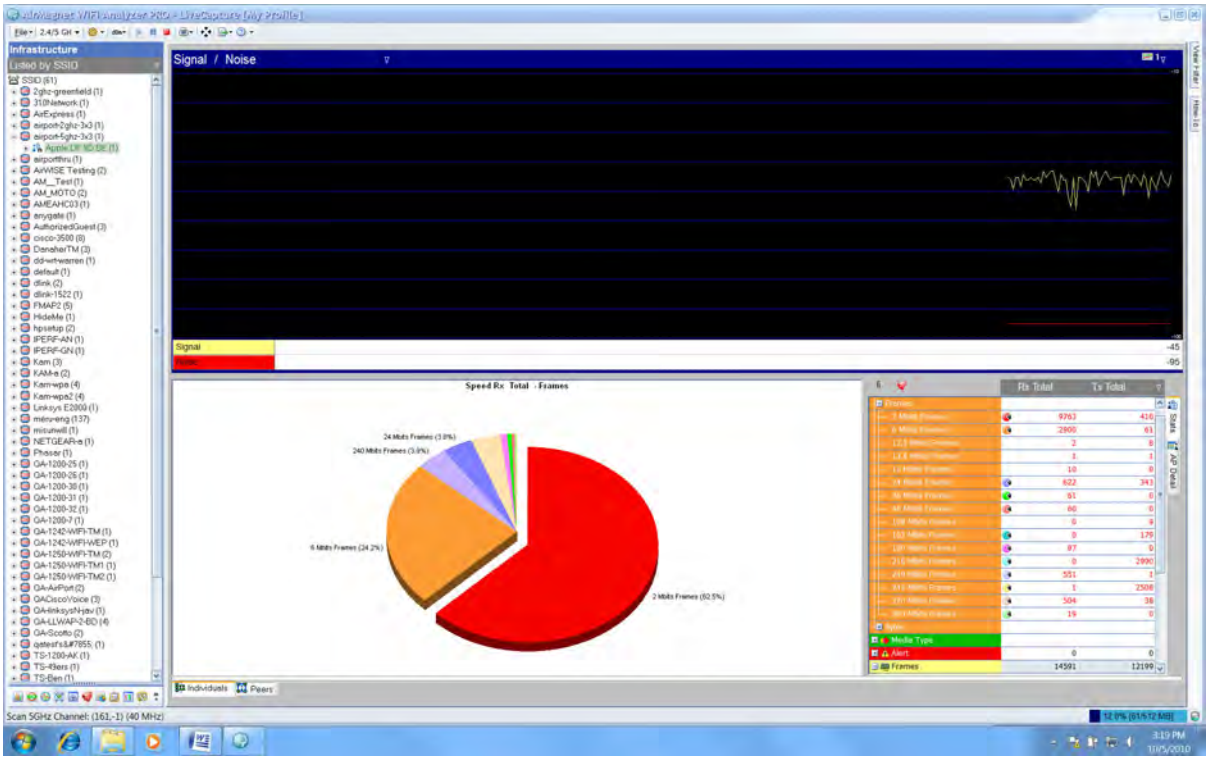
Chart Color	Data Type	Description
Purple	Max Hold	The maximum power value detected at any time since the plot was initiated. *Max Hold* means that the plot holds onto the maximum power value up to the present.
Yellow	Max	The maximum power value detected during the most recent measurement interval.
Cyan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

Infrastructure Screen

About Infrastructure Screen

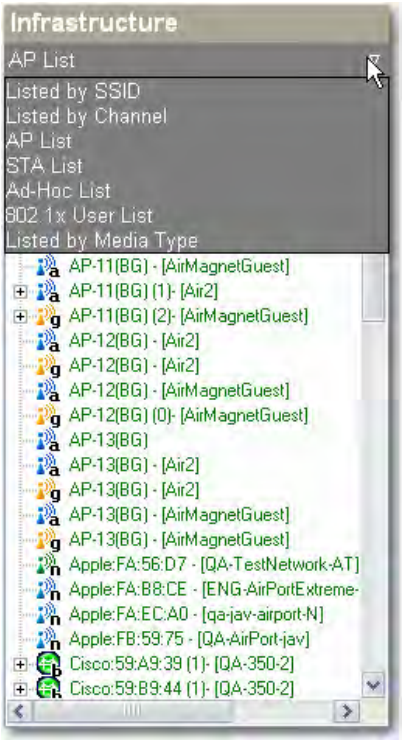
The Infrastructure screen provides comprehensive information about the infrastructure of your network, allowing you to conduct in-depth analysis of data of all devices that makes up the network. You can navigate to the Infrastructure screen at any time by clicking 

on the navigation bar. The image below shows AirMagnet WiFi Analyzer's Infrastructure screen.



Infrastructure Screen Viewing Options

The left-hand side of the Infrastructure screen shows the components that form the infrastructure of your wireless network. It provides a number of options for displaying components of a network. You can select any option by clicking the down arrow across its top and selecting an option from of interest from the drop-down list menu. By default, the screen shows devices by AP list.



Item	Description
Listed by SSID	This option allows you to view devices (APs and stations) by SSID. APs belonging to the same SSID are grouped together under that SSID. Stations, if any, belonging to the same AP are then grouped together under that AP. This option enables you to see easily all SSIDs of the network as well as which APs belong to which SSIDs.
Listed by Channel	This option allows you to view devices (APs and stations) by channel. APs operating on the same channel are grouped together under that channel. Stations, if any, belonging to the same AP are then grouped together under that AP. This option enables you to see easily all channels available on the network as well as which APs are operating on which channels.

AP List	This option allows you to view all APs detected on the network. Stations, if any, associates with an AP are then grouped together under that AP.
STA List	This option allows you to see all stations detected on the network. The plus sign "+" in front of a station indicates that the station is associating with an AP. Expand that entry to reveal the identity of that AP. Smart devices are indicated by a blue cell phone icon.
Ad-Hoc List	This option displays all ad hoc stations, if any, detected on the network.
802.1x User List	This option displays devices (AP and station) that are using the 802.1x standard.
Listed by Media Type	This option displays APs by 802.11 media type (that is, 802.11a, b, g, n and ac).

Note: *As seen from the screen, all device identification (that is, their names, IP addresses, vendor names, and so on) are color-coded; each color indicating a specific operating status of the network components. Click* ***here*** *for more information.*

Note: *This part of the Infrastructure screen is equipped with a right-click menu, which can be activated when you right-click a device (for example, AP, STA, and Ad Hoc). Some of the options in the pop-up menu may vary depending on the nature of the device being right-clicked. Most of the options in the right-click menu are identical to those in the right-click menu (in the data analysis pane) on the Start screen. Click* ***here*** *for easy reference.*

Color and Device Operating Status

All network devices shown on the left-hand side of the Infrastructure screen are color coded, each color representing a specific operating status, as described in the following table.

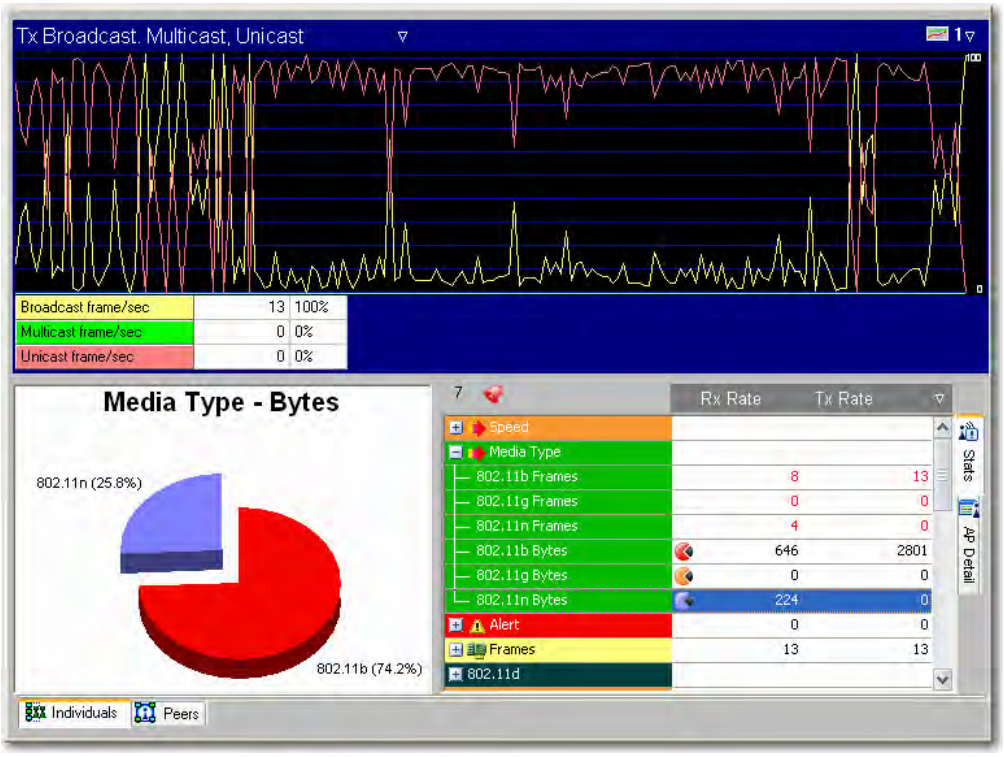
Color Code	Device Operating Status

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

Note: *The color scheme described here applies only to device names. It should not be confused with the color scheme used on device icons (that is, AP, STA, and Ad Hoc) which indicates the 802.11 protocols (that is, 802.11a/b/g/n/ac) and/or frequency bands (that is, 2.4 GHz vs. 5 GHz) used by the devices. Click* ***here*** *for information on the color schemes for AP icons.*

Analyzing Data About Individual Devices

When you select the Individuals tab, the Infrastructure screen allows you to view and analyze various network data about any specific devices detected on the network. All you have to do is to select an individual device (AP, STA, and so on) from the left-hand side of the screen and then use the tools on the right-hand side to view and analyze the various network data involving that device.

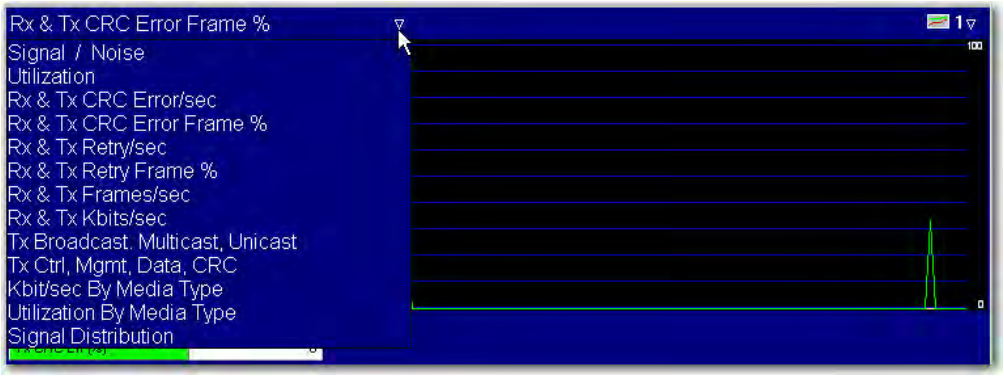


As seen from the illustration, the **Infrastructure>Individuals** screen contains the following UI components for viewing and analyzing network data involving a selected device:

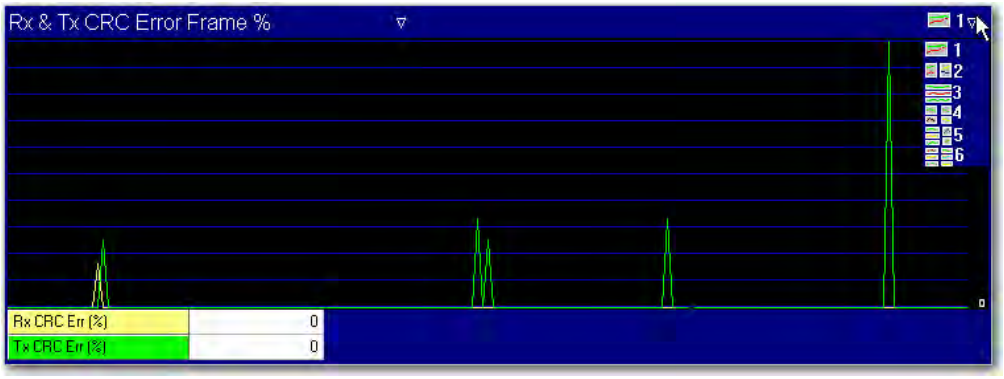
Data Graph

The upper part of the screen is a graph pane, which allows you to view data about the selected device in the form of a line chart. This part of the screen provides the following tools for viewing and analyzing data involving the selected device:

- **Data Filter** - Located in the upper-left corner of the graph pane, the data filter contains more than a dozen data options for the chart. Click the down arrow and select an option from the drop-down menu.



- **Graph Filter** - Located in the upper-right corner of the graph pane, the graph filter allows you to select the number graphs to be shown simultaneously. Click the down arrow and select an option from the drop-down menu.

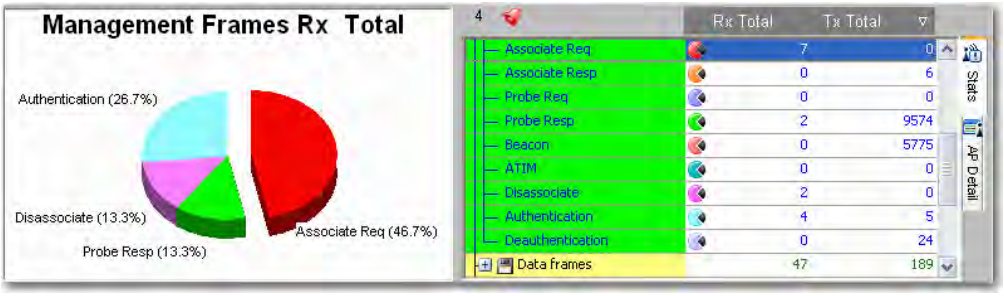


- **Data Summary** - Located in the lower-left hand corner of the graph pane, the data summary, whose content varies with the option selected from the data filter (described above), provides a numerical summary of the data being graphed.

Data Analysis

The lower part of the **Infrastructure>Individuals** screen allows you to view and analyze various data involving the device selected from the left-hand side of the screen. Along the right-hand edge of the screen are two tabs:

- **Stats** - Shows statistical data about the selected device in five categories: Speed, Media Type, Alerts, Frames, 802.11d, and 802.11h. The screen shows two columns of data for each category, which can be filtered using the filter in the upper left-hand corner of this section. Click the "+" or "-" sign to expand or contract each category. Selecting an entry in an expanded category may update the content of the pie chart to the left.



> ***Note:*** *Only entries marked with small pie chart icons are reflected in the pie chart. Also the chart will be empty if the selected category has no data.*

- **AP/Station Details** - Displays detailed information about a selected device.

> ***Note:*** *The tab is marked AP Detail when an AP is selected and Station Detail if a station is selected. This section has no effect on the pie chart to the left.*

- **Alarm Count** - The number next to the alarm icon across the top of this section indicates the total number of alarms that have been triggered by the device.

> ***Note:*** *Clicking the alarm icon directly opens the AirWISE screen where you can conduct detailed alarm analysis.*

802.11d/h Information

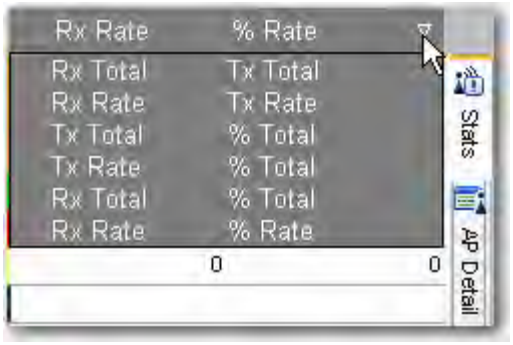
Two additional fields that aren't found in the Channel screen provide information regarding any 802.11d or 11h packets detected.

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 use 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 allows you to view the settings of any device using 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.

Infrastructure Statistics Filter

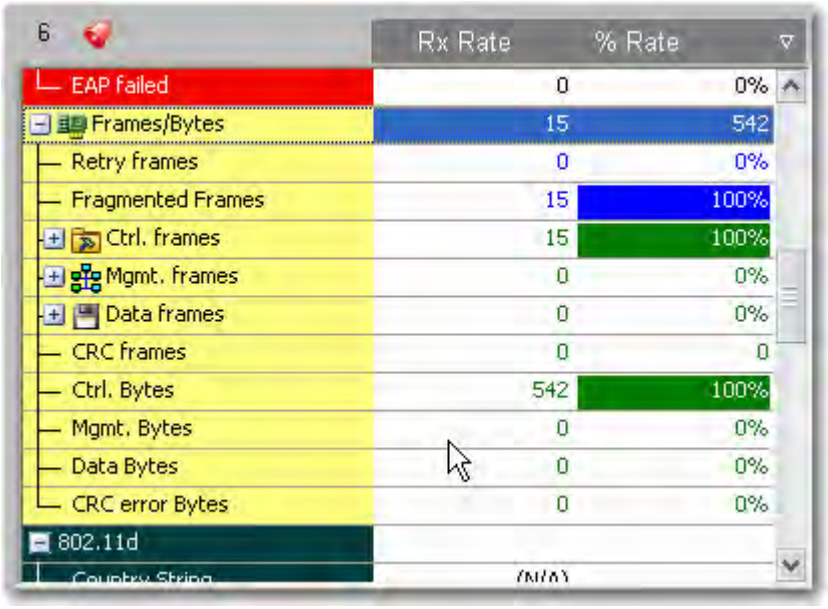
When you select the Stats tab, you will see a filter in the upper right-hand corner of the data analysis section of the Infrastructure screen. It provides options for selecting data to be shown in the table below. You can choose any option by clicking the down arrow and then choose a desired option from the drop-down list menu.



Left Column	Right Column	Description
Rx Total	Tx Total	Receive Total; Transmit Total (that is, the total number of frames/bytes received vs. the total number of frames or bytes transmitted).
Rx Rate	Tx Rate	Receive rate; Transmit Rate (that is, the number of frames/bytes per second received vs. the number of frames/bytes per second transmitted).
Tx Total	% Total	Transmit Total; Percentage of the Total (that is, the total number of certain frames/bytes transmitted vs. its percentage of the total number of all frames/bytes transmitted.
Tx Rate	% Total	Transmit Rate; Percentage of the Total (that is, the number of certain frames/bytes per second transmitted vs. its percentage of the total number of all frames/bytes transmitted.

Rx Total	% Total	Total Received; Percentage of the Total (that is, the total number of frames/bytes received vs. its percentage of the total number of all frames/bytes received).
Rx Rate	% Rate	Receive Rate; Percentage of Rate (that is., the number of certain frames/bytes per second received vs. its percentage of the total number of all frames/bytes received.

Note: *The word "total" refers to either the total number of frames or bytes, whereas the word "rate" implies either the number of frames per second or the number of bytes per second transmitted or received. A frame or byte may be further broken down into many sub-categories. Refer to the following example about how to interpret the statistics shown in this part of the Infrastructure screen.*



Note: *The image above shows statistics displayed on the screen filtered by* ***Rx Rate - % Rate****. The values shown on the screen convey the following information:*

- The receive rate is 15 frames per second or 542 bytes per second.
- All the 15 frames received within the second are fragmented frames which are also Control Frames; thus the % Rate is 100% for both.
- The 15 frames equal to 542 bytes. Therefore, the Rx Rate is 542 bytes per second and % Rate is 100% in terms of bytes.

Infrastructure Data Analysis

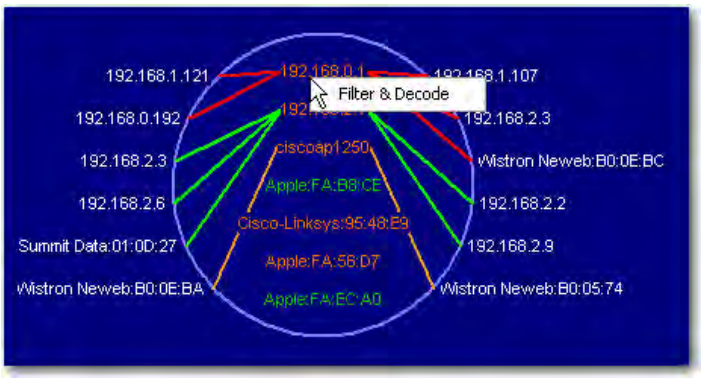
The right-hand side of the Infrastructure screen allows you to view and analyze the network infrastructure data based on the Viewing Option selected from the left-hand side of the screen. The part of the screen also has two options:

- **Individuals** - Allows you to view and analyze data about individual infrastructure components (AP, STA, or Ad Hoc) one at a time.
- **Peers** - Allows you to view the connections between the selected device and other devices.

The options are represented by the two tabs located in the lower left-hand corner of the screen. You can switch between the two options using the tabs. By default, the Individual tab is automatically selected when the Infrastructure screen opens.

Note: *The two tabs (Individuals and Peers) show directly on the screen when AP List, STA List, Ad-Hoc List, or 802.1x User List is selected as the viewing option. However, when you select Listed by SSID, Listed by Channel, or Listed by Media Type as the viewing option, the two tabs will not show unless a specific device is selected.*

Note: *While on the Infrastructure>Peers screen, you can move to the Decodes screen by right-clicking a device in the graph and click the Filter & Decode pop-up menu.*

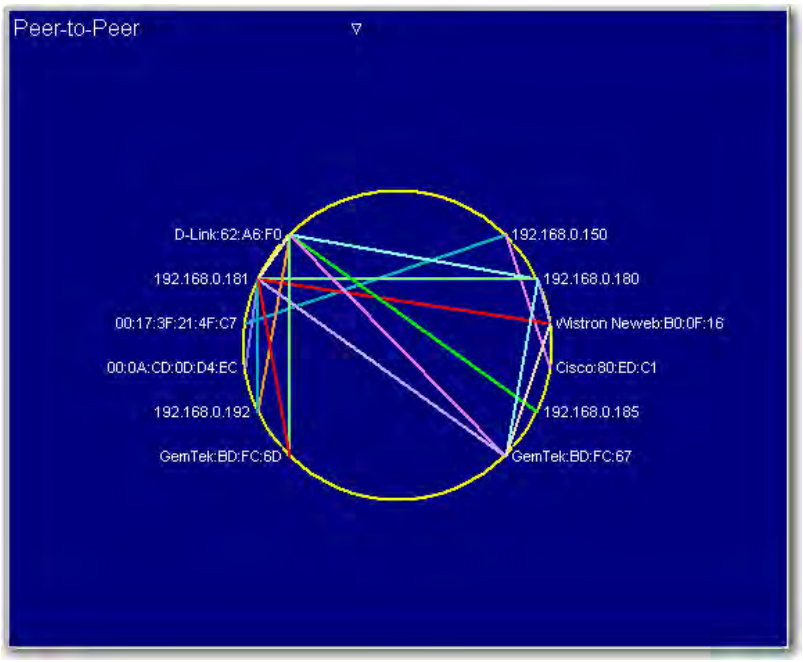


Analyzing Device Connections

The Peers tab in the lower left-hand corner of this part of the Infrastructure screen allows you to change the Infrastructure screen display to view the mapping. It allows you to visualize the connection between the selected device and other device or devices at Layers 2 and 3 when they are associating with each other. There are two scenarios as indicated by the drop-down list in the upper-left corner of the graph screen:

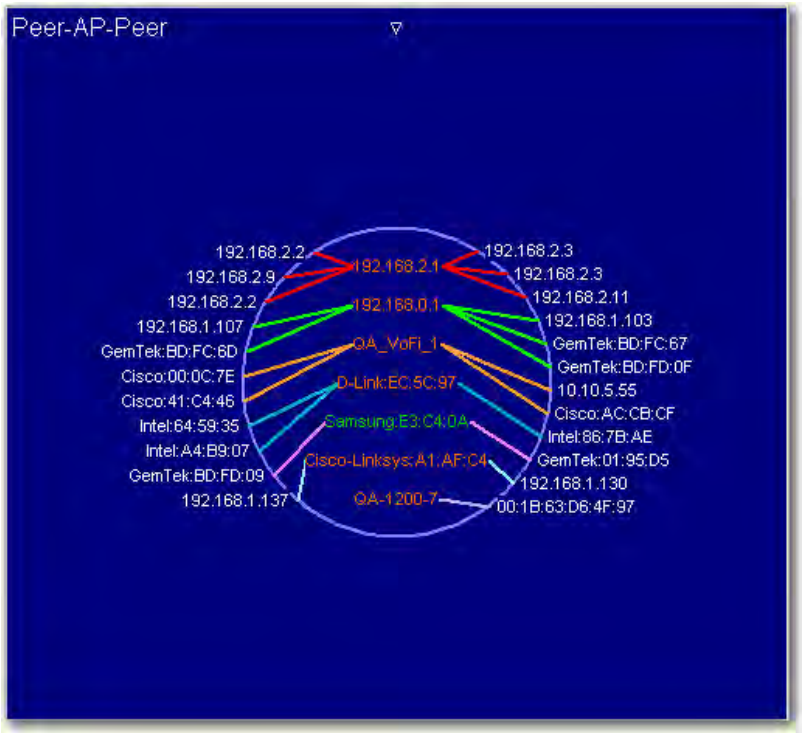
Peer-to-Peer

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 soles purpose of easy differentiation.



Peer-AP-Peer

The Peer-AP-Peer graph shows two wireless stations associating with each other through an AP.



In a Peer-AP-Peer relationship, devices inside the circle are APs and those that are outside the circle are stations. While all stations are marked white in color regardless the 802.11 protocols they use, APs are color-coded to reflecting the 802.11 protocols they use:

- **802.11a** — Blue
- **802.11b** — Green
- **802.11g** — Orange
- **802.11n** — Green (for 2.4 GHz) and Blue (for 5 GHz)
- **802.11ac** — Purple

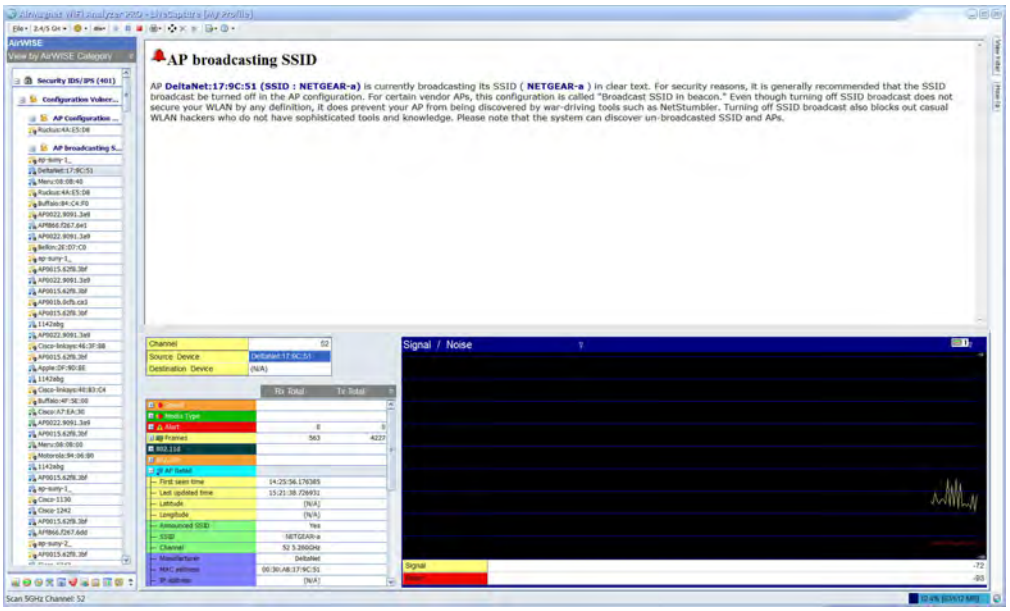
The lines between APs and stations are also of different colors. However, unlike the color scheme used for APs, the colors for the lines are randomly assigned with the sole purpose of differentiating the different AP-station connections on the screen.

AirWISE Screen

About AirWISE Screen

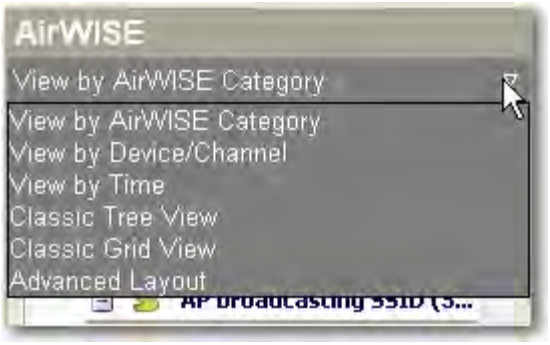
The AirWISE screen provides various means for viewing and analyzing alarms triggered on your network. You can navigate to the AirWISE screen by clicking 

on the navigation bar. The figure below illustrates AirMagnet WiFi Analyzer's AirWISE screen.



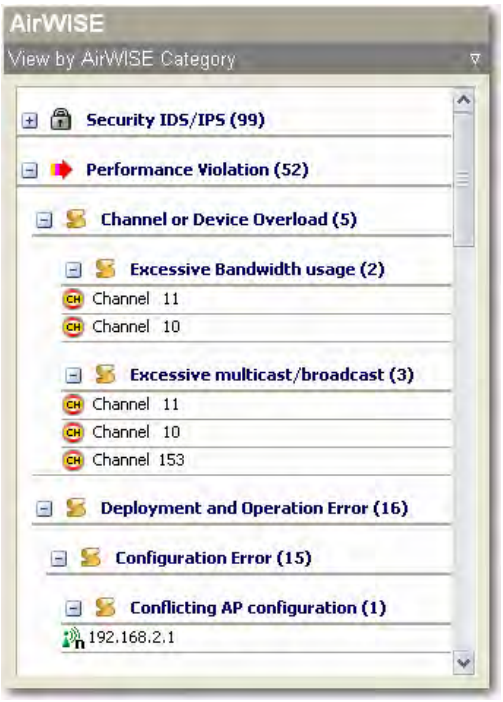
AirWISE Screen Viewing Options

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 you selects. You can select an option using the filter across the top of the screen. Click the down arrow and select an option from the drop down list.



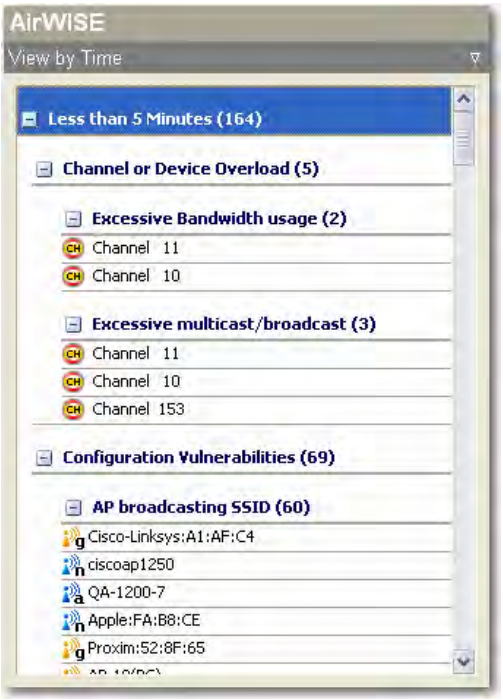
The AirWISE screen offers the following viewing options:

- **View by AirWISE Category** - This option displays alarms by the structure of the AirMagnet AirWISE network policy.

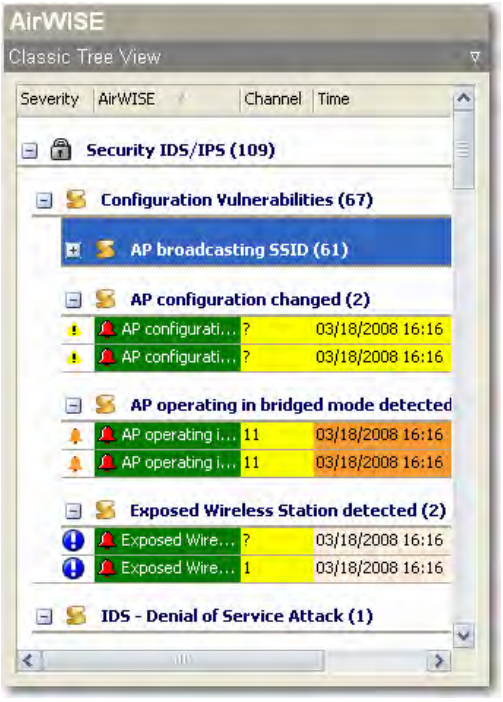


- **View by Device/Channel** - This option displays alarms by channel or by device.

- **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 AirWISE network policy.



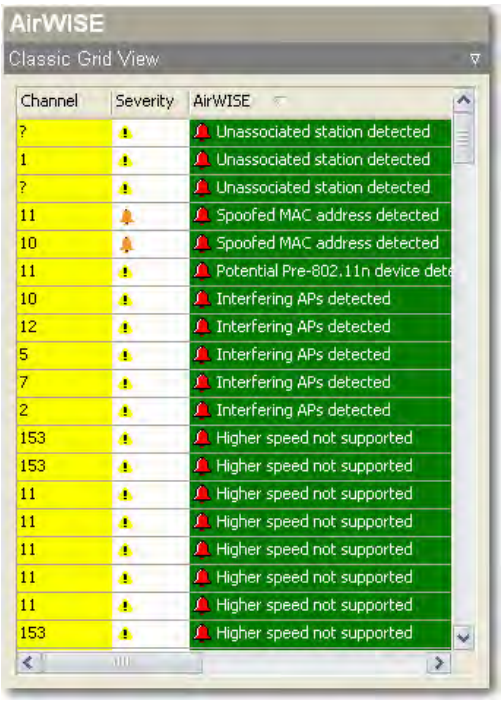
- **Classic Tree View** - This option displays alarms using the classic AirMagnet tree structure which is based on the structure of the AirWISE network policy. All alarms belonging to the same policy category are grouped together. It also shows the level of severity of each alarm.



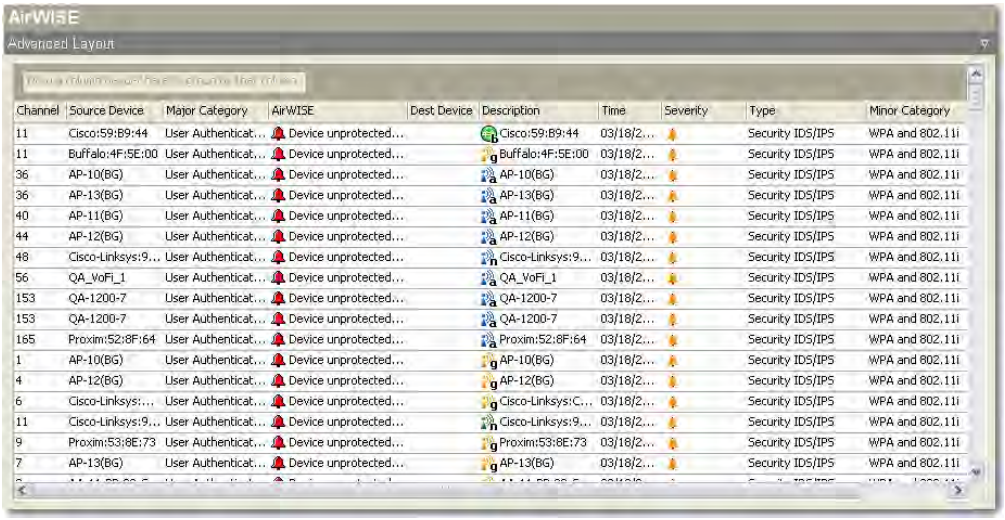
The severity of an alarm is indicated by the icon in front of it, as explained in the table below:

Alarm Icon	Alarm Severity
	Critical
	Urgent
	Warning
	Informational

- **Classic Grid View** - This option displays alarms using the classic AirMagnet grid structure.



- **Advanced Layout** -This option allows you to customize the way alarms are displayed on the screen. To use this option, you may need to stretch the right edge of this part of the screen towards the right to reveal all options available. Then you can stack the data columns in any order you want by dragging and dropping them in place.



Managing the Alarm List

AirMagnet WiFi Analyzer displays all alarms as they are captures. The alarms are shown on the screen in the order they were generated, with the oldest one appearing on top of the list. To efficiently use your screen space, you may want to remove screen alarms, especially

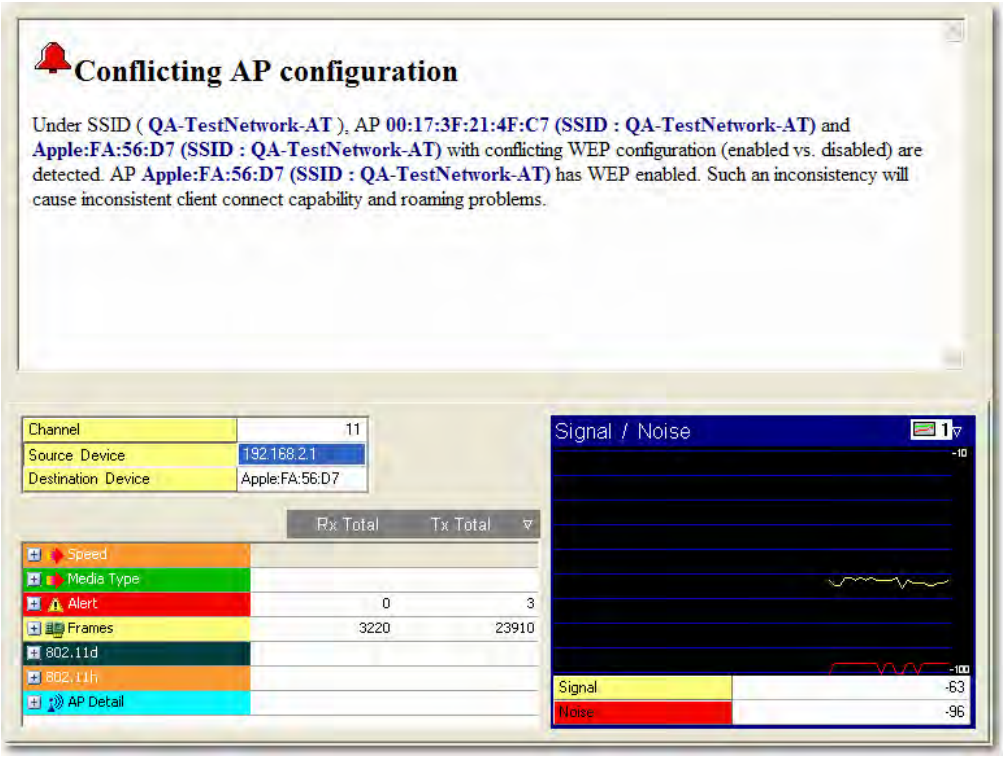
those that have already been taken care of. The two special tools on the AirWISE screen are designed just for this purpose.

- — Delete the selected alarm (or the one on top of the list if no alarm is selected). To delete an alarm, highlight an alarm of interest from the left-hand side (viewing options) of the screen and click this button.
- — Delete all alarms currently shown on the screen. To delete all alarms on the screen, click this button.

AirWISE Screen Alarm Analysis Pane

The right-hand side of the AirWISE screen is the alarm analysis pane which allows you to conduct in-depth analysis of an selected alarm.

Note: *The data displayed here depends on selection you made in the policy tree on the left-hand side of the screen. As you drill down deeper into the policy structure, the information becomes more specific.*

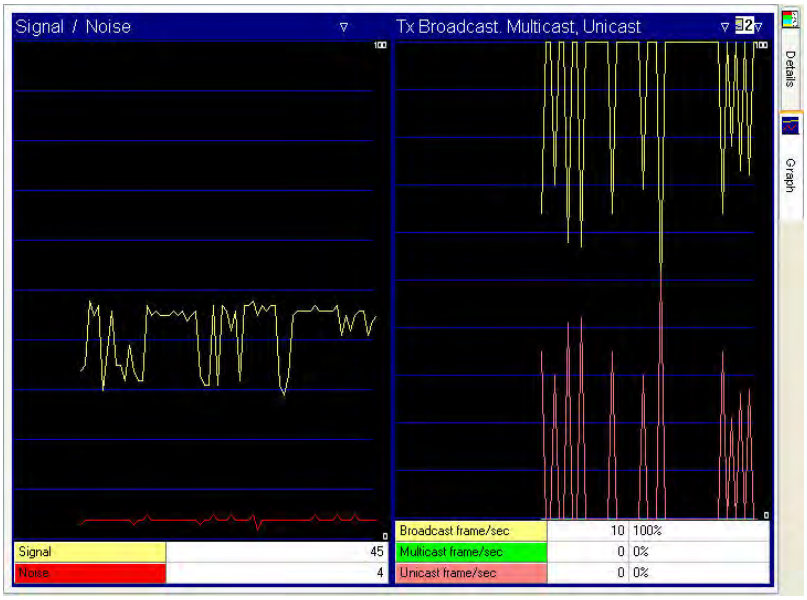


Viewing Alarm Description and Expert Advice

As shown above, the top right-hand part of Advice provides a detailed explanation of the selected alarm and a recommendation to prevent it from happening. You may need to use the scroll bar along the right edge of the screen to view the complete advice.

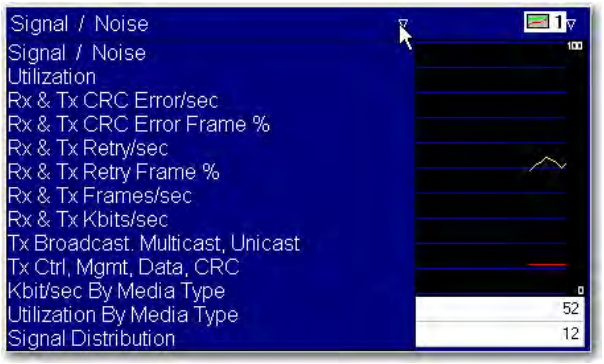
Data Analysis

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. The following figure shows the Data Analysis screen when you select the Graph tab. If the screen resolution is high enough or if the screen itself is wide enough, the contents for each tab is displayed in a separate screen.



AirWISE Screen Data Graph

The data graph is located in the lower right-hand corner of the AirWISE screen. It allows you to view and analyze in the form of line charts various data about the channel or device involved in the alarm being selected. In its upper right-hand corner is a data filter which contains all the data options for you to choose from. Click the down arrow and select an option from the drop-down menu.



In its upper left-hand corner is a graph filter which allows you to choose the number of graphs to be displayed simultaneously on the screen. Click the down arrow and select an option from the drop-down menu.

Note: *When a specific device (that is, AP, station, ad hoc) is selected, the graph shows data about the selected device only; when a channel is selected, then the graph will display data for the entire channel.*

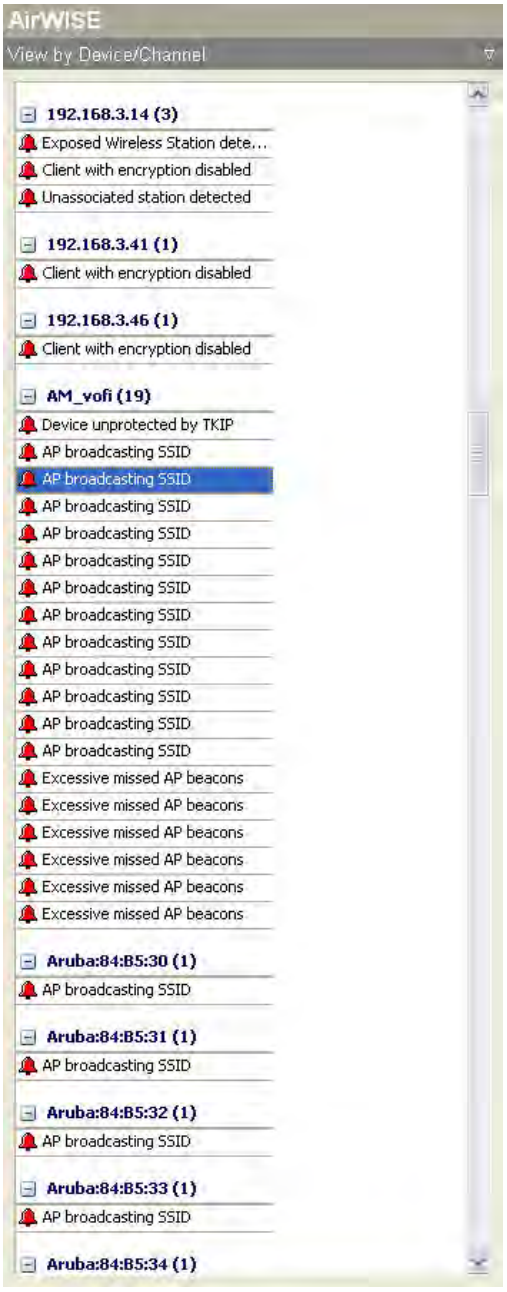
Viewing All Alarms by a Specific Device

This feature allows you to view all alarms generated by a specific device on the same screen. It provides a way 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.

Once you click View Device Alarms, the AirWISE screen refreshes and focuses on all alarms generated by the same device.



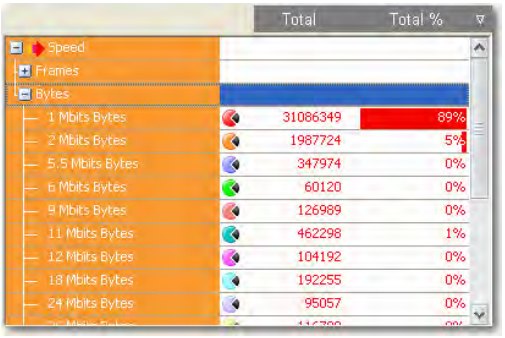
3. Click each alarm to view the information about the device and alarm description.
4. To return to the general AirWISE screen, click the filter down arrow above the **Network Policy Hierarchy** and select **View by AirWISE Category** from the drop-down list.

Channel or Device Data Analysis

The lower left-hand side of the alarm analysis pane is the section provides comprehensive, detailed information about the channel, source device, or destination device being selected.

Refer to the section above. The data are listed grouped into seven categories. You can expand each category by clicking the corresponding '+" sign.

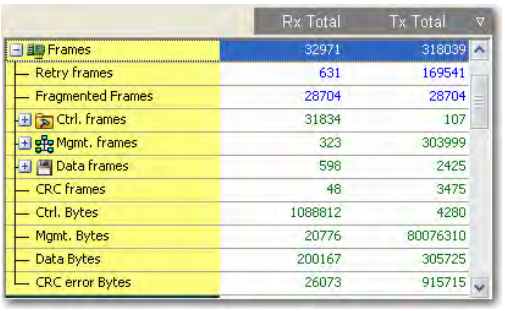
- **Speed** - Shows all available data rates in terms of frames or bytes on the channel (if a channel is being selected), or the data rates used by the device (if the source or destination device is highlighted).



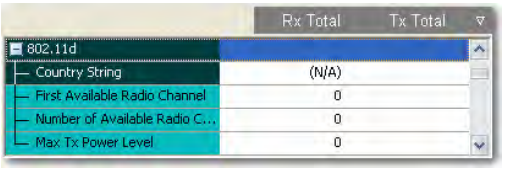
- **Media Type** - Shows the 802.11 protocols that is, 802.11a, 802.11b, 802.11g, 802.11n and 802.11 ac) in terms of frames and bytes used on the channel or by the source/destination device being selected.

- **Alert** - Shows all types of alerts data on the channel or triggered by the device being selected.

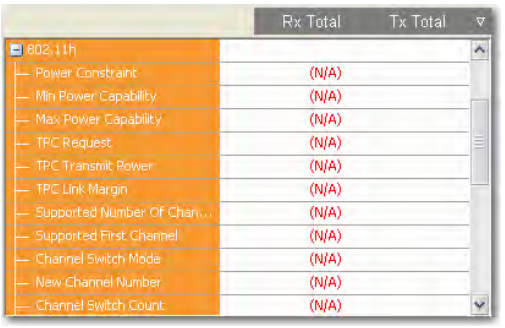
- **Frames** - Shows all types of frames data involving the channel or device being selected.



- **802.11d** - Shows 802.11d data about the channel or device being selected.

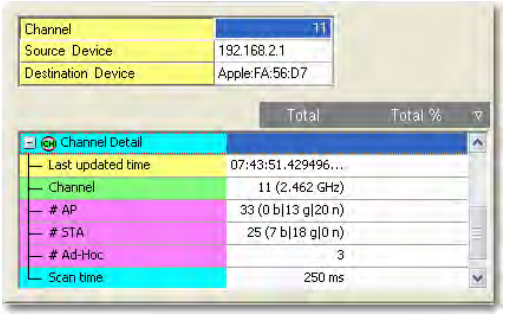


- **802.11h** - Shows 802.11h data about the channel or device being selected.

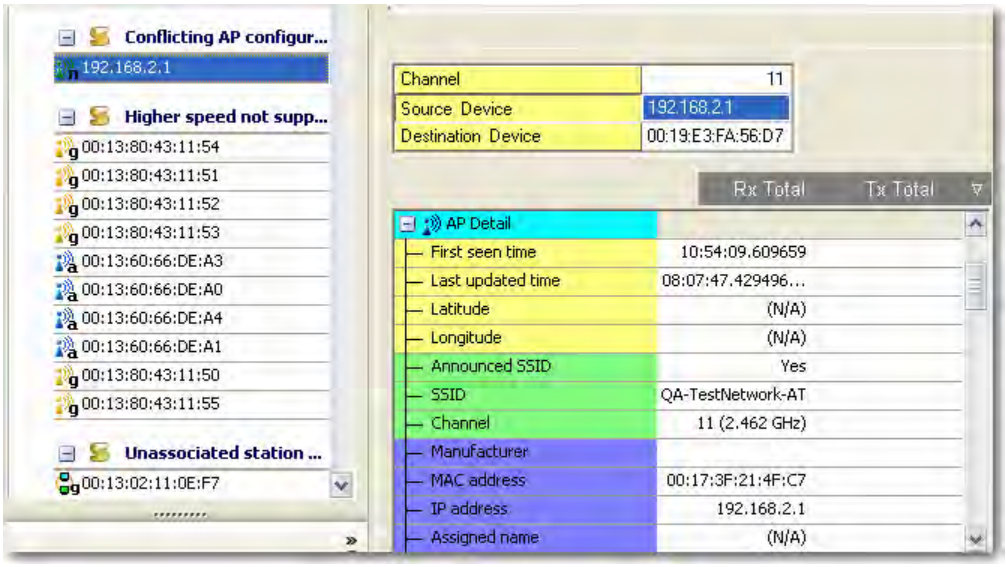


- **Channel Detail/AP Detail/Station Detail** - Shows detailed information about the channel, AP, or station being selected. The title and content of this folder depends on the selection made from the viewing option on the left-hand side of the screen and/or in the alarm physical information section above.

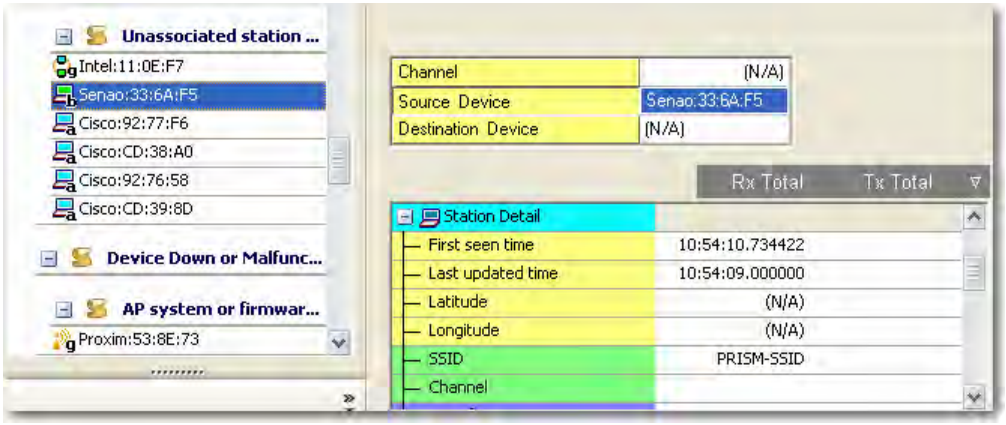
Channel Detail



AP Detail



Station Detail



Alarm Physical Information

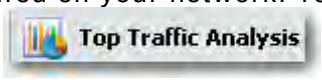
Located in the middle-left part of the screen, right below the alarm description, this part of the AirWISE screen provides some basic physical information about device that triggered the selected alarm.

- **Channel** - The channel on which the device was on that triggered the alarm.
- **Source Device** - The device (identified by name, IP address, and so on) on the transmit side of a connection.
- **Destination Device** - The device (identified by name, IP address, and so on) on the receive side of a connection.

Note: *When you select a device (AP, station, and so on) from the viewing option on the left-hand side, this part of the screen shows the channel on which the device is operating and information (name, IP address, and so on) about the source device and destination device, if available. However, if you select a channel from the viewing option, it shows a channel only; the source device and destination device fields are empty (that is, N/A). What you highlight (click) in this part of the screen is reflected in the Channel or Device Data Analysis section: if you highlight the channel, then everything you see in the section below is about the whole channel; if you highlight the source device, then everything you see in the section below is about that source device, and so on so forth.*

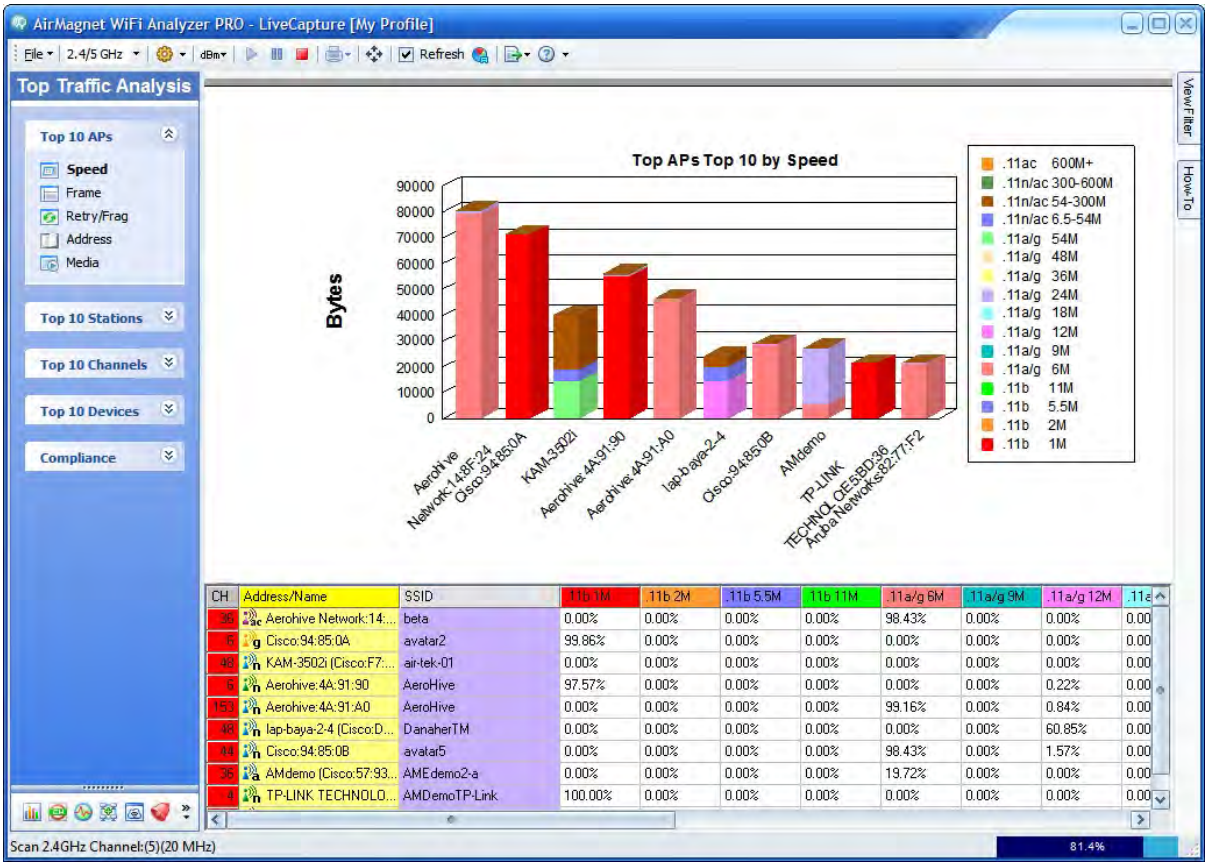
Top Traffic Analysis Screen

About the Top Traffic Analysis Screen

The Top Traffic Analysis screen enables you to view and analyze (in the form of charts) various types of data captured on your network. You can navigate to the Top Traffic Analysis screen by clicking 

on the navigation bar. The figure below illustrates WiFi Analyzer's Top Traffic Analysis screen.

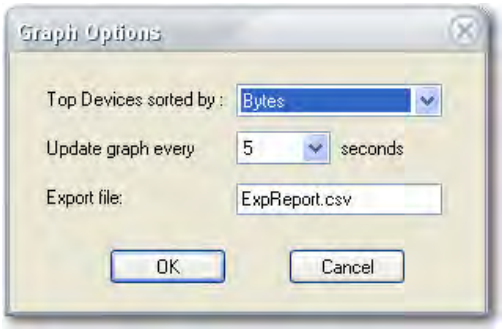
> ***Note:*** *When you are running at 800x600 resolution you will see a drop-down menu that allows you to zoom in on the charts displayed. We recommend that you uncheck the Refresh box when using the zoom feature.*



Top Traffic Analysis Screen Menu and Tools

Most of the menu and tool options on the Top Traffic Analysis screen are the same as those described in the **Commonly Used Menus and Tools**. The image below shows the menu bar as seen on the Top Traffic Analysis screen.

The following menu or tool options are specific for the Top Traffic Analysis screen:

Menu/Tool	Description
	If checked (selected), the data on the screen is updated at the frequency you set using the Options dialog box. Refer below. ***Note:*** *When you select this button, the Top Traffic Analysis Screen refreshes at the specified interval, which may cause a flickering effect on your screen. You canstop this from happening by unchecking it.*
	Opens the **Graph Options** dialog box where you can configure the following parameters for the graph:  • **Top devices sorted by** (byte, frame,bytes/sec., or frames/sec.) • **Update graph every** <5, 10, 15, 20, or 30> **seconds** • **Export file** (You either accept the default file name or override it with a unique name of your own.) ***Note:*** *You can configure the graph option by making the desired entries or selection in the dialog box and click* ***OK****.*

Top Traffic Analysis Screen Data Pane

The right-hand side of the Top Traffic Analysis screen displays the data option being selected from the left. By default, the screen shows the **Top 10 APs>Speed** (the top 10 most active APs as sorted by data rate) when it opens. Choose to display any other option by clicking the option of your interest.

Normally, you can view a device-centric 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

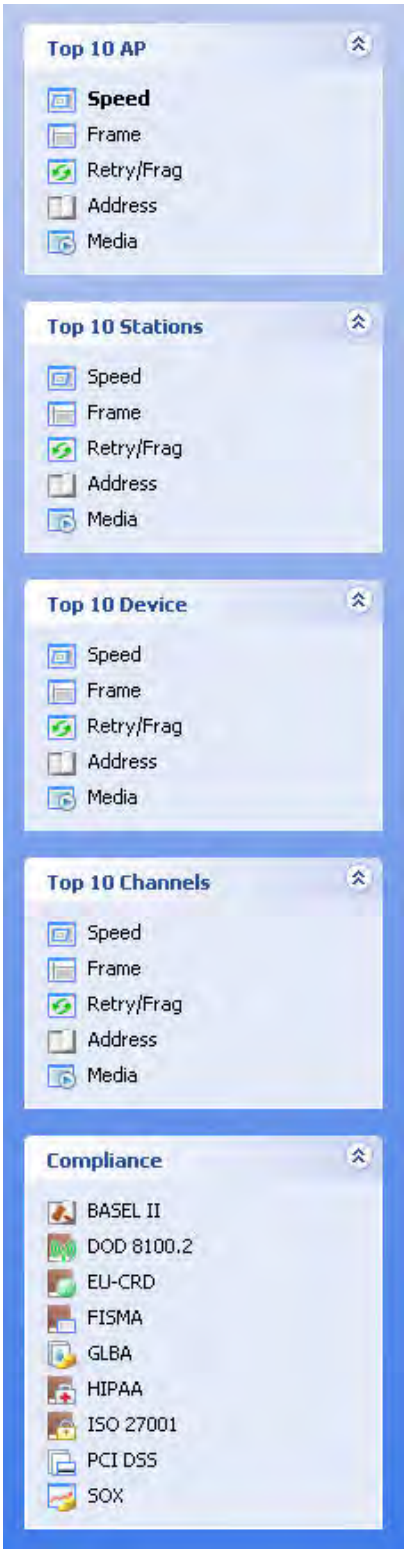
selected category. However, if you want to view the most active devices in certain SSIDs or on certain channels, do so by using the **View Filter** tab along the right-hand edge of the screen to select only the SSIDs or channels in which you are interested. In this case, you can focus on the 10 devices in the selected SSIDs or on the selected channels.

Note: *For any option in a top 10 category, the number of devices displayed in the graph depends on the actual number of devices that are active in the SSIDs or on the channels. For instance, if there are only five devices are detected on a channel, you will see five devices in the graph even though you are selecting an option from the Top 10 APs, Top 10 Stations, or Top 10 Devices category.*

Note: *When clicking any device in the device table, the graph takes you directly to the Infrastructure screen, which shows detailed data specific to that device. The name of the will be automatically highlighted among the list of devices in left-hand side of screen.*

Viewing Device Charts

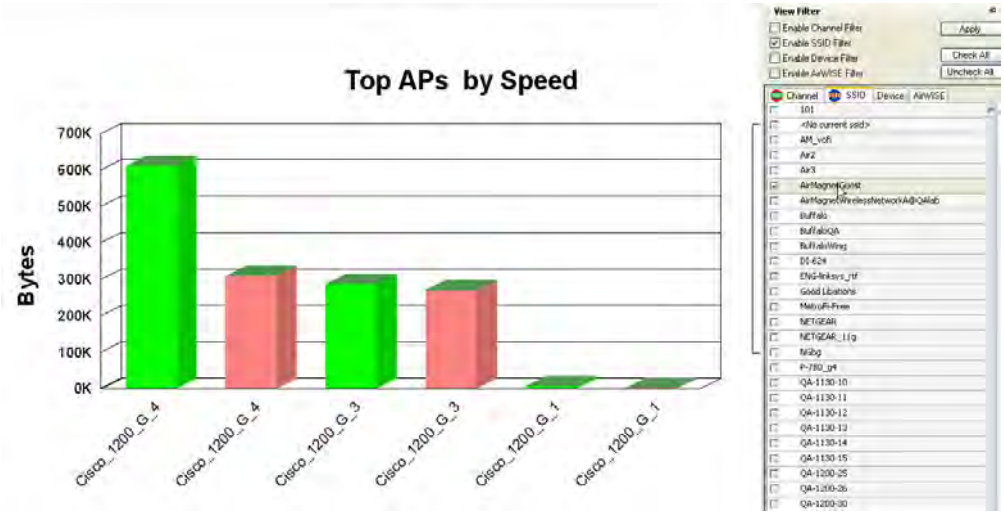
By default, all the channels and SSIDs are selected when the Top Traffic Analysis screen opens. The screen can provide graphical display of the top 10 devices in various categories. The Compliance section below displays the various compliance charts, giving you a detailed summary of how well your network complies with regulatory security standards.



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 to display 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.

The following figure shows a device chart for only 6 devices on a single SSID.

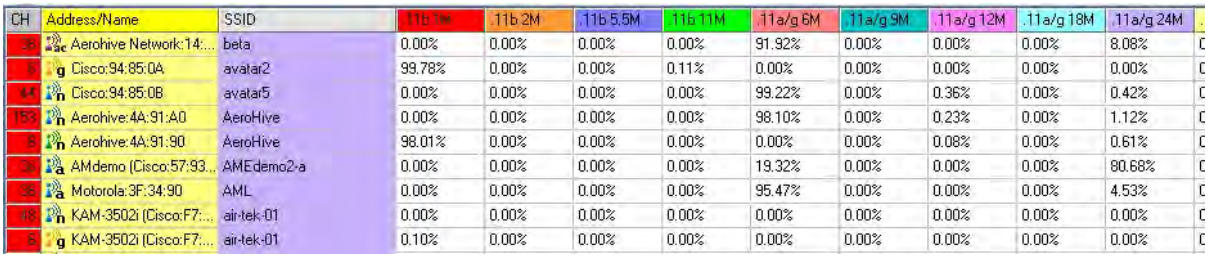


Exporting Chart Data

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.

Chart Data Tabulation

Below the graph is a table that offers a breakdown of the selected data type for the top 10 devices.



CH	Address/Name	SSID	11b 1M	11b 2M	11b 5.5M	11b 11M	11a/g 6M	11a/g 9M	11a/g 12M	11a/g 18M	11a/g 24M
36	Aerohive Network:14:...	beta	0.00%	0.00%	0.00%	0.00%	91.92%	0.00%	0.00%	0.00%	8.08%
1	Cisco:94:85:0A	avatar2	99.78%	0.00%	0.00%	0.11%	0.00%	0.00%	0.00%	0.00%	0.00%
44	Cisco:94:85:0B	avatar5	0.00%	0.00%	0.00%	0.00%	99.22%	0.00%	0.36%	0.00%	0.42%
153	Aerohive:4A:91:A0	AeroHive	0.00%	0.00%	0.00%	0.00%	98.10%	0.00%	0.23%	0.00%	1.12%
6	Aerohive:4A:91:90	AeroHive	98.01%	0.00%	0.00%	0.00%	0.00%	0.00%	0.08%	0.00%	0.61%
36	AMdemo (Cisco:57:93...	AMEdemo2-a	0.00%	0.00%	0.00%	0.00%	19.32%	0.00%	0.00%	0.00%	80.68%
36	Motorola:3F:34:90	AML	0.00%	0.00%	0.00%	0.00%	95.47%	0.00%	0.00%	0.00%	4.53%
108	KAM-3502i (Cisco:F7:...	air-tek-01	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
6	KAM-3502i (Cisco:F7:...	air-tek-01	0.10%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

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

The grid expands dynamically. More columns are dynamically added to each speed grid as data at that particular speed are observed. 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.

Note: *If the top 10 channels are graphed, click in the table to open the Channel screen.*

Compliance

FISMA (Federal Information Security Management Act) 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:

- **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** : FISMA (Federal Information Security Management Act) 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.

- **HIPPA** : HIPAA was passeed 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 isssued 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 organizations 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 PCI Data Security Standard 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.

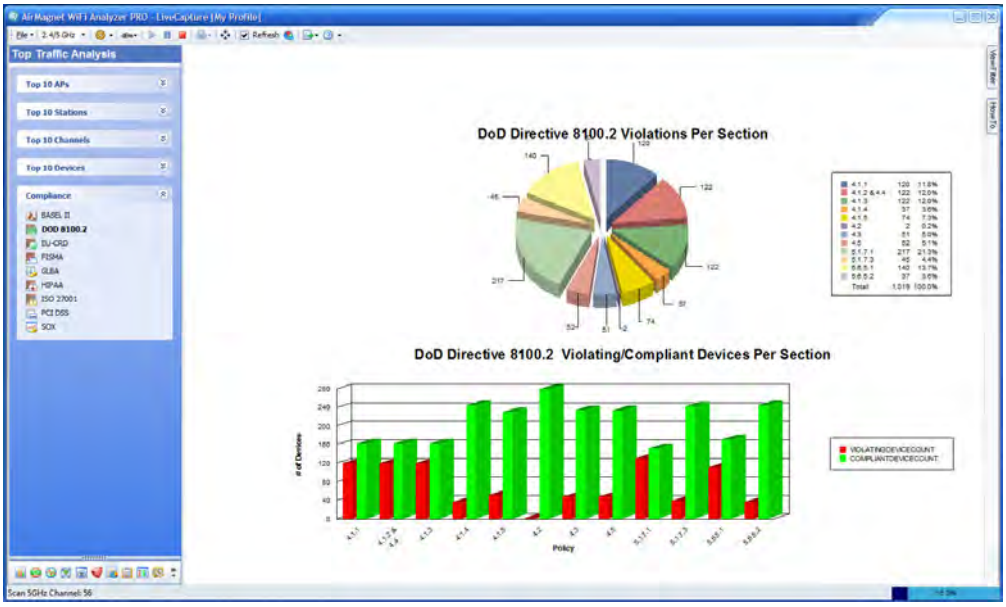
- **SOX** : The Sarbanes-Oxley (SOX) Act, also known as the Public Company Accounting Reform and Investor Protection Act, was passed by the US Congress in 2002 as a comprehensive legislation to reform the accounting practices, financial disclosures, and corporate governance of public companies.

Note: *You are advised to read the* ***Disclaimer*** *when using WiFi Analyzer's network compliance graphs or reports.*

Viewing Compliance Charts

To display a Compliance chart:

Select the compliance chart you wish to display from the Compliance section in the left-hand pane.



Disclaimer

AirMagnet Basel II, DoD 8100.2, EU-CRD, FISMA, GLBA, HIPAA, ISO 27001, Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes Oxley Compliance graphs and 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.

Top 10 APs

The charting options in the Top 10 APs group allow you to graph the top 10 APs on the network in the following categories:

- **Speed** - Displays the top 10 APs by data rate ion the screen (that is, 1M, 2M, 5M, and so on.).

- **Frame** - Displays the top 10 APs by frame type in the bar chart (that is, CRC, data, management, and/or control frame).
- **Retry/Frag** - Displays the top 10 APs by total, retry, and fragmentation frame.
- **Address** - Displays the top 10 APs by address type (that is,, broadcast, multicast, and/or unicast).
- **Media** - Displays the top 10 APs by 802.11 protocol (that is, 802.11a, b, g, n, ac).

Top 10 Channels

The charting options in the Top 10 Channels group allow you to graph the top 10 channels on the network by the following standards:

- **Speed** - Displays the top 10 channels by data rate (that is, 1M, 2M, 5M, and so on).
- **Frame** - Displays the top 10 channels by frame type (that is, CRC, data, management, and control frame).
- **Retry/Frag** - Displays the top 10 channels by total, retry, and fragmentation frame.
- **Address** - Displays the top 10 channels by address type (that is, broadcast, multicast, and unicast).
- **Media** -Displays the top 10 channels by 802.11 protocol (that is, 802.11a, b, g, n and ac).

Top 10 Devices

The charting options in the Top 10 Devices group allow you to graph the top 10 devices (including both APs and stations) on the network in the following categories:

- **Speed** - Displays the top 10 devices by data rate in the bar chart (that is, 1M, 2M, 5M, and so on).
- **Frame** - Displays the top 10 devices by frame type in the bar chart (that is, CRC, data, management, and/or control frame).
- **Retry/Frag** - Displays the top 10 devices by total, retry, and fragmentation frame.
- **Address** - Displays the top 10 devices by address type (that is, broadcast, multicast, and/or unicast).
- **Media** - Displays the top 10 devices by 802.11 protocol (that is, 802.11a, b, g, n, ac).

Top 10 Stations

The charting options in the Top 10 Stations group allow you to graph the top 10 stations on the network in the following categories:

- **Speed** - Displays the top 10 stations by data rate on the screen (that is, 1M, 2M, 5M, and so on).
- **Frame** - Displays the top 10 stations by frame type (that is, CRC, data, management, and/or control frame).
- **Retry/Frag** - Displays the top 10 stations by total, retry, and fragmentation frame.
- **Address** - Displays the top 10 stations by address type (that is, broadcast, multicast, and/or unicast).
- **Media** - Displays the top 10 stations by 802.11 protocol (that is, 802.11a, b, g, n, ac).

Viewing Compliance Reports

Compliance data are also available in compliance reports. Refer to About Reports Screen.

Compliance Reports Disclaimer

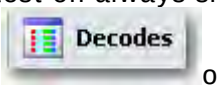
AirMagnet DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley, and Payment Card Industry Data Security Standard (PCI DSS) Compliance Reports provide a security framework to comply with regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on 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.

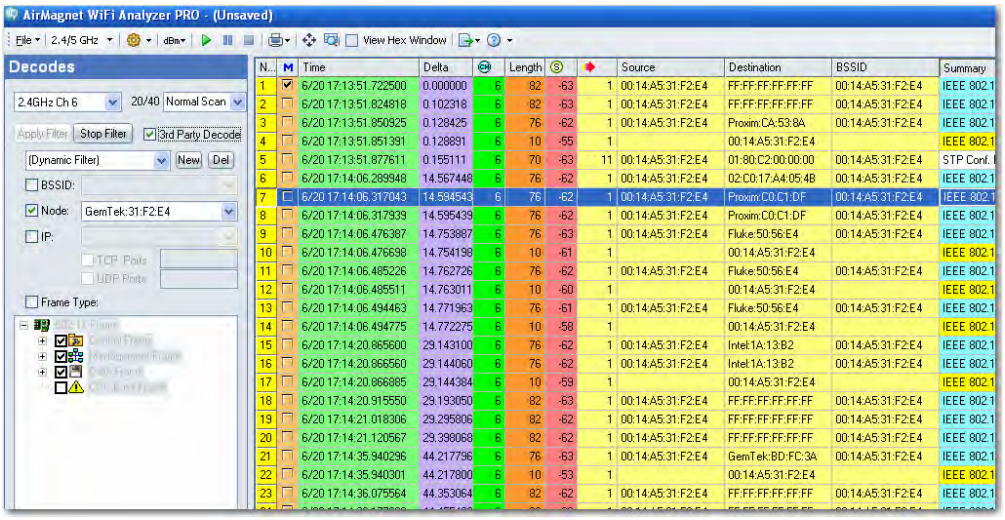
The information contained in the Policy Compliance Reports is furnished under and subject to the terms of the Software License Agreement (“License”). The Policy Compliance Reports do not create a binding business, legal, or professional services relationship between you and AirMagnet. Because business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

Decodes Screen

About the Decodes Screen

By default, the Decodes screen displays in real time all packet frames as they are captured. The packets are displayed in the order they are captured, with the latest on always shown on the top of the scrolling list. Access the Decodes screen by clicking 

on the navigation bar. The figure below illustrates AirMagnet WiFi Analyzer's Decodes screen.

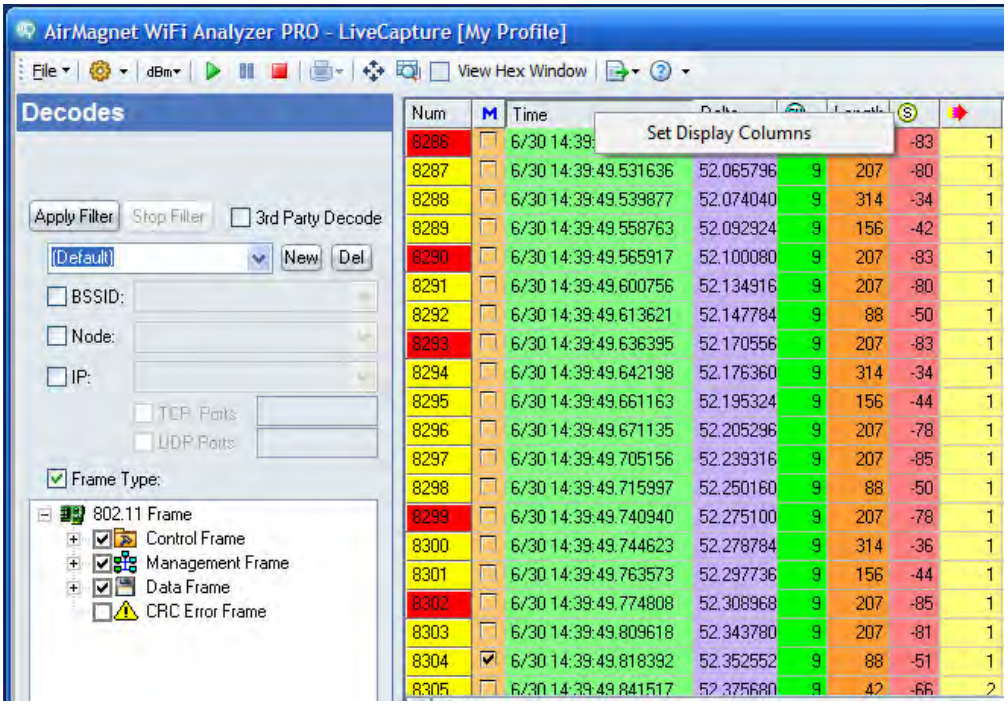


Add/Remove Columns

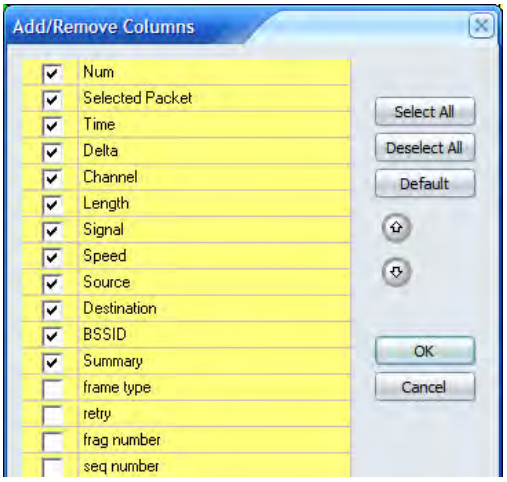
You can adjust which columns to display in the Decodes table by using the Add/Remove Columns dialog.

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**. Refer to the figure below.



2. Use the check box controls to set the columns to display. Click **OK**. Refer to the figure below.



This section covers the following topics about the Decodes screen:

- Packet Information Fields
- Setting Up Packet Filters
- Creating a New Filter
- Using a Custom Filter
- Conducting Packet Decoding
- Finding Packets on Decodes Screen

AirMagnet WiFi Analyzer has two different live capture modes: The regular mode and the Capture-to-Disk mode.

- **Regular capture mode**: The maximum size of the capture memory is 64 MB and the captured data are saved in a *.amc* file format. It is good for capturing a small amount of network traffic data.
- **Capture-to-Disk mode**: This enables the application to stream captured Wi-Fi traffic data to the PC's hard drive concurrent with live data capture. With this feature, the amount of data captured is no longer limited by the size of the capture buffer.

By default, the Capture to Disk feature is off when the application is launched. You must manually turn it on (using **File>Configure>Profile>Capture to Disk>File Size**) in order to enable it. Once enabled, it remains so until the Maximum Capture File Size is reached. The image above shows the Decodes screen in Capture-to-Disk mode.

The status bar in the lower right corner of the screen indicates the size of the disk space allocated to the capture memory (that is, 512 MB) and the percentage or amount of the disk space being used. The disk icon indicates that the application is in Capture-to-Disk mode.

The **Pause Live capture** button on the toolbar is available for Capture-to-Disk mode only. It is grayed out when the application is in the regular capture mode (that is, .amc).

By default, the **Apply Filter** button on the top-left part of the screen is disabled (grayed out). It becomes available only when you have made changes on the screen. In that case, your must click this button to implement the changes made to the filters.

Packet Information Fields

The Decodes screen provides a variety of data regarding every packet captured. Each piece of information is displayed in a separate column, as described in the table below.

Column	Description
No	The sequence of the captured packet, 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.
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.

Setting Up Packet Filters

The AirMagnet WiFi Analyzer comes with its factory default filter settings. You can also configure your own filters to restrict packet captures to a specific channel, SSID, AP, station, or frame type. Keep in mind that all filters are optional. They are intended to help you focus your analysis on a certain channel, SSID, node, IP address, or type of frames if you want to. Also, the filters can be used individually or in any combination that the application allows.

The left side of the Decodes screen contains options for filtering data to be displayed on the screen. By default, the **Apply Filter** button is disabled (grayed out) and will not be available unless you make changes to the filter settings. Once you make changes to the filter settings, you must click **Apply Filter** to implement them.

Note: *The Filter pane on the left of the Decodes screen is a mirror image of the Filter tab of the Configure screen. However, the filters on the Decodes page only affect data displayed in that page, whereas the master filter applies to all pages. If you wish to set a master filter to function globally, click*  *and select the Filter tab to open the filter configuration screen. Refer to* ***Configuring Data Filters*** *for more information.*

Creating Custom Filters

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

To create a custom filter:

1. Click **New** and rename the [New Filter] with a unique name.
- To focus on a specific SSID, check **SSID** and select it from the **List** menu.
- To focus on a specific node on the network, check **Node** and select the MAC address of that node from the **List** menu.
- To focus on a specific IP address, check **IP** 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.

2. 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 monitoring traffic by channel, SSID, node, or frame type.

To apply a filter:

1. Select a channel, if you want to focus on a particular channel.
2. Click the down arrow and select the filter of interest. See the figure below.

3. Click **Apply Filter**.

Note: *The list menu contains all filters that you have created. If you want to disable a filter that is in use, click* ***Stop Filter****. Delete any filter by highlighting it from the list menu and clicking* ***Del*** *(Delete).*

Conducting Packet Decoding

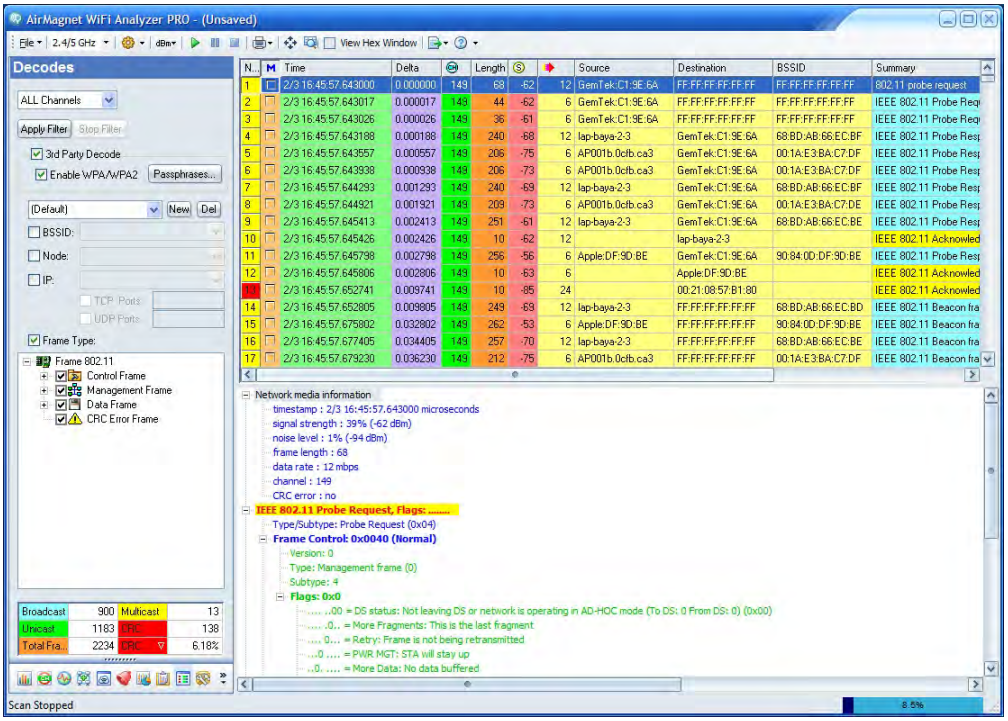
By default, the Decodes screen shows the data packets as they are captured live in a first-in first-out scrolling order. To conduct detailed packet analysis, you have to stop the screen from scrolling so that you can take a close look at any packet you are looking for.

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

The first figure below shows the view using the 3rd party decode engine. The second figure shows the default decodes engine.

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

Stop the live capture by tapping **(Stop Live Capture)** so that you can take a closer look at the list of packet decodes on the screen. You can then tap the **(Start Live Capture)** button to resume the packet capture.



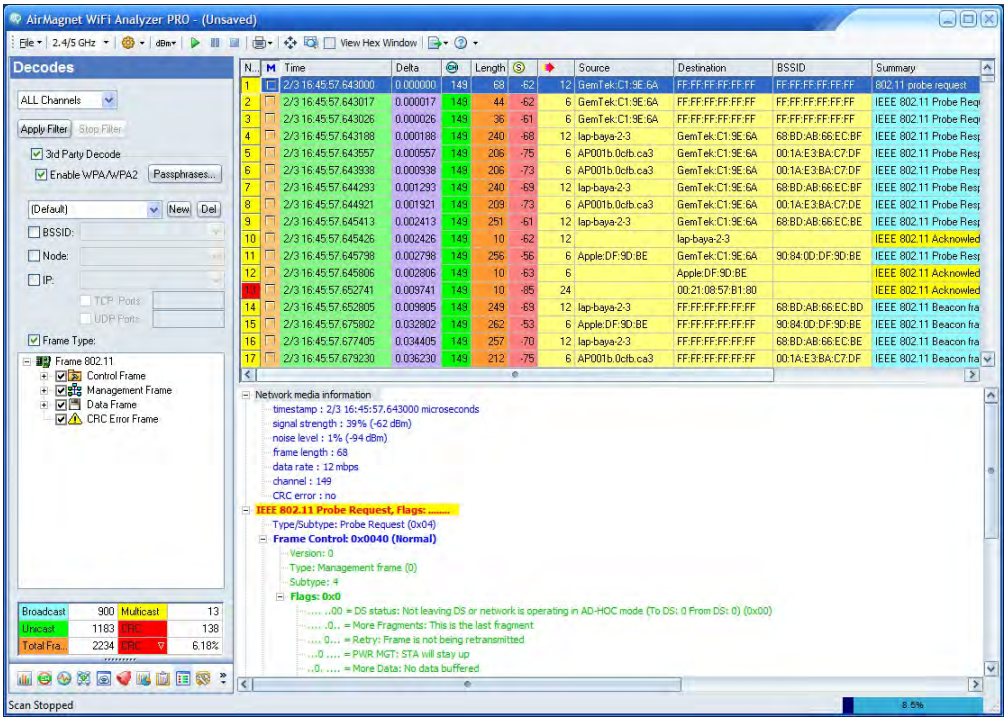
3rd party decodes enabled

Note: *The Pause Decodes button ( ) is available only when the Capture to Disk (.amm) mode is enabled; it does not apply to the regular live capture (.amc) mode. The image above shows the Decodes screen when the application is set in the Capture-to-Disk mode.*

If you are in the regular capture mode, you need to follow the instructions below to decode the captured packets.

To conduct packet decoding:

1. From the Toolbar, click  . The Decodes screen gradually comes to a standstill. Refer to the figure below.



Decodes default view

2. From the toolbar, check the **View Hex Window** check box.
3. From the screen, select a packet and review all the information about it.
4. Start decoding the packet by expanding all entries in the lower part of the screen.
5. Repeat Steps 3 and 4 to analyze other packets of interest.
6. To resume live packet capture, click  **(Start Live Capture).**

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

WPA/WPA2-PSK Decryption

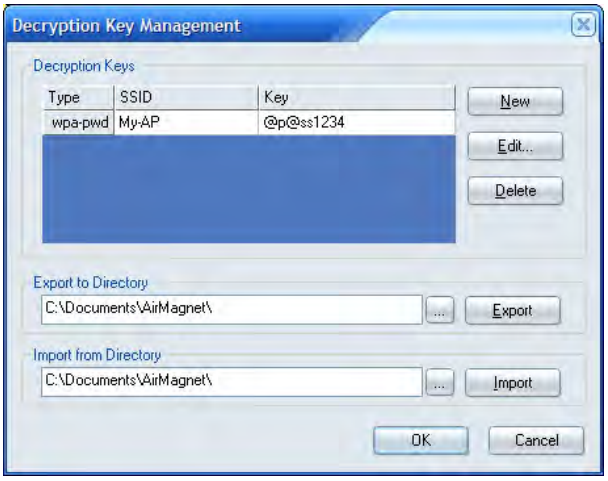
Devices that are using WPA/WPA2-PSK encryption can be decrypted using the SSID and the passphrase for WPA/WPA2-PSK. WPA-PSK Decryption is only supported in CTD mode (capture to disk).

If a packet is encrypted, the phrase "encrypted data" is noted in the Decodes view **Summary** column.

Decryption requires that whole frames are captured including the 4-way handshake between the client and the AP. Keep in mind it is important for the scanning to be locked on the channel when you will decrypt frames.

Decryption is also supported for a trace file that includes the 4-way handshake and is provided the correct SSID with passphrase.

1. From the Decodes view, check **3rd Party Decodes** (If this feature is not available, it needs to be installed. Refer to **Configuration dialog>Filter** tab).
2. Check **Enable WPA/WPA2**.
3. Click **Passphrase**.



4. Click **New**. Type the SSID and Passphrase. Click **OK**.
5. Click **OK** to close the dialog.

Once a decryption key is created, it can be Edited and Deleted using the associated options in the Decryption Key Management dialog.

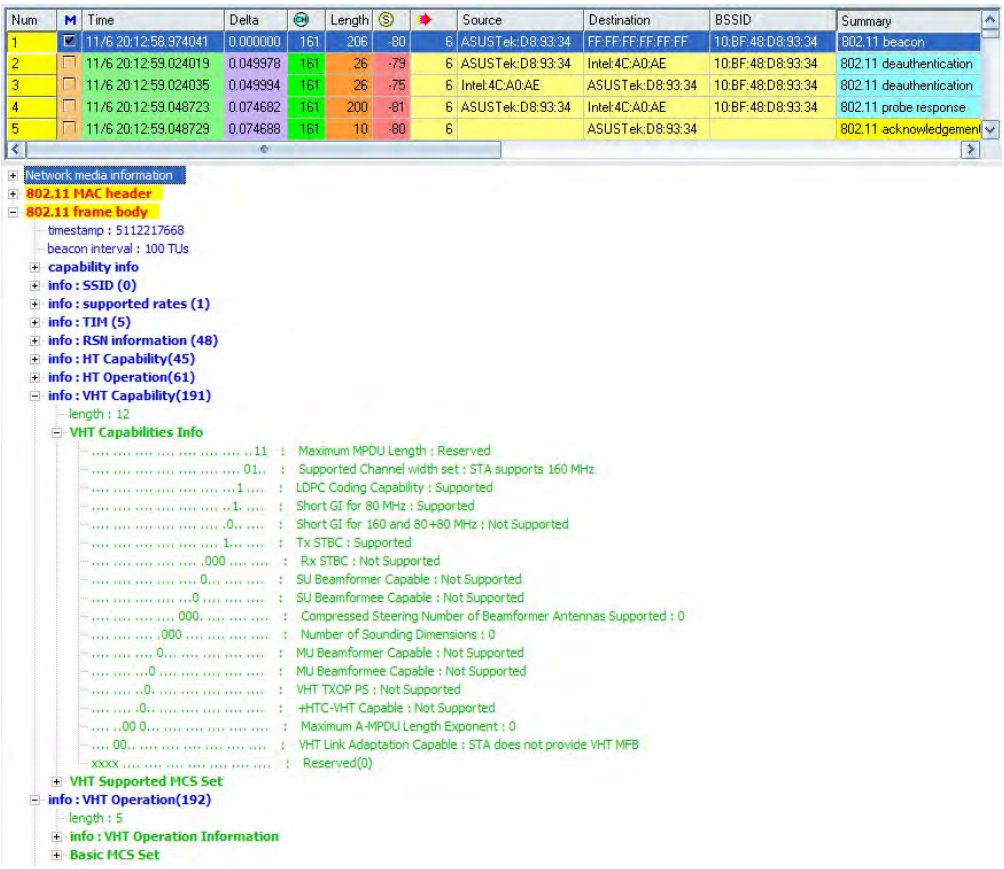
The set of decryption keys created can also be exported for use in another instance of AirMagnet WiFi Analyzer.

1. Open the **Decryption Key Management** dialog. Create one or more Decryption Keys.
2. Click **Export** and save the Decryption Key preferences.
3. Open an instance of AirMagnet WiFi Analyzer. Navigate to the Decodes view.
4. Open the **Decryption Key Management** dialog.
5. Click the **Import** navigation button and navigate to the directory location where the Preferences file was saved.
6. Select the file named **Preferences**.

7. Click **Open**.
8. Click **Import**.

802.11ac Decodes

The following example of the **Decodes** view shows the management frames of 802.11ac under **VHT** (Very High Throughput) **Capability**.

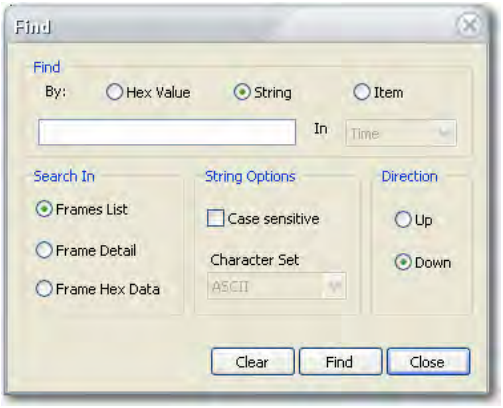


Finding Packets on Decodes Screen

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 menu bar, click . The Find dialog box appears. See the figure below.



3. Make the desired entries and selections and click **Find.**

Capturing and Saving a Large Amount of Data

You can choose to capture packet data to disk by two methods:

Capture to disk: Check this option to capture and save a maximum file size based on the selection from the Buffer size drop-down. You can also choose a Byte slice size from the Slice size drop-down. Capturing is stopped once the buffer size is reached.

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

Non-stop Capture: By also checking Non-stop Capture, once the configured Buffer size is reached, the data will automatically be saved to the directory location set in the save file text box. The file name will be a date/time stamp. At this point a new data capture will automatically begin. This process will continue until the configured Max allocated disk space (HDD) is reached (the default is 10GB). The Max allocated disk space size may be set as large as the available disk space.

To capture and save a large amount of data:

1. From the toolbar, click **File>Configure....**
2. Select the **Profile** tab.
3. Check the **Capture to Disk** check box. For **Non-Stop Capture**, also check this option.
4. Select a **File Size** and **Slice Size**.
5. If you are using Non-stop Capture, set the Max allocated disk space (HDD).
6. Use the browse button to the right of the file save text box to set the file save location.
7. Click **OK.**

Conducting Packet Decoding Concurrent with Live Capture

This feature enables you to conduct detailed packet decoding while still leaving the application in live capture mode. Unlike the normal decoding operation which completely halts live capture and you may miss some network traffic, this feature allows you to conduct decoding without missing any data passing through the network.

To conduct packet decoding concurrent with live capture:

1. From the toolbar, click **File>Configure>Profile**.
2. Check the Capture to Disk check box, select a File size and Slice size, and click **OK.**

Note: *Once the Capture to Disk feature is enabled, the status bar in the lower-right corner will show the total amount of disk space allocated and the amount or percentage of the space that has been used.*

3. From the Decodes screen, click  **(Pause Decodes)**.
4. Make sure that the **View Hex Window** check box is checked.
5. Perform decoding using the same procedure outlined in Conducting Packet Decoding.
6. When completed, click  **(Start Live Capture)** to resume live capture.

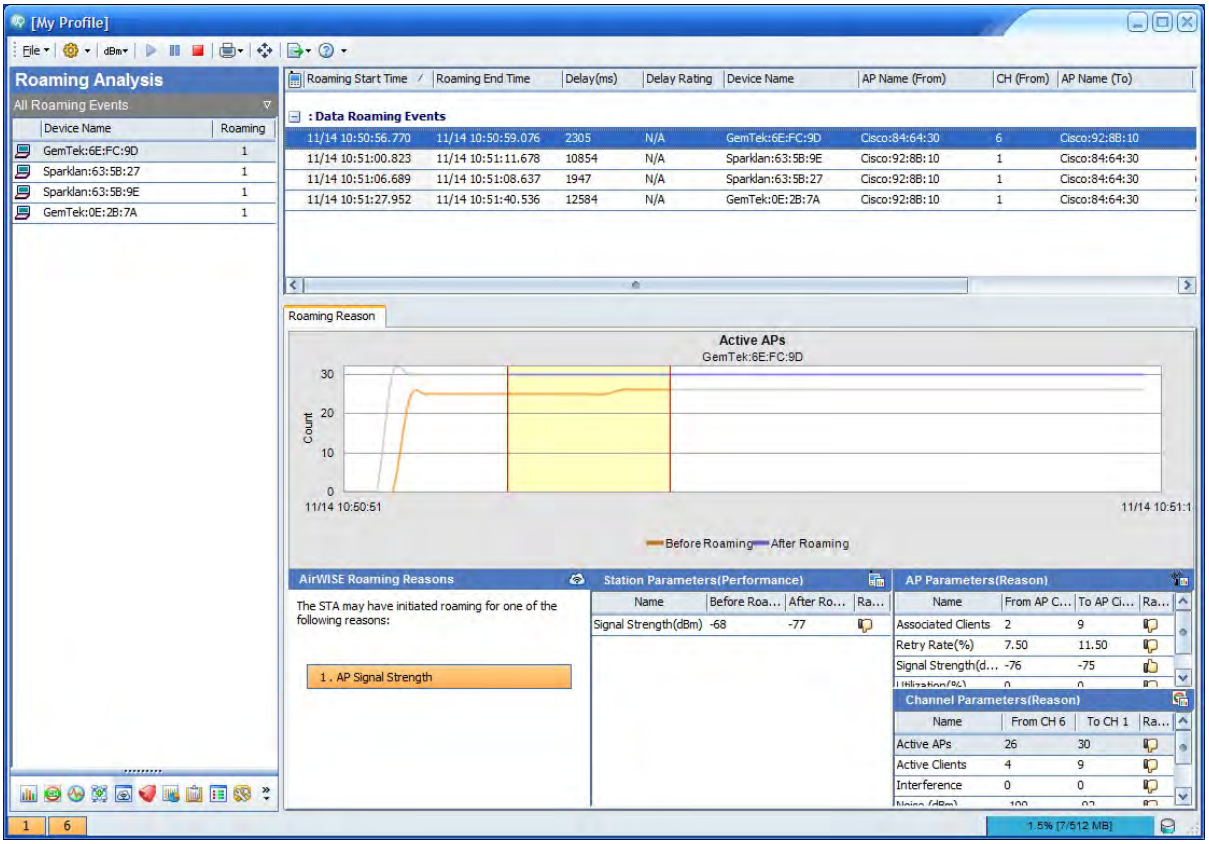
Note: *When you click **Pause Decodes**, the packet at the bottom of the packet capture list automatically becomes highlighted, indicating that it is the packet that is captured at that point in time. Because the live capture is still going on even when you are decoding, you'll notice new packets being captured from the slow scrolling movement of the scroll bar on the right.*

Roaming Screen

About the Roaming Analysis Screen

The Roaming Analysis screen shows all devices that have been detected to have roamed from one AP to another. The screen also provides details of all the detected roaming events associated with each device.

You can get to the Roaming Analysis screen by clicking  on the navigation bar. The image shows the Wi-Fi Roaming Analysis screen.

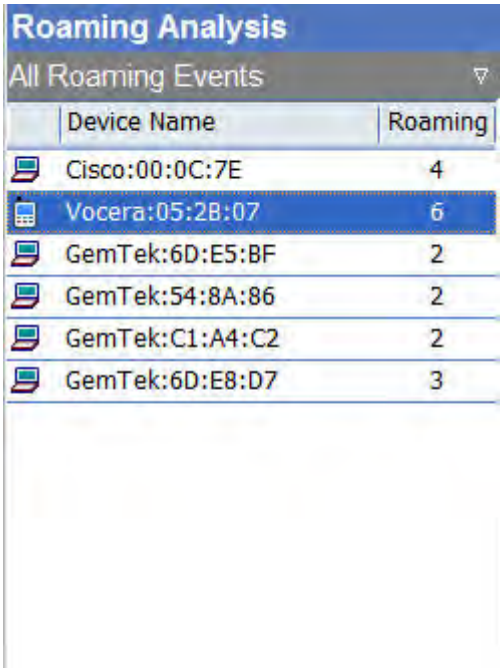


This section explains the following topics about the Roaming Analysis screen:

- Device Listing
- Analysis Roaming Details

Device Listing

The Device Listing pane on the left shows All Roaming Events by default. This is usually the starting point for any roaming analysis. You can filter the devices list by selecting an option in the drop-down.



Begin your analysis by selecting a device from the list.

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

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. When viewing roaming by channel, this column simply indicates the channel number.
Roaming	This field allows you 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.

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.

Note: *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, you can adjust the information displayed in the Device Listing by using the drop-down filter provided at the top of the pane.

Since the columns provided vary depending on the selection made, you can tailor the display to provide exactly the data required:

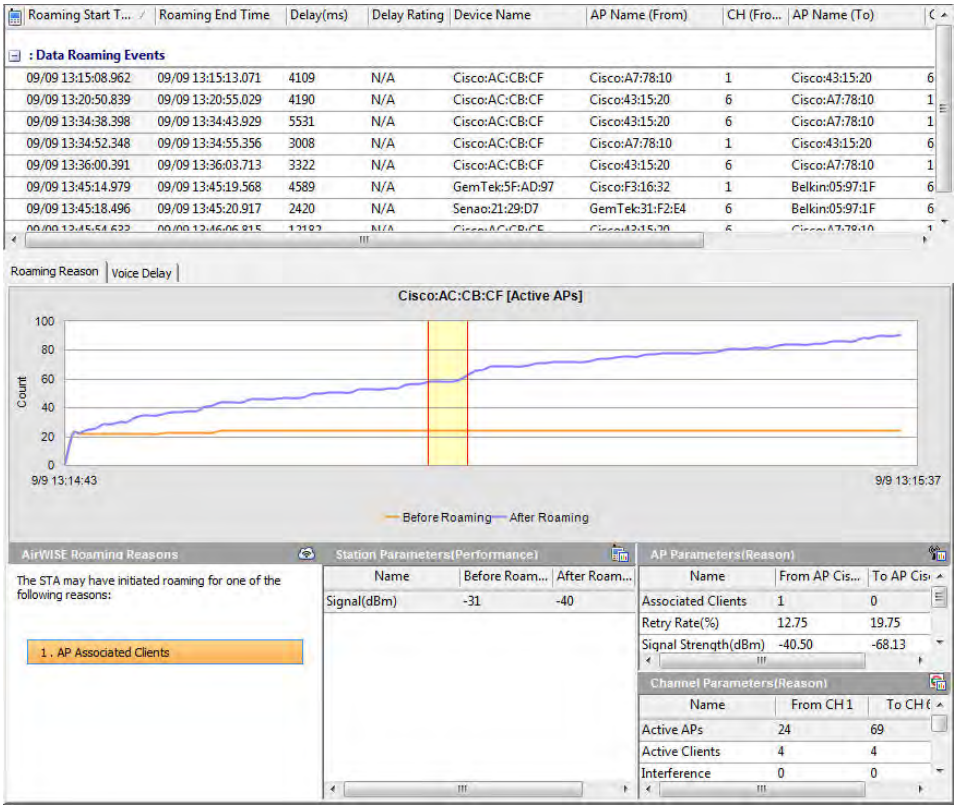
- **All Roaming Events**—The default option, this selection provides a broad overview of all devices experiencing roaming and the number of instances detected. This listing can include both standard wireless stations as well as VoFi phones.
- **List by Station**—This option displays only wireless stations, 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 (that is, 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 your selections in the Device Listing. After you have 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.

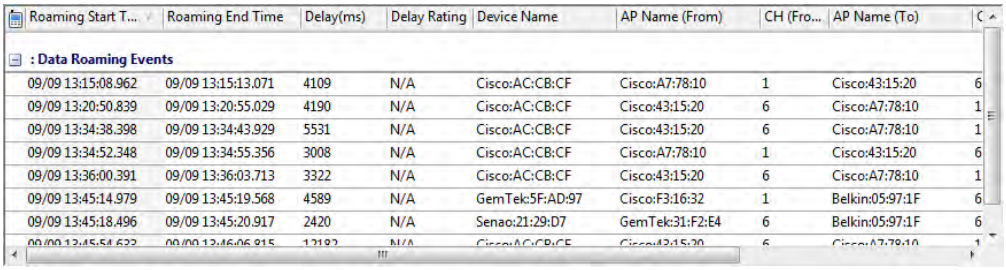


Due to the amount of information available, the Roaming Details pane is divided into three major sections: the Roaming Instance Table (across the top), Roaming Reasons (the first tab selected from the bottom), and Voice Delay Information (the second tab).

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, click the desired selection in the table and the other portions of the screen will refresh accordingly.



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 13:34:55.356	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	Senao:21:29:D7	GemTek:31:F2:E4	6	Belkin:05:97:1F	6

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

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.
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. ***Note:*** *The Rating column only applies to VoFi calls; data roams will simply display "N/A".*
Device Name	The name of the roaming device.
AP Name	These columns indicate the names of the APs involved in the roam (that

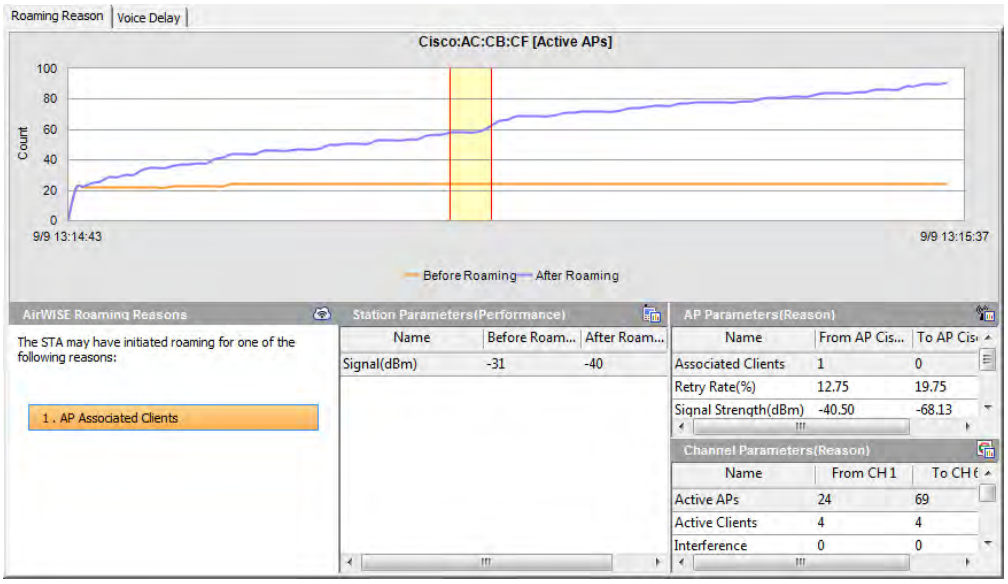
(From / To)	is, both the original AP and the one to which the device roamed).
CH (From / To)	These columns display the original channel (before roaming) and the final one (after roaming).
Signal (From / To)	These columns display the signal strength detected both before and after the roam.
MOS (From / To)	These fields provide the MOS score for the call both prior to and after roaming. ***Note:*** *The MOS columns pertain only to VoFi calls and will display "N/A" for data instances.*

Determining the Roaming Cause

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

Roaming Reasons

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



Note: *The Roaming Reasons pane in the lower-left lists possible reasons behind the instance of roaming. Clicking these reasons adjusts 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 you click 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.

Note: *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.*

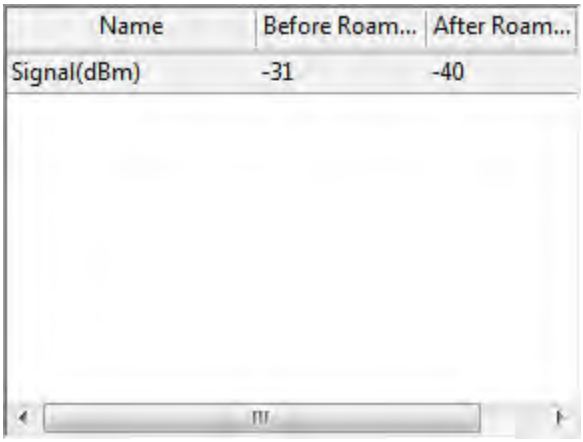
Each of the parameter panes display data in three basic columns:

- **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 (for example, MOS, Retry Rate, Jitter, and so on) improved after the roam finished; a thumbs-down will appear if the category suffered as a result of the roam.

This data can help you identify problems with your experience during the call process. For example, the roam shown in the figure above 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

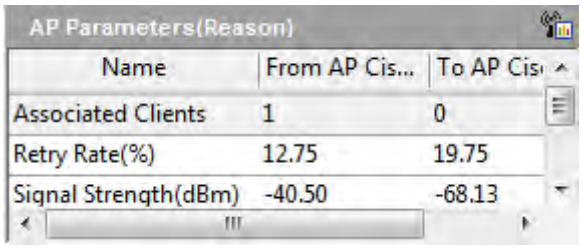
Immediately to the right of the Roaming Reasons pane, the Device Parameters field will vary depending on the type of roaming instance selected; instances of data roaming display the retry rates, CRC errors, and signal level both before and after the roam. For a VoFi roam, these details are supplemented by MOS and Jitter information.



Name	Before Roam...	After Roam...
Signal(dBm)	-31	-40

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 (for example, the original and final APs).



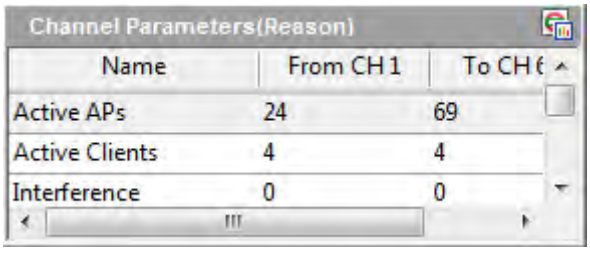
AP Parameters(Reason)

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

As shown above, you 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 only 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 you to identify whether a crowded or blocked channel is the root cause.



Channel Parameters(Reason)

Name	From CH 1	To CH 6
Active APs	24	69
Active Clients	4	4
Interference	0	0

By identifying the number of APs and clients present on the selected channel, you can see whether there were 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

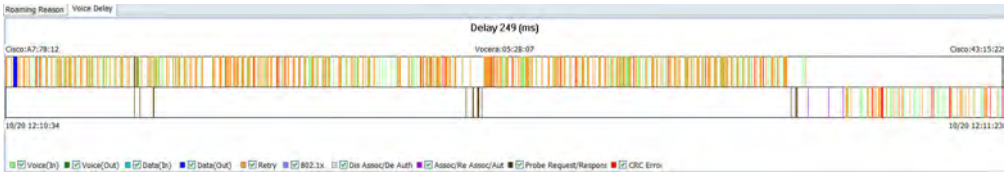
> ***Note:*** *The Voice Delay tab will only be available if an instance of VoFi roaming is selected, as its information does not apply to standard data roaming.*

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

- Packet Chart
- Delay Analysis
- Packet Decodes

Packet Chart

After you have made the desired selection in the Roaming Table, the Packet Chart updates to display a detailed chart of the frames transmitted and received during the conversation both before and after the instance of roaming.

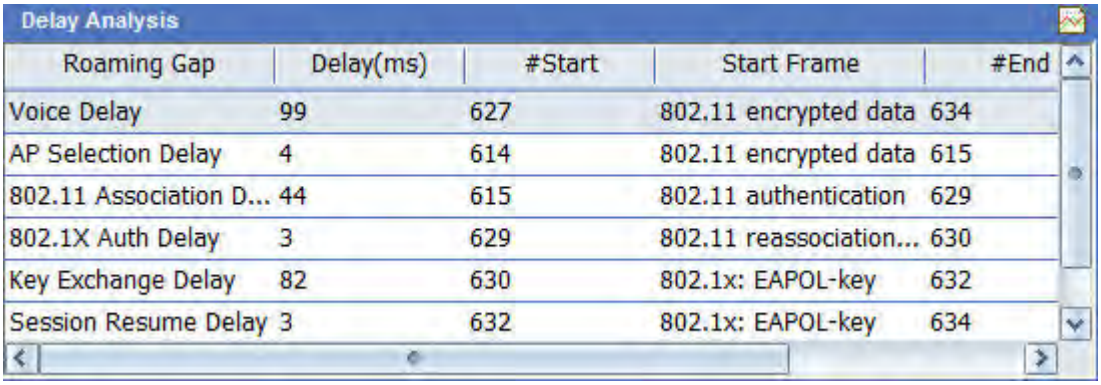


The chart highlights the selected roaming instance in red, with the color-coded packet displays on either side of the gap. You can check or uncheck options as desired in the color legend in order to view the frames detected during the call.

> ***Note:*** *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.

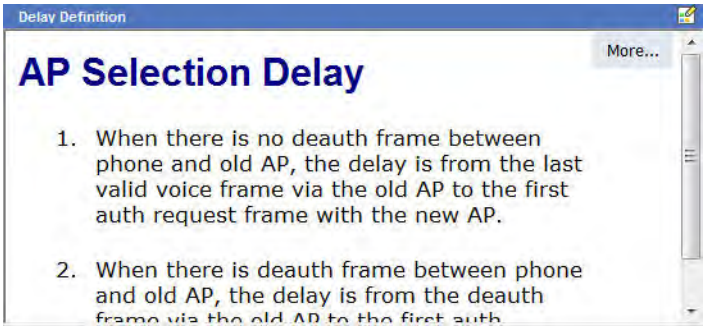


The Voice Delay Analysis (upper) portion of the pane breaks the total delay during the roam into (up to) 5 components, as described below:

- 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.

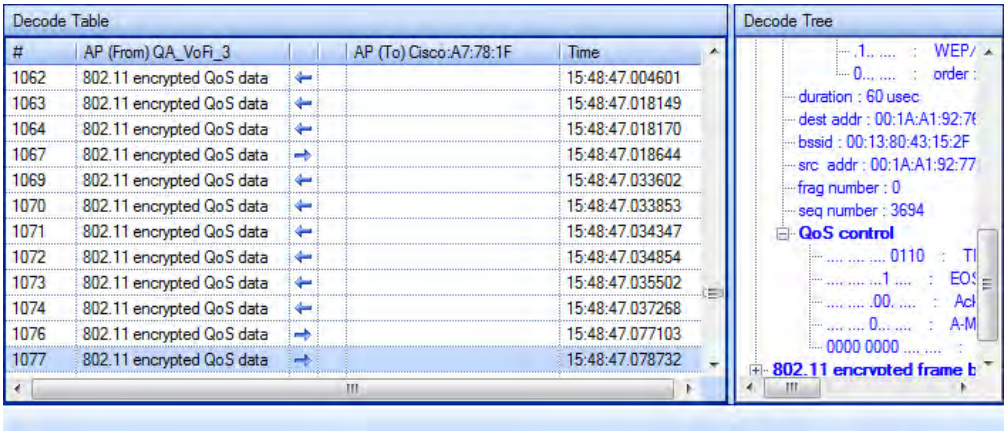
Note: *Selecting a specific delay option from the Delay Analysis table adjusts the Packet Chart to display frames specific to the selection made.*

The lower portion of the window displays advanced details about the delay selected. You can scroll through this information for specific data regarding how the delay is identified or click **More Info...** for additional details.



Use the Decode Table and Tree to help identify the packets transmitted before and after the roaming process. Selecting a specific packet displays its summary in the Decode Tree.

Packet Decodes



The table below describes the columns found in the Decode Table.

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, for example, 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.

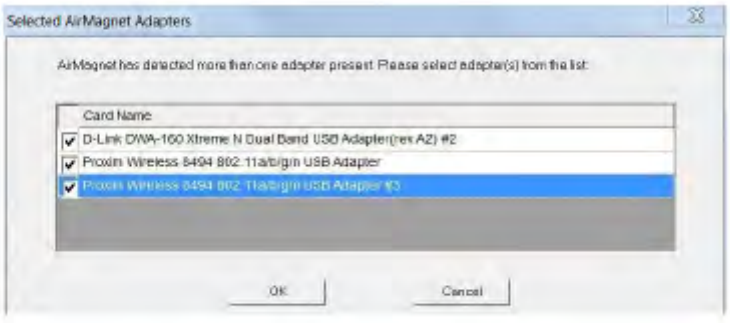
Multiple Adapters

The multiple adapter function is a capability whereby more than one Wi-Fi 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.

Notes: *1] The Roaming Analysis page requires the use of multi-adapters. 2]Packets captured from multiple adapters get saved as a single trace file.*

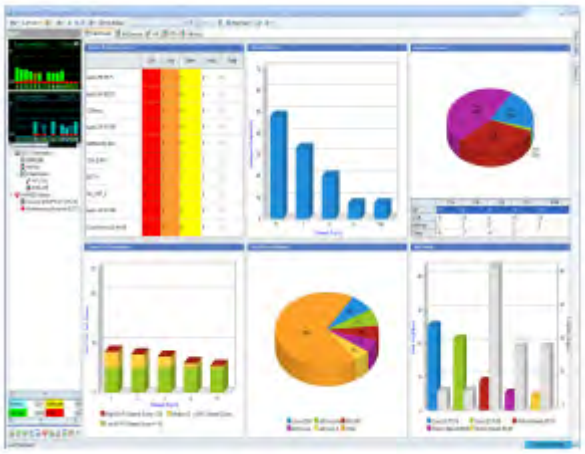
To take advantage of the multi-adapter capability, different pages use different display modes to render data. Refer to Roaming Instance Table.

For Adapter-Specific screens, a new menu appears in the toolbar that allows you to specify the adapter to be used. Refer to Utilizing Multiple Wireless Adapters.

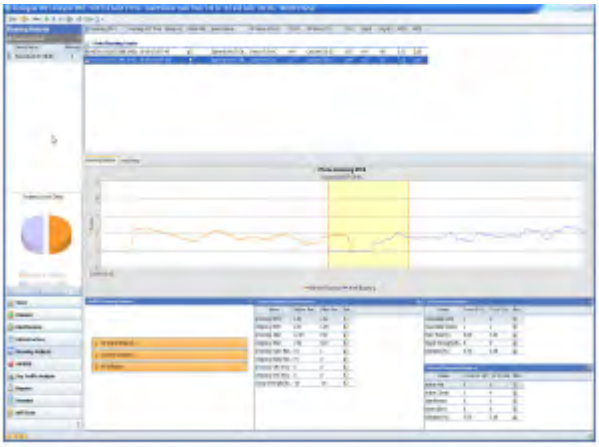


View	Page
Consolidated Captured data from all adapters is analyzed and presented in a single 'virtual' view.	Start Roaming Analysis
Split Data and analysis for each adapter is presented in its own window within a page.	Channel Decodes
Adapter Specific Data and analysis for an adapter are shown singly. User selects which adapter view to use.	Infrastructure AirWISE Top Traffic Analysis Reports Wi-Fi Tools
Not Available	Interference

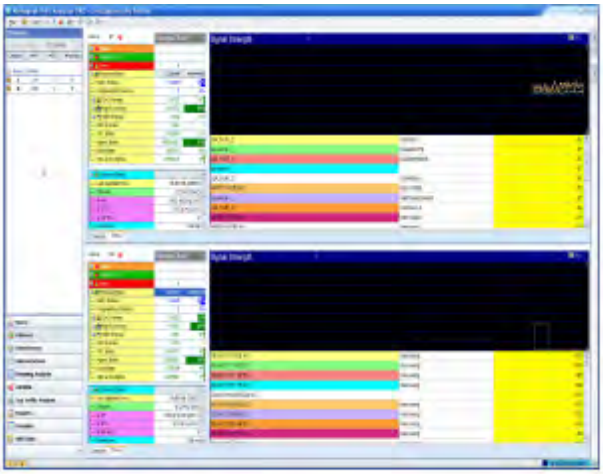
Start Page



Roaming Analysis Page

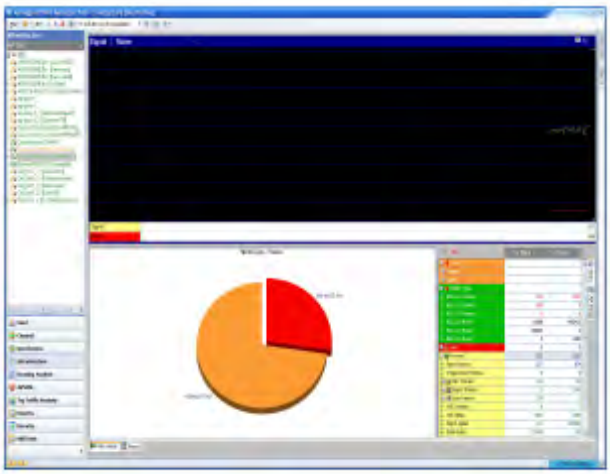


Channel Page

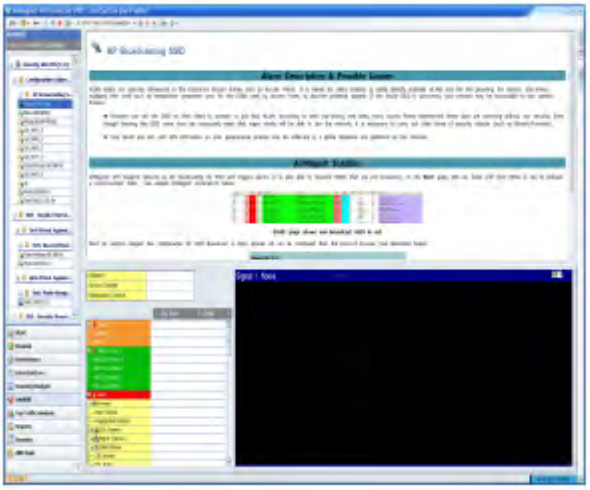


Decodes Page

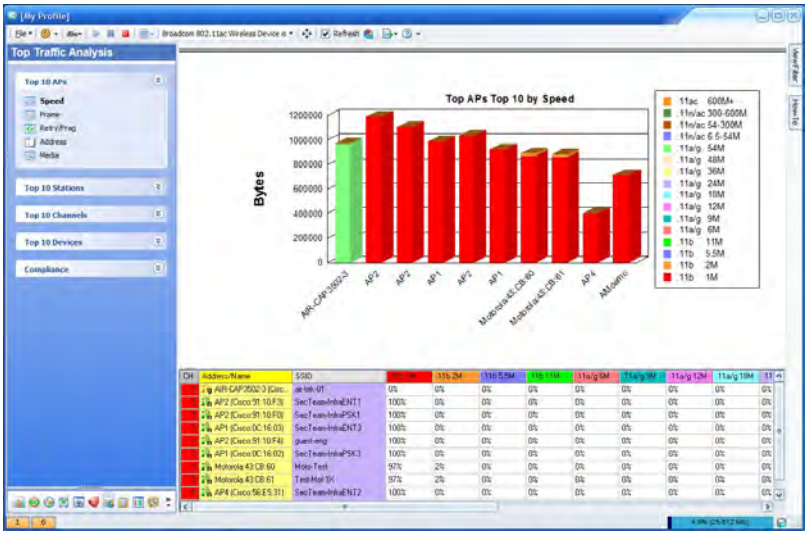
Infrastructure Page



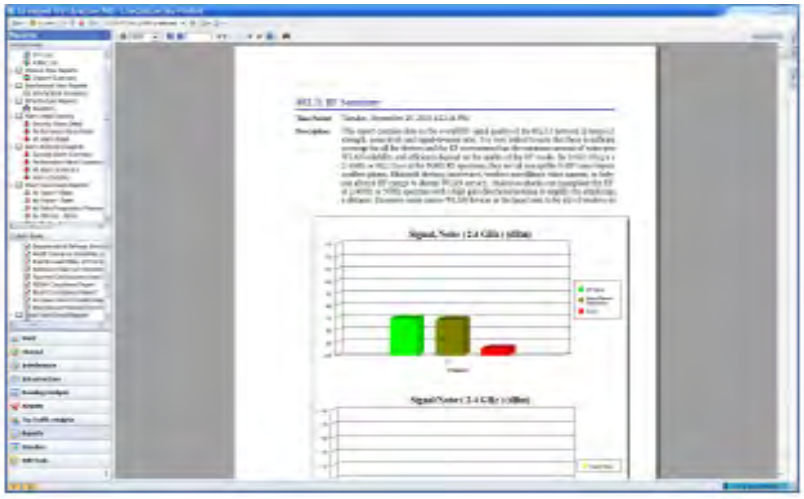
AirWISE Page



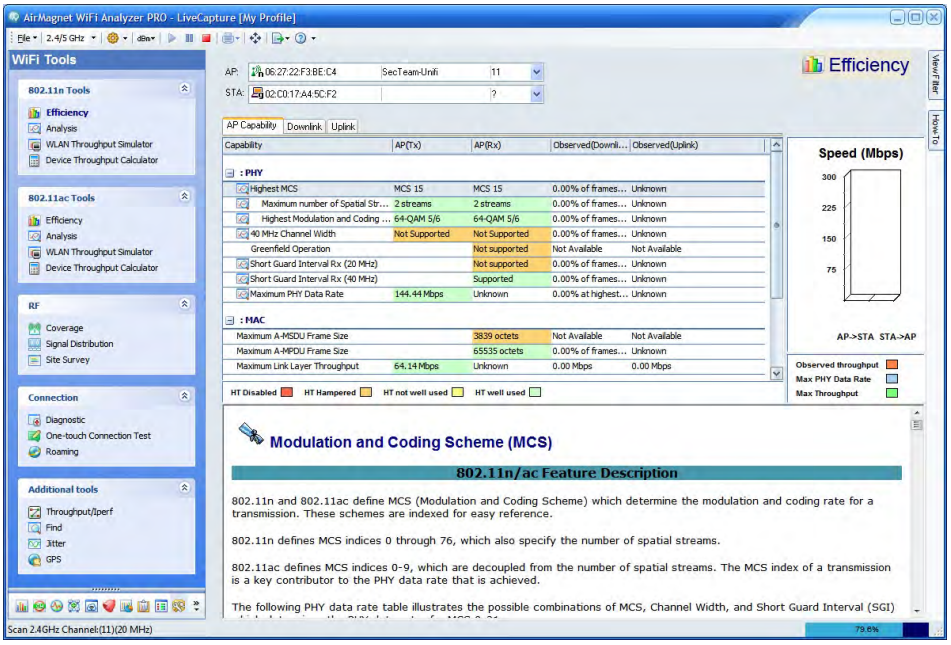
Top Traffic Analysis Page



Reports Page

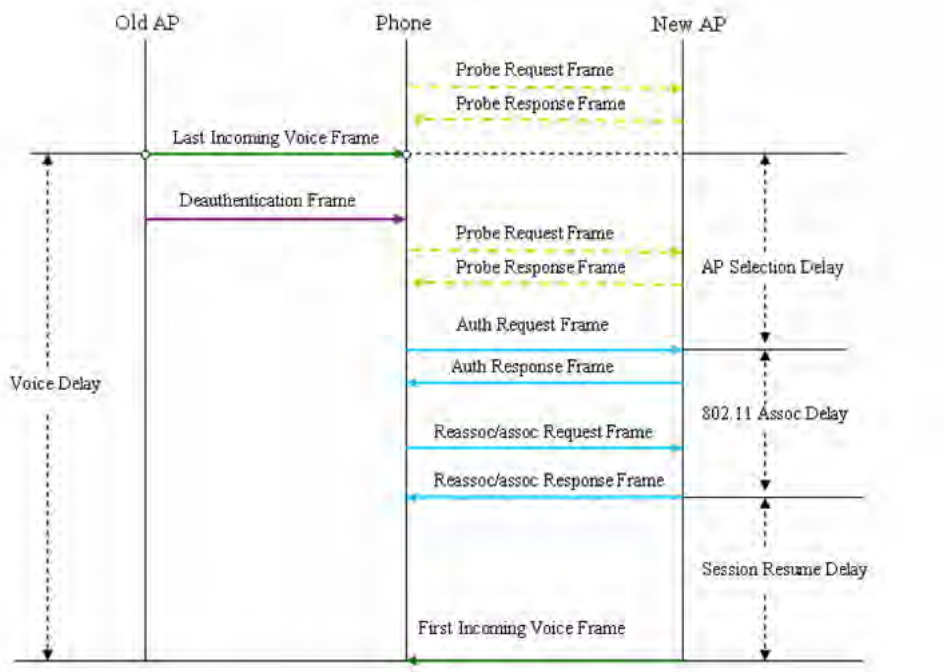


Wi-Fi Tools Page



Roaming Gap Definition and Calculation for Cisco and Vocera Phones

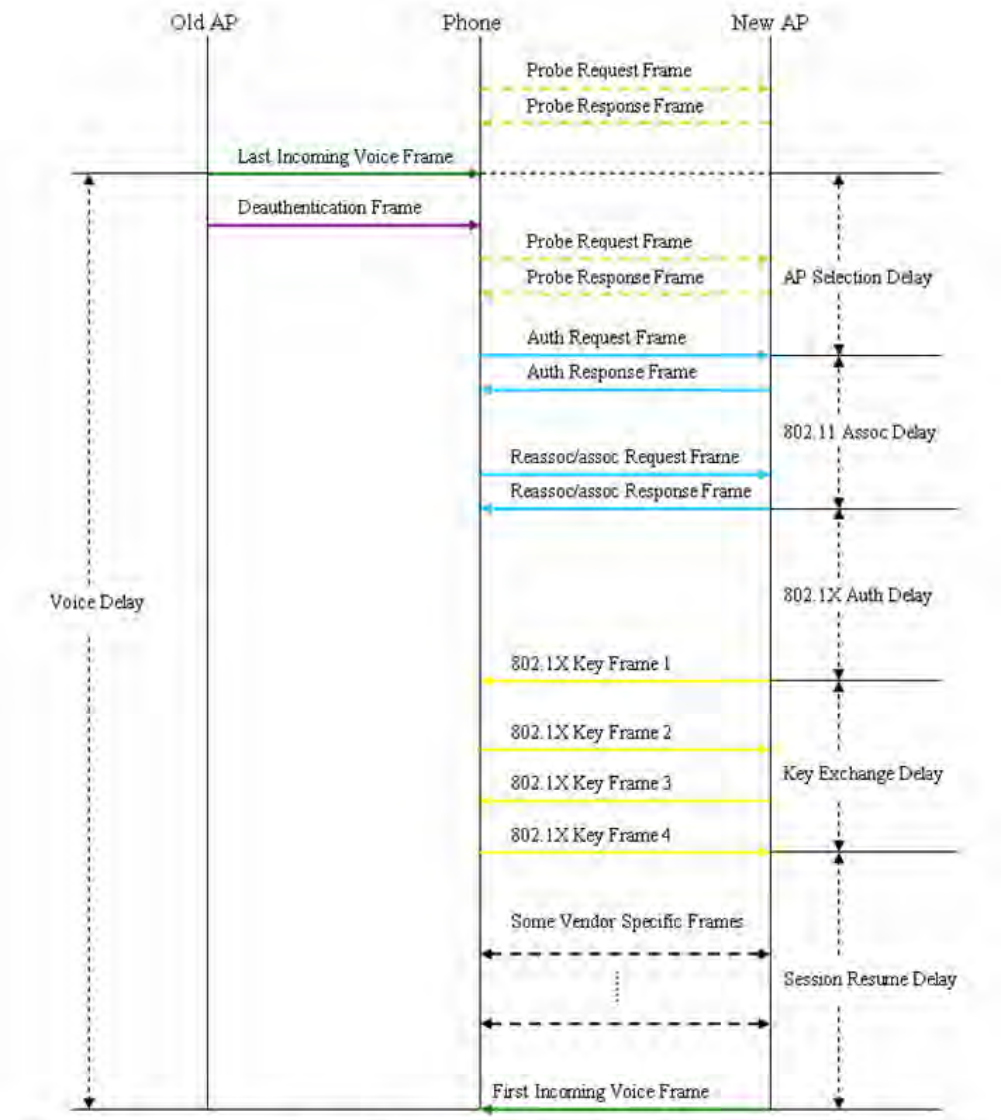
A. Without 802.1X Authentication



Gap Types	From Frame	To Frame
AP Selection Delay	Last Incoming Voice via Old AP/ or Deauth frame(if available)	First Auth Request
802.11 Assoc Delay	First Auth Request	Last Reassoc/Assoc Response
Session Resume Delay	Last Reassoc/Assoc Response	First Incoming Voice via New AP
Voice Delay	Last Incoming Voice via Old AP	First Incoming Voice via New AP

Notes:
If you use the last incoming voice with an old AP as the beginning of AP selection delay:Voice Delay = AP Selection Delay + 802.11 Association Delay + Session Resume Delay
If you use the Deauthentication frame as the beginning of an AP selection delay:Voice Delay>AP Selection Delay + 802.11 Association Delay + Session Resume Delay

B. With 802.1X Authentication

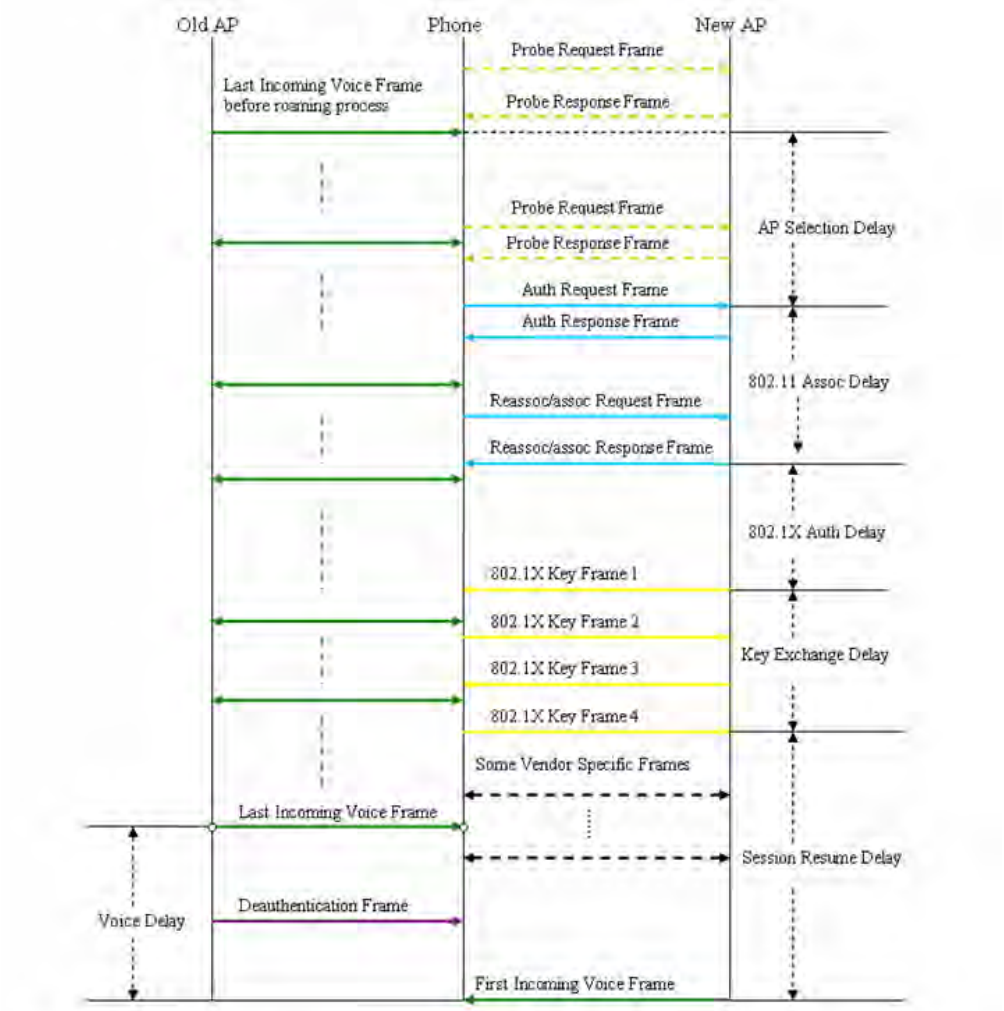


Gap Types	From Frame	To Frame
AP Selection Delay	Last Incoming Voice via Old AP/ or Deauth frame(if available)	First Auth Request
802.11 Assoc Delay	First Auth Request	Last Reassoc/Assoc Response
802.1X Auth Delay	Last Reassoc/Assoc Response	First Key Exchange
Key Exchange Delay	First Key Exchange	Last Key Exchange
Session Resume Delay	Last Key Exchange	First Incoming Voice via New AP
Voice Delay	Last Incoming Voice via Old AP	First Incoming Voice via New AP

Notes:
If you use the last incoming voice wusing an old AP as the beginning of AP selection delay:Voice Delay = AP Selection Delay + 802.11 Association Delay + Session Resume Delay
If you use the Deauthentication frame as the beginning of an AP selection delay:Voice Delay>AP Selection Delay + 802.11 Association Delay + Session Resume Delay

Roaming Gap Definition and Calculation for SpectraLink Phones

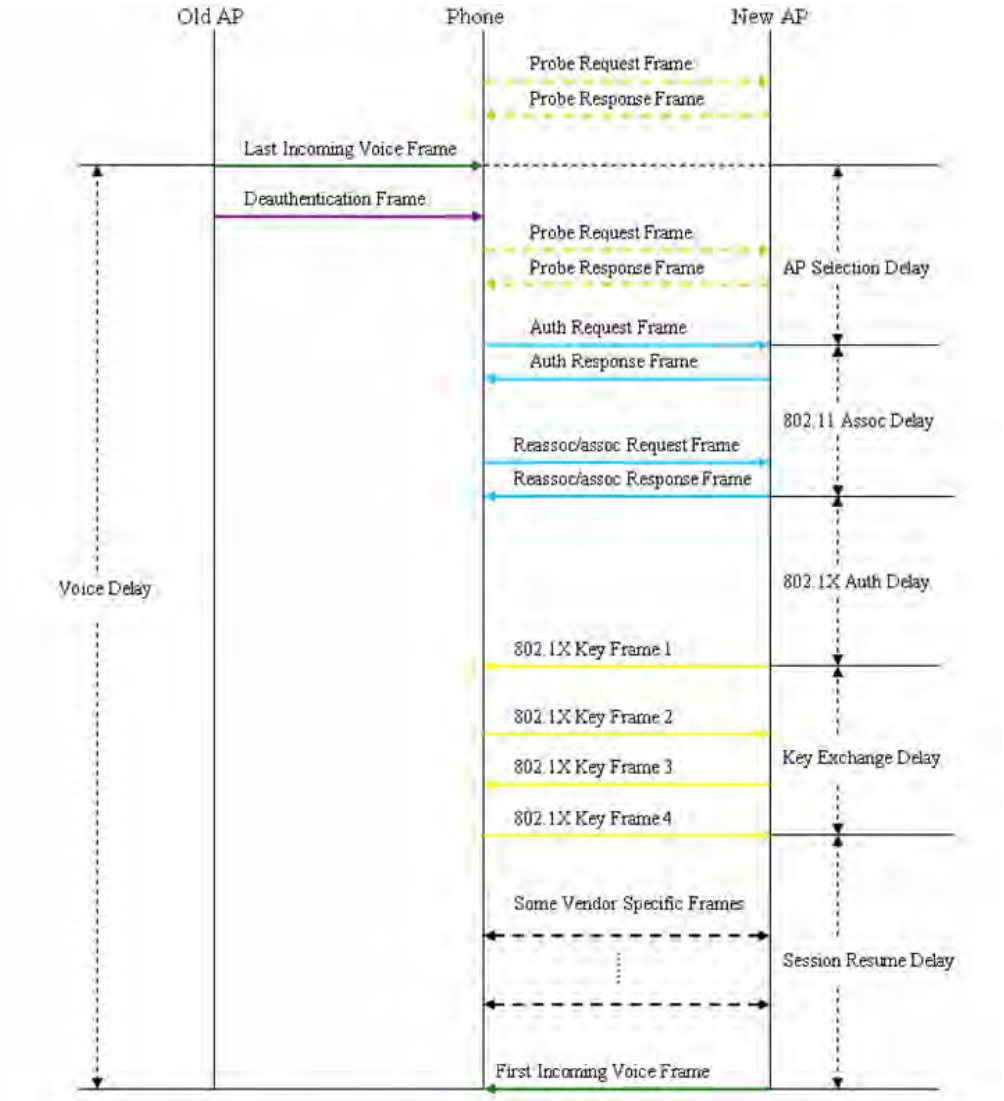
A. With Voice Frames During the Roaming Process



Gap Types	From Frame	To Frame
AP Selection Delay	Last voice frame via old AP/or Deauth frame(if available)	First Auth Request
802.11 Assoc Delay	First Auth Request	Last Reassoc/Assoc Response
802.1X Auth Delay	Last Reassoc/Assoc Response	First Key Exchange
Key Exchange Delay	First Key Exchange	Last Key Exchange
Session Resume Delay	Last Key Exchange	First Voice Frame via New AP
Voice Delay	Last Incoming Voice via Old AP	First Incoming Voice Frame via New AP
Roaming Delay	First Probe Request	First Voice via New AP

Note: *In this case, voice delay is not the sum of other delays. It may be very small, since the voice frames keep going during the roaming process.*

B. With No Voice Frame During the Roaming Process



Gap Types	From Frame	To Frame
AP Selection Delay	Last Incoming Voice via Old AP/ or Deauth frame(if available)	First Auth Request
802.11 Assoc Delay	First Auth Request	Last Reassoc/Assoc Response
802.1X Auth Delay	Last Reassoc/Assoc Response	First Key Exchange
Key Exchange Delay	First Key Exchange	Last Key Exchange
Session Resume Delay	Last Key Exchange	First Incoming Voice via New AP
Voice Delay	Last Incoming Voice via Old AP	First Incoming Voice via New AP

Notes: *If you use the last incoming voice with an old AP as the beginning of AP selection delay:Voice Delay = AP Selection Delay + 802.11 Association Delay + Session Resume Delay.*
If your use a Deauthentication frame as the beginning of the AP selection delay:Voice Delay>AP Selection Delay + 802.11 Association Delay + Session Resume Delay.

System Configuration

Configuring AirMagnet WiFi Analyzer

To effectively solve your network issues with AirMagnet WiFi Analyzer, the first thing you need to do is to make sure that the various system parameters in the application are properly configured. All system configurations are conducted in the Configuration dialog box, which contains a number of tabs across its top, each representing a specific system parameter.

All AirMagnet WiFi Analyzer system configuration settings 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.

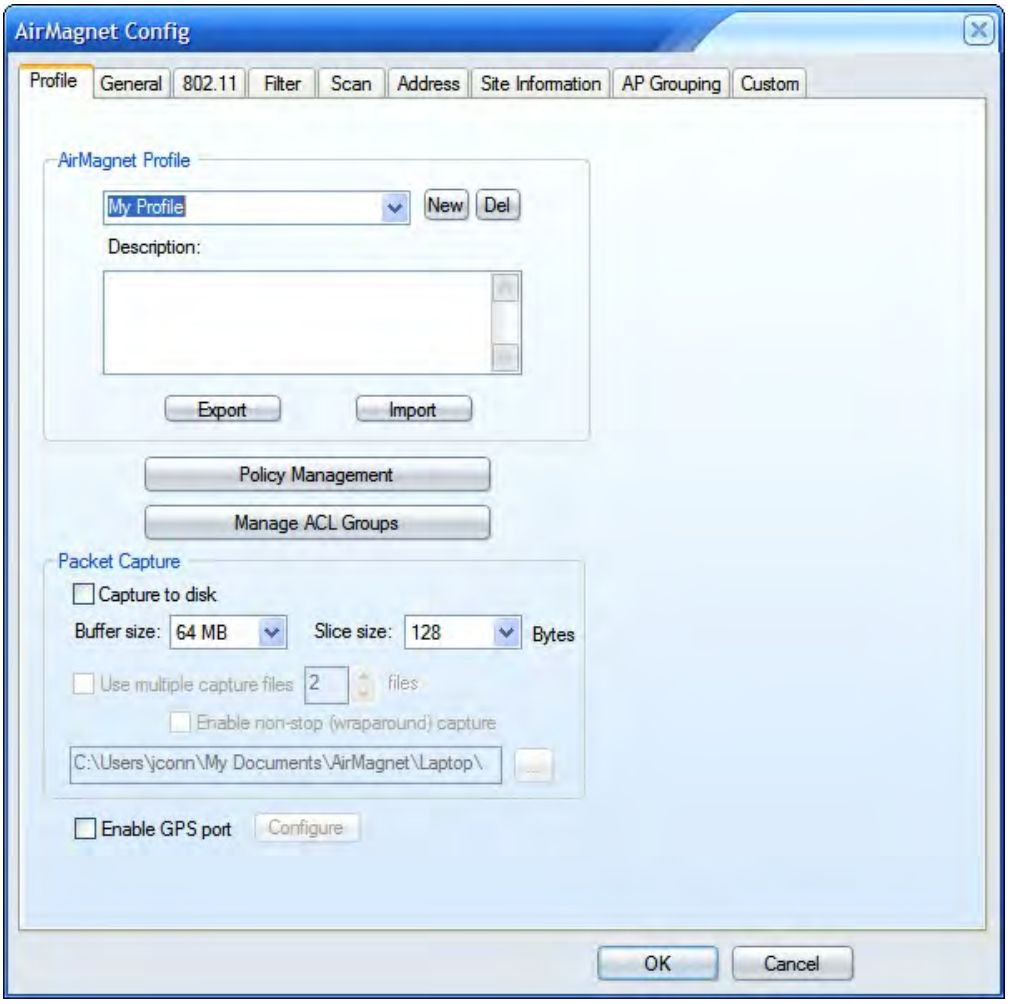
If your wireless LAN administration responsibility covers more than one site, or if you are servicing more than one customer, you will find the AirMagnet Configuration Profile utility very helpful for managing various configuration settings.

For integration with Windows wireless profiles, refer to Integration with Windows Wireless Configuration.

To access the AirMagnet Configuration screen, do one of the following from the menu bar:

- Double-click  (**Configure**).
- Click **File>Configure....**

The AirMagnet Configuration dialog box appears. The image below shows the default AirMagnet Configuration dialog box.



Note: *By default, the Profile tab is highlighted when the AirMagnet Configuration dialog box opens. You can choose to view or configure any system parameters by clicking the corresponding tab across the top of the dialog box.*

Setting Up System Profile

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

Note: *Once configured, the name of the profile appears in the title bar on the screens. If no profile has been configured, then the default profile name [My Profile] displays in the title bar instead.*

Import: If available, you can import a previously created profile. Click **Import** and browse to the *.APF* file.

Export: You can export the current system profile. Click **Export**. Name the file and browse to the desired save location. Click **Save**.

To set up your AirMagnet WiFi Analyzer's system profile:

1. From the AirMagnet Configuration dialog box, make sure the Profile tab is selected.
2. Select **New**, and overwrite **[New Profile]** with a unique a name for the profile.
3. Click in the **Description** box and enter a description for this profile.
4. Click **Policy Management** to set the policy of the profile. Refer to Managing Network Policies for more information.
5. Click **Manage ACL Groups** to configure the ACL groups of the profile. Refer to Assigning Policies to ACL Groups for more information.

Packet Capture:

6. You can choose to capture packet data to disk by three methods:Capture to disk, Use multiple capture files and Enable non-stop capture.

   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** drop-down. You can also choose a Byte Slice size from the **Slice size** drop-down. 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 can choose to set the number of multiple consecutive files to be captured of the file size specified in "**Capture to disk**." Each file will receive an end-of-capture time stamp file name (for example, July 12, 2011-1410.amm). The file will be saved to the location set in the browse box. The default save location is *airmagnet/laptop*.

   Enable non-stop (wrap around) capture: Checking this option enables a non-stop capture mode. 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 is continuously captured while the total number of files is limited to the number set in "Use multiple capture files." non-stop capture continues until this check box is unchecked.

   Optionally, check the **Enable GPS port** option to use this feature and then click **Configure...** to complete the GPS configuration.

7. Click **OK** to finish setting up the profile.

***Note:** If applicable, click **Import** to browse and import an existing profile. Optionally, you can export the profile for record-keeping or to share it with others.*

Configuring GPS Settings

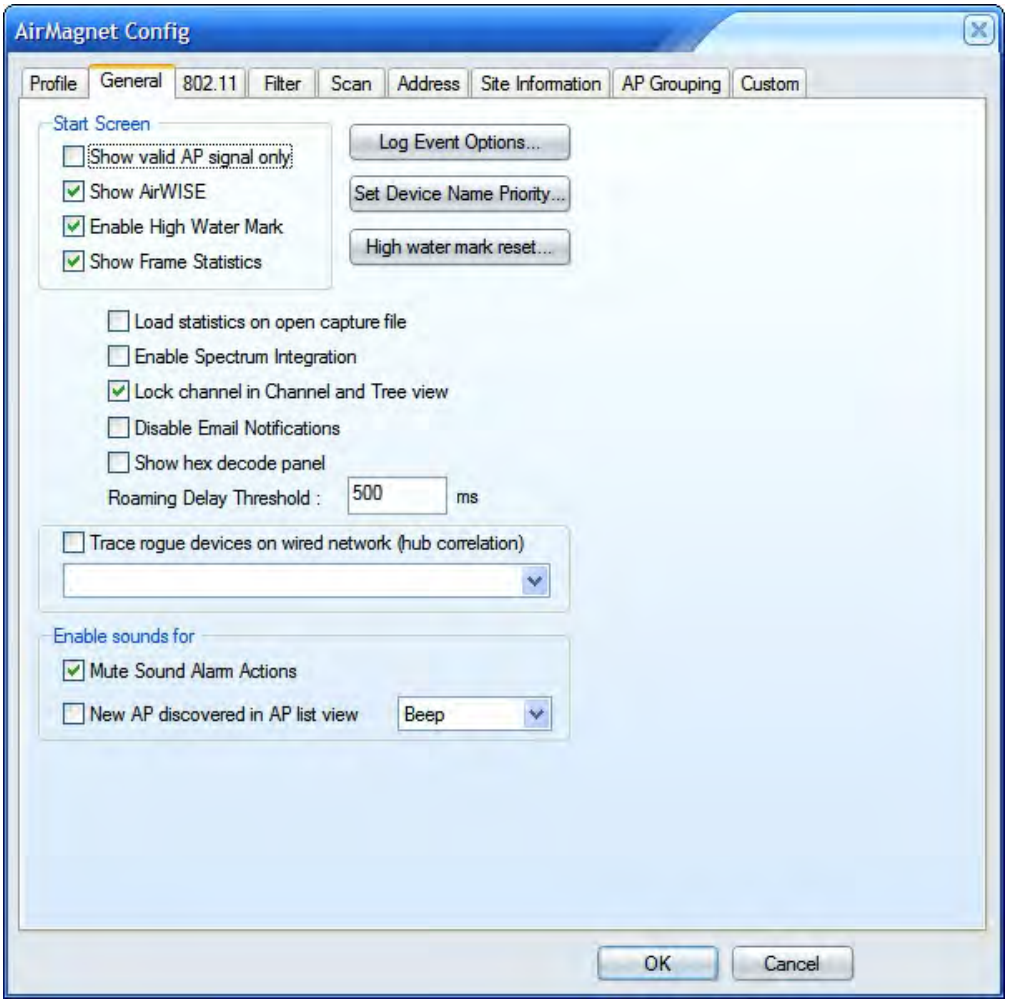
Once you have checked the Enable GPS Port check box and then clicked the Configure button, the GPS Configuration dialog box appears, as shown in the figure below. The dialog box provides the interface for you to configure the port that AirMagnet WiFi Analyzer will use to communicate with the GPS device.

To configure the GPS port:

1. Make the desired selections from the dialog box.
2. Click the **AP GPS Location...** button to configure the GPS locations of the APs of interest on the network, as shown in Getting AP GPS Location Information.

Configuring General System Parameters

The General tab shows the parameters that dictate the general behavior of AirMagnet WiFi Analyzer. When opened for the first time upon installation, it shows the default settings. You can make changes to any of the parameters at any time according to the need of your WLAN.



To configure the General settings of your AirMagnet WiFi Analyzer:

1. From the AirMagnet Configuration dialog box, select the **General** tab.
2. Make the desired selections, as described in the following table.
3. Click **OK** when finished.

Parameter	Description
Show valid AP signal only	If checked, the system will not display brown bars representing Cross-Channel Interference in the signal graph on the Start screen.
Show AirWISE	If selected, the AirWISE pane will appear in the lower-middle part of the Start screen.
Enable High Water	If checked, the graphs in the top left corner of the start screen

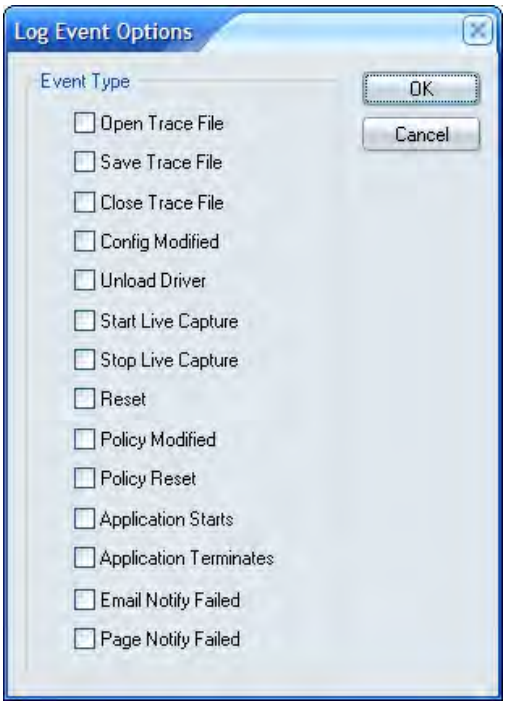
Mark	will store a high point during a user-specified interval. This allows you to see the highest point your network traffic has reached within a given time. To specify this time, click the Start screen high water mark reset button.
Show Frame Statistics	If selected, the frame count pane will appear below the pie chart on the Start screen. ***Note:*** *A larger screen display is needed in order to show the frame statistics.*
Load statistics on open capture files	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 Integration	If checked, AirMagnet Spectrum XT integration will be enabled. Refer to AirMagnet Spectrum Analyzer Integration 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, the system will not send email notification.
Show hex decode panel	If checked, the hexadecimal panel will be displayed on the Decodes screen.
Roaming Delay Threshold	The difference between Roaming Start and End time. Generally, only for voice roaming, if the delay is longer than voice roaming delay threshold it will show a thumb-down.
Trace rogue devices on wired network	If checked, the system will trace rogue devices on the wired side of the network. When tracing is active, AirMagnet WiFi Analyzer will attempt to trace all rogue devices that are connected to the same hub as the Wi-Fi computer. ***Note:*** *Your laptop must be connected via an Ethernet*

	connection to use this option.
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. ***Note:*** *You can use click the down arrow to select a sound option from the list menu.*

Customizing Event Log Options

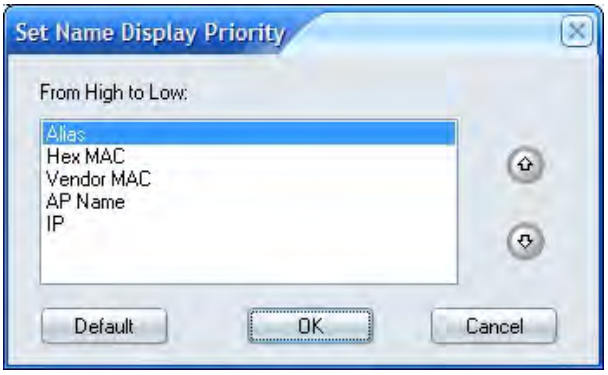
This option allows you to specify the actions by AirMagnet WiFi Analyzer that will be recorded to the Windows event log. While having all of these options enabled allows you to keep a record of all historical data or events on that AirMagnet WiFi Analyzer has captured, it can also consume a large amount of disk space rapidly.

1. Click **Log Event Options**....
2. Select the options you wish to record.
3. Click **OK**.



Setting Device Name Display Priority

This option allows you to set the order of priority devices are shown on the screen.



1. Click **Set device name priority**....
2. Highlight the options one at a time and set their order of priority using the up and/or down arrow.
3. Click **OK** when done.

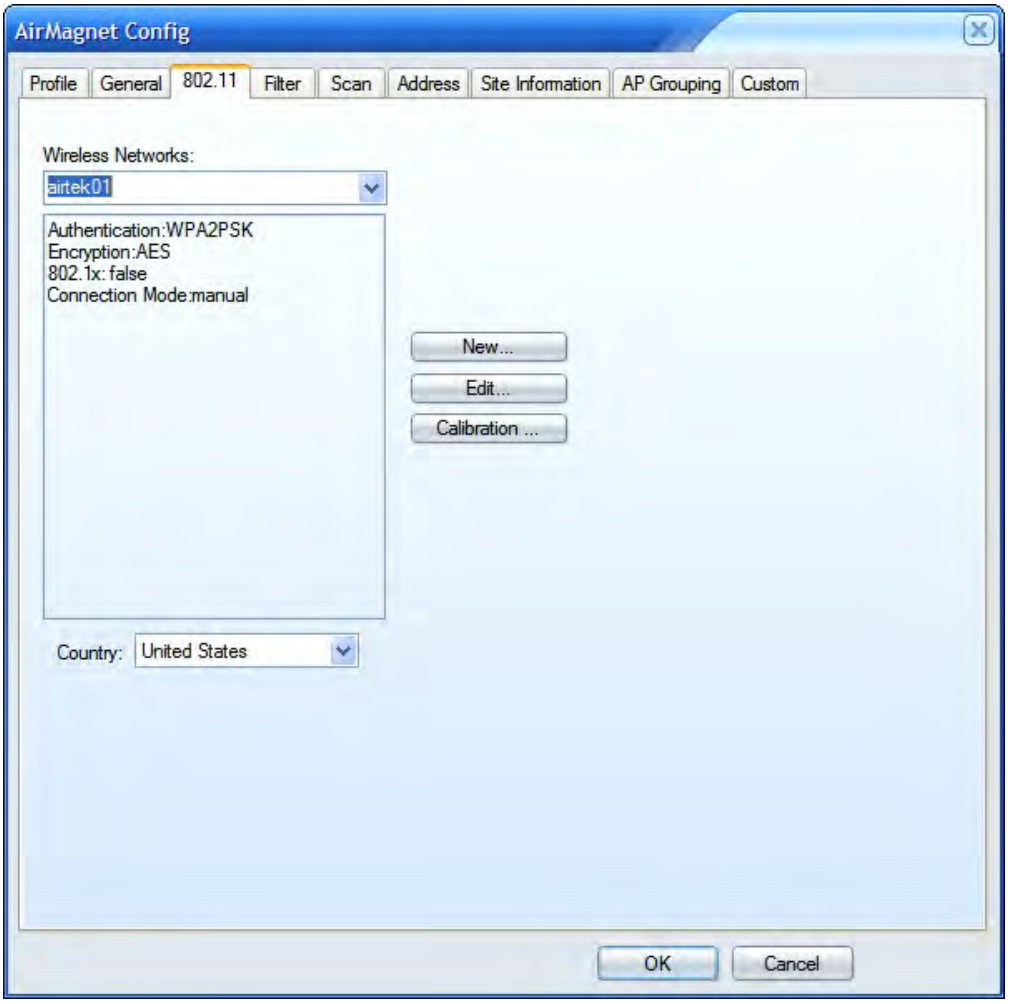
Resetting High Water Mark

Click this button to reset the high water mark.

1. Click **High water mark reset**....
2. Select an reset option.
3. Click **OK**.

Configuring 802.11 Settings

The 802.11 configuration screen allows you to set the parameters to enable an active association with an AP on the network. You need to set up at least one wireless network before using any of the active tools such as One Touch Connection Test or Site Survey Tool.



This procedure enables establishing the authentication and security password for the AP or SSID. The options available depend on the adapter and OS being used.

Note: *This can also be accomplished in Windows by setting up a Windows wireless network connection.*

1. Open **Configure** and click the **802.11** tab.
2. Click **New** to create a new profile. Type the correct name for the AP or SSID and click **OK**.
3. With the SSID or AP name selected in the Wireless Networks drop-down, click **Edit**.
4. Make the desired entries and/or selections in the **Connections** tab and **Security** tab as you normally would for a new Windows Wireless connection.
5. Click **OK**.

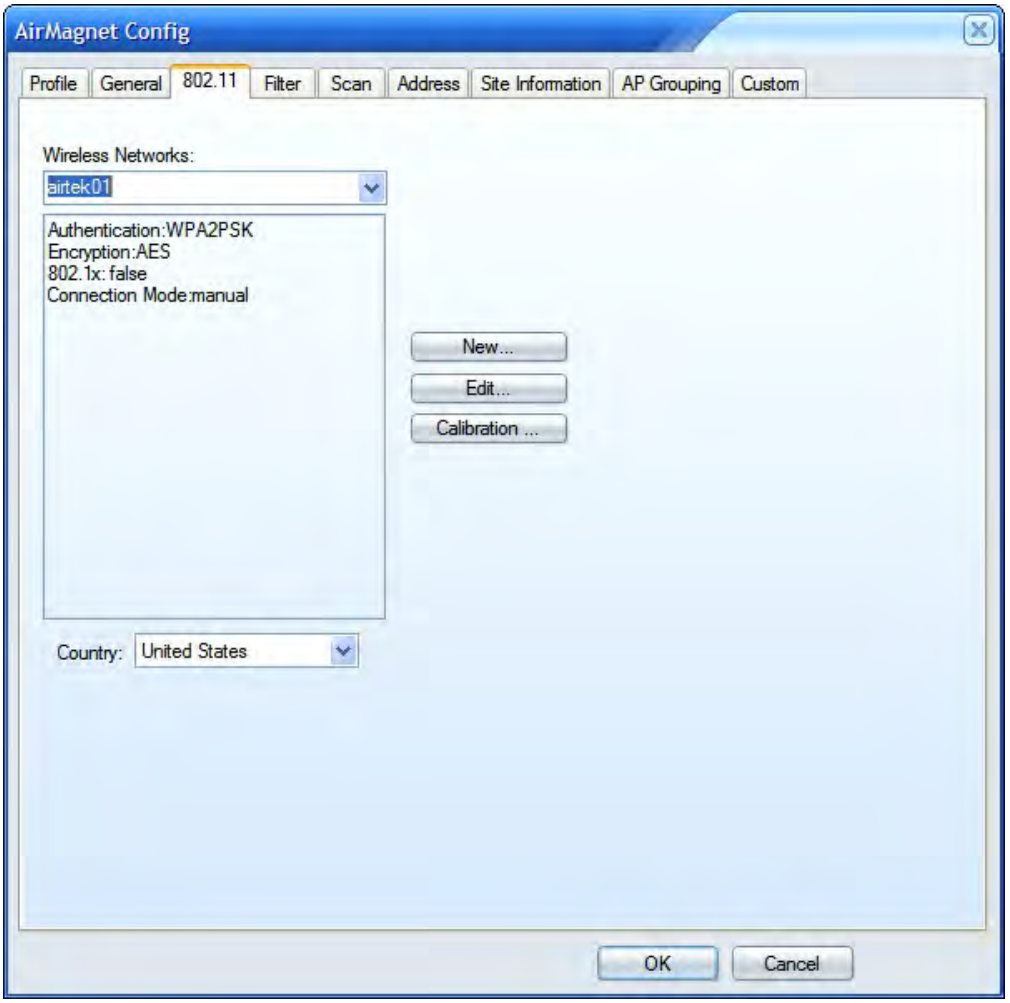
RF Signal Calibration

About RF Calibration

Consumers have a wide variety of 802.11 wireless network adapters to choose from for use with different applications. Since these adapters are designed and manufactured by different vendors, there is a possibility of manufacturing differences between the vendors leading to the possibility of different signal readings.

As the leader in Wi-Fi network analysis and troubleshooting, AirMagnet has completed an exhaustive calibration and testing program for most of our “preferred” list of Wi-Fi 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 Wi-Fi 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.

How to Use RF Calibration Options 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….**

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:

- **No Calibration**
- **Pre-Defined Calibration** (This is the entry below No Calibration, for example., AirMagnet 802.11 a/b/g/n Wireless PC card.)
- **Custom Calibration**

Import/Export Calibration Configuration

You may import and export modified calibration configurations (not applicable to No Calibration). This feature enables you to share adapter calibration settings among AirMagnet WiFi Analyzer applications (version 10.7.1 or higher).

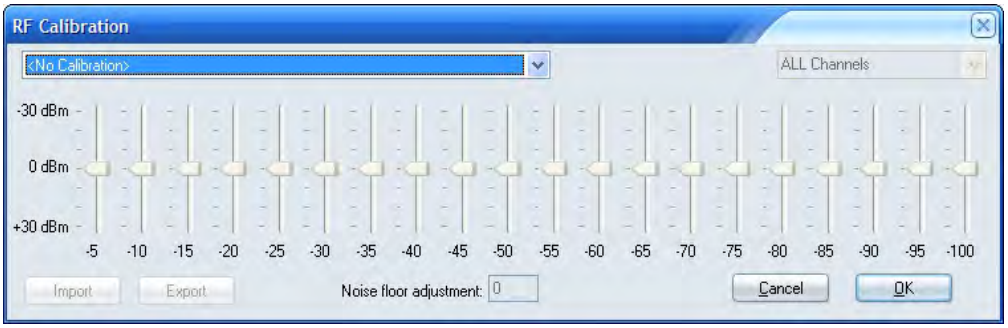
1. From the File menu, click **Configure**.
2. Click the **802.11** tab. Click **Calibration**.
3. From the **RF Calibration** drop-down, select either **Pre-Defined Calibration** or **Custom Calibration.**
4. To Import, Click **Import**. Browse and select the desired file (.ini extension). Click **Open**.
5. To Export, Click **Export**. Give the file a name and browse to the desired save location. Click **Save**.

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, perform the following steps:

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 the figure below.



Note: *When the user has selected the "No calibration" option, all other controls in the RF calibration dialog box will be grayed out (unavailable).*

2. Click the **OK** button to implement the selection.

Pre-Defined Calibration

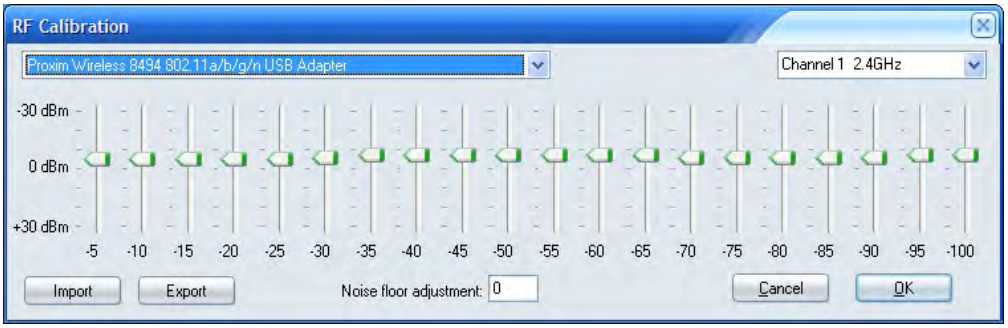
If the wireless network adapter you are using happens to be on the pre-calibrated list, then the AirMagnet application automatically recognizes the adapter and displays the pre-defined calibration option. In other words, if your wireless network adapter is displayed as a Pre-Defined Calibration entry 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 attenuator placed in between the two. The attenuation is achieved by tuning down the radio signal power the attenuator receives from the AP. For example, if the attenuator 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.

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 Wi-Fi 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, do the following:

1. Click the down arrow and verify if your wireless network adapter appears as a Pre-defined Calibration entry. Refer to the figure below.



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

Note: *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, do the following:

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.

Note: *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 make changes to any other channels, you have to make the changes channel by following the same steps.*

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.

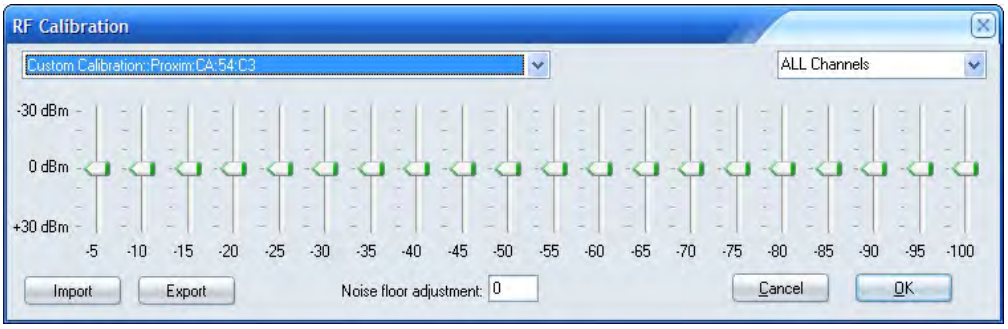
Custom calibration patterns can be created to equalize the signal strength readings between any combination of Wi-Fi adapters. Begin by measuring (similar to the process defined in the pre-calibration section) two different radios with zero offsets at varying distances, comparing the received signal strengths at each distance, then calculating the differences between Wi-Fi adapters and using the differences to set the offset of one radio in an effort to match the signal strength reading of the other Wi-Fi adapter.

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 Wi-Fi adapters to exhibit similar signal level readings. Without using this feature, the signal level readings may vary significantly between Wi-Fi 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 Wi-Fi 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, do the following:

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 the figure below.



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

> ***Note:*** *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.*

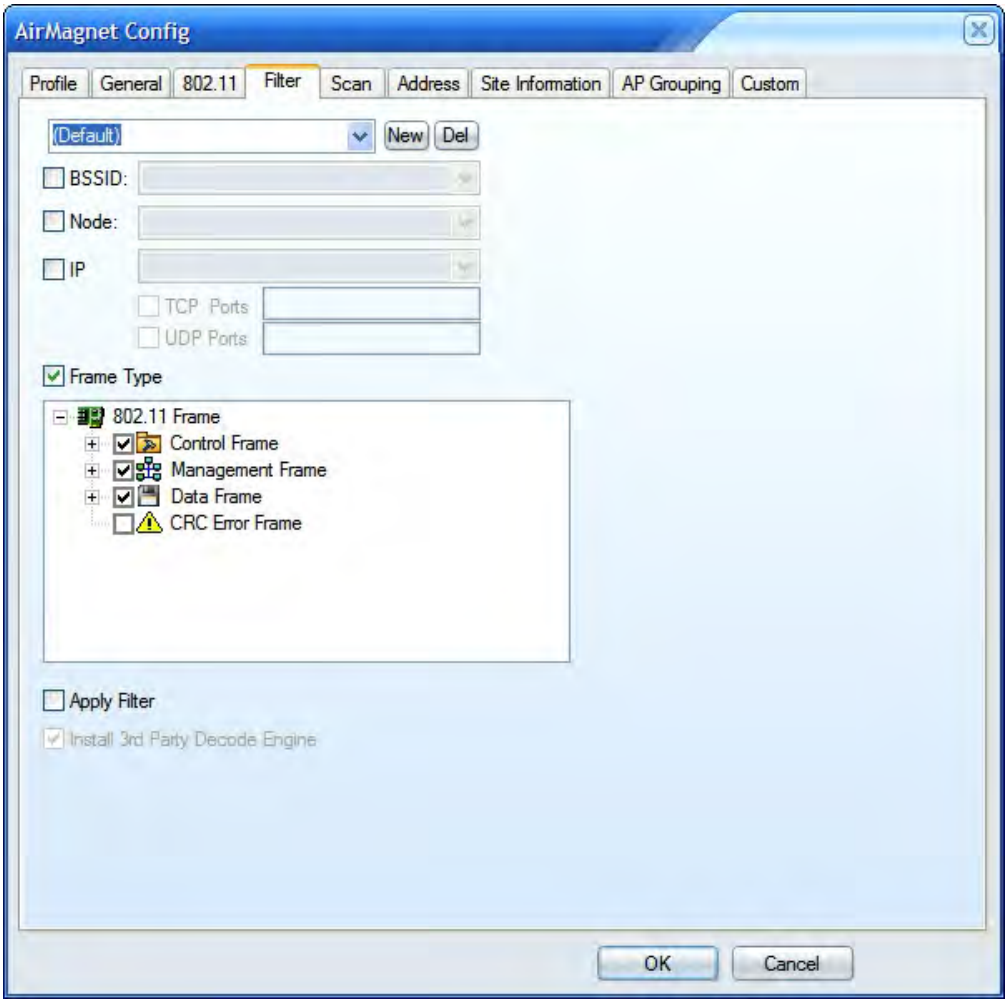
3. Use the sliders to adjust the RF signal strengths.
4. If you wish, highlight the number for noise floor adjustment box and type a new value over it.
5. Click **OK** when complete.

Configuring Data Filters

AirMagnet WiFi Analyzer provides four options for filtering the data it captures, that is, by BSSID, Node, IP, and/or Frame Type. They allow the user to use various sampling techniques to scan all available channels for 802.11 frames for statistical analysis. By default, AirMagnet WiFi Analyzer captures all data that pass through the WLAN and displays them on the screen. This, at times, may make it difficult for users to identify and solve issues that are the most critical to their networks.

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 WiFi Analyzer to filter or discard those unwanted 802.11 packets. These basic troubleshooting techniques will help detect and pinpoint any problem that may exist.

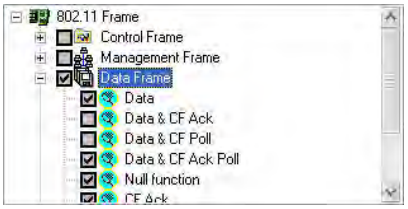
Creating a New Filter



1. From the AirMagnet Configuration screen, click the **Filter** tab.
2. From the Filter dialog box, click **New** and enter a name for the filter.

3. Configure the options one at a time, that is., SSID, Node, IP, or Frame Type.

- To filter by BSSID, check the **BSSID** check box and select a BSSID from the drop-down list.
- To filter by Node, check the **Node** check box and select a node from the drop-down list.
- To filter by IP, check the **IP** check box, select an IP address from the drop-down list, and check TCP and/or UDP and enter the port number(s).
- To filter by Frame Type, check the **Frame Type** check box, expand the frame options one by one, uncheck all frame types, and then select only those of interest.



4. Check the **Apply Filter** check box. This check box must be checked in order to activate the filter.
5. Click **OK**.

Note: *When* ***Apply Filter*** *check box is checked, the filter you choose in this dialog box will be automatically applied on the Decodes screen, meaning that only the frames that match the parameters of the filter will pass through the filter. All filters you have created will be kept in the drop-down list in the top part of the Filter dialog box. You can use any of them simple by selecting it.*

Deleting an Existing Filter

The Filter drop-down list could become crowded as more and more filters are created. To work efficiently, you want to delete filters that are no longer in use.

To delete a filter:

1. From the AirMagnet *Configuration>Filter* dialog box, click the drop-down list and highlight the filter to be deleted.
2. Click **Del**.
3. Click **OK**.

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 3rd party decodes feature will decode the upper levels of your capture files.

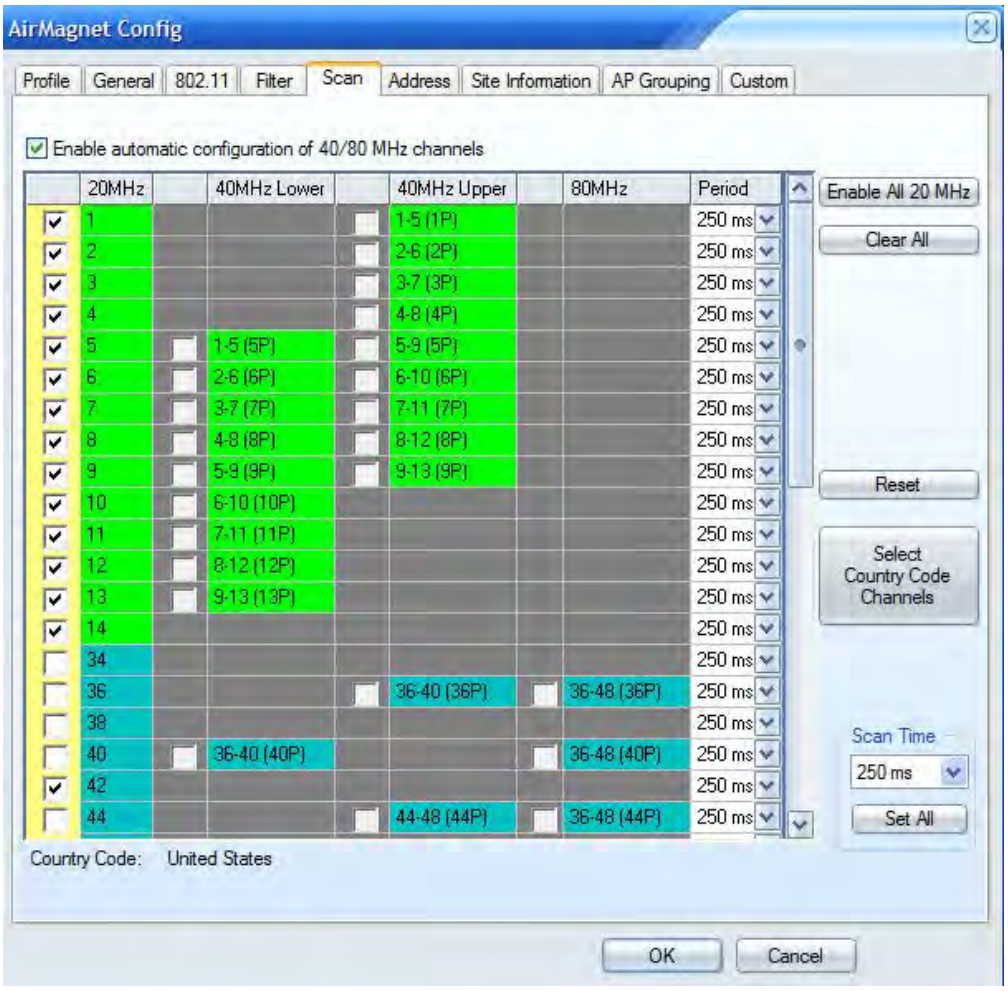
To install the 3rd Party Decodes Engine:

1. Check 3rd Party Decodes Engine. Doing this will begin running its installation.
2. Agree to the GNU license terms. See 3rd Party Decodes License.
3. You may also choose to permit everyone who uses the computer to access this feature.

Configuring Channel Scan

This option allows the user to select the channel or channels that AirMagnet WiFi Analyzer scans and set the frequency at which they are scanned.

Note: *Depending on the Wi-Fi adapter used, options may vary (for example, 802.11n vs. 802.11ac)*



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. The following table summarizes the channel allocation in major parts of the world.

Region/Country	802.11b/g	802.11a/ac
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
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 Configuration dialog box, select the **Scan** tab.

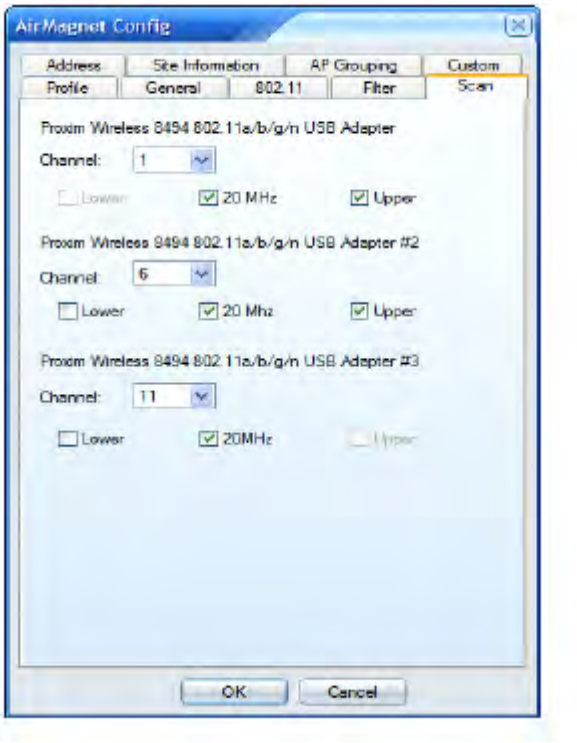
Note: *By default, all 20-MHz channels are selected.*

2. Click **Clear All** to remove the default scan settings and then select only the channel or channels you want scanned.
3. Clicking **Country Code** selects 5 GHz supported channels based on the **Country** setting in the **802.11** tab.
4. Click in the corresponding field in the **Period (ms)** column for each channel and select a frequency for the channel to be scanned from the drop-list.
5. Optionally, click the down arrow below **Scan time** (in the lower right-hand corner of the dialog box), select an option from the drop-down list, and then click **Set All** to change the scan time of all channels to the selected value.
6. If necessary, click **Reset** to restore the default scan settings.
7. Click **OK**.

Note: Enable automatic configuration of 40 MHz channels (802.11n) or 40/80 MHz channels (802.11ac) *is checked by default.*

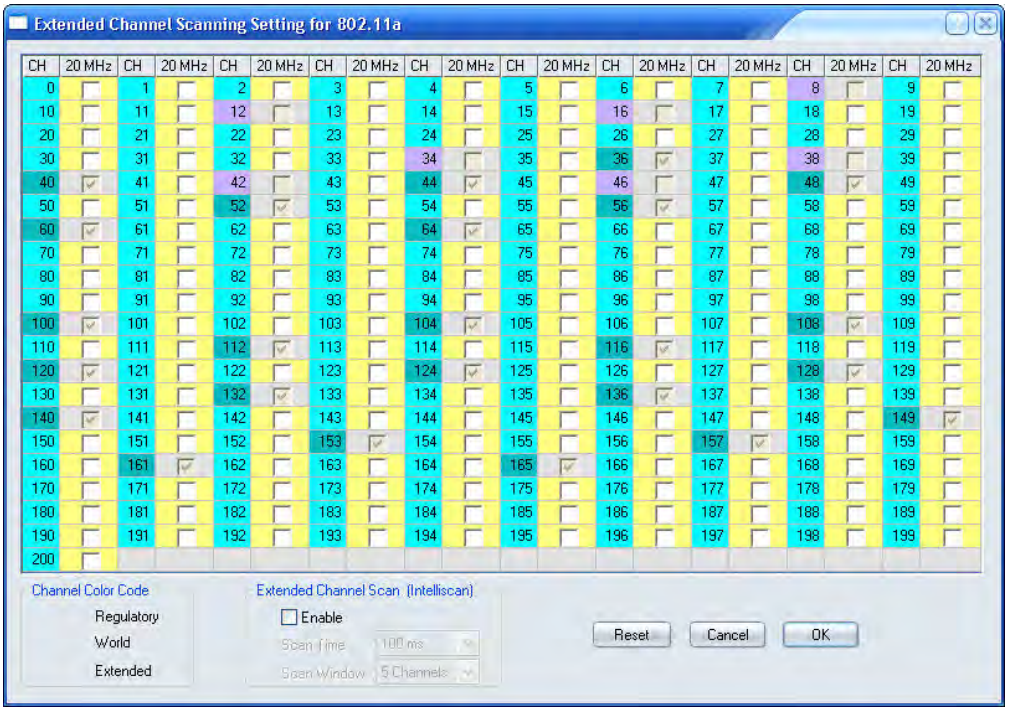
Configuring Channel Scanning for Multiple Adapters

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 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 Wi-Fi Analyzer to scan these channels will help ensure that all the devices in your network are configured properly according to your company’s policies.

You may configure as many channels as you desire for 802.11a scanning. AirMagnet Wi-Fi 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 Wi-Fi Analyzer scans the channels you don’t check as well.

During a normal scan, AirMagnet Wi-Fi 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 Wi-Fi 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.

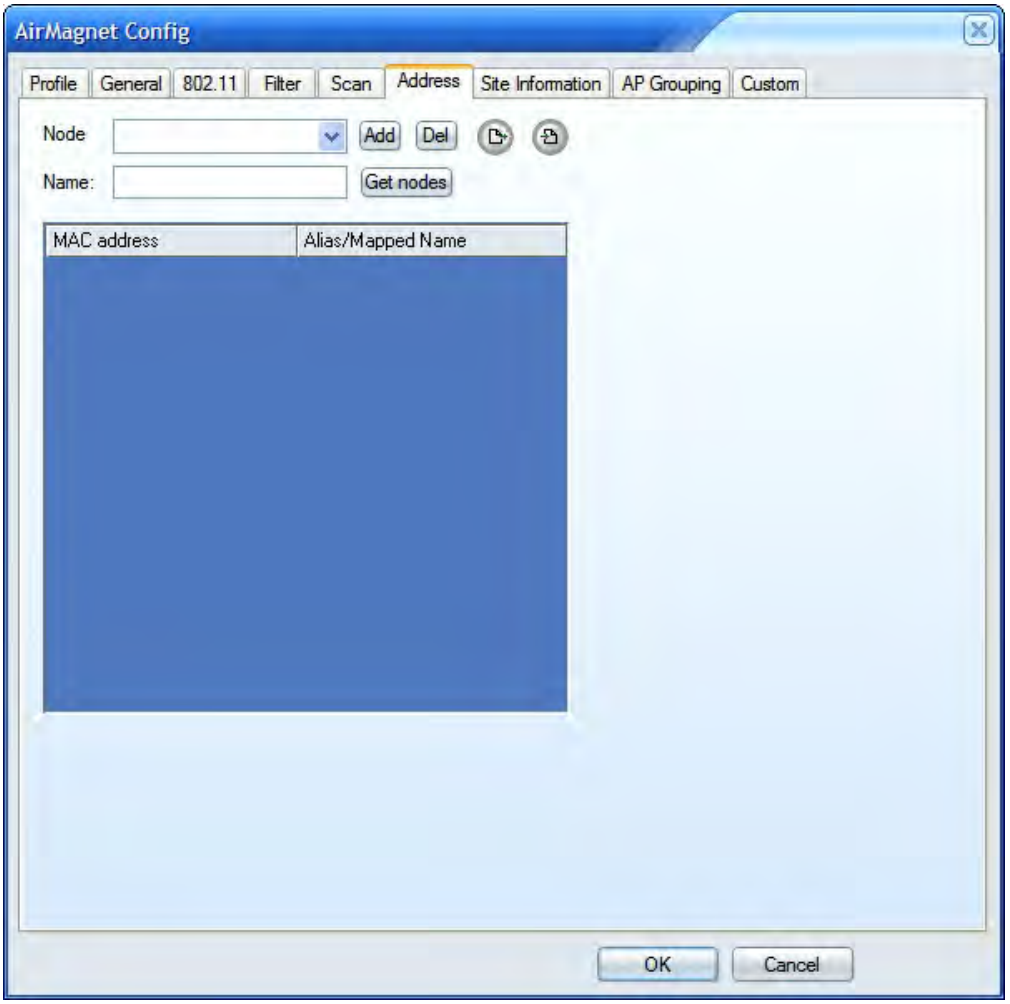
Configuring System Address Book

AirMagnet WiFi Analyzer captures the MAC addresses of all wireless devices it has detected on the network since it was turned on and saves the data 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

Creating an address book involves adding MAC addresses of devices and match each of them with an alias.



To create an address book:

1. From the AirMagnet Configuration dialog box, click the **Address** tab.
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 for the MAC address.
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 book.

Create an Address Book using Get Nodes

Alternatively, you can click the Get nodes button to let AirMagnet WiFi Analyzer automatically populate the address book with all the MAC addresses it has captured since the moment it was turned on. Once the book is populated, you can match the entries with aliases.

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.
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 Entries from an Address Book

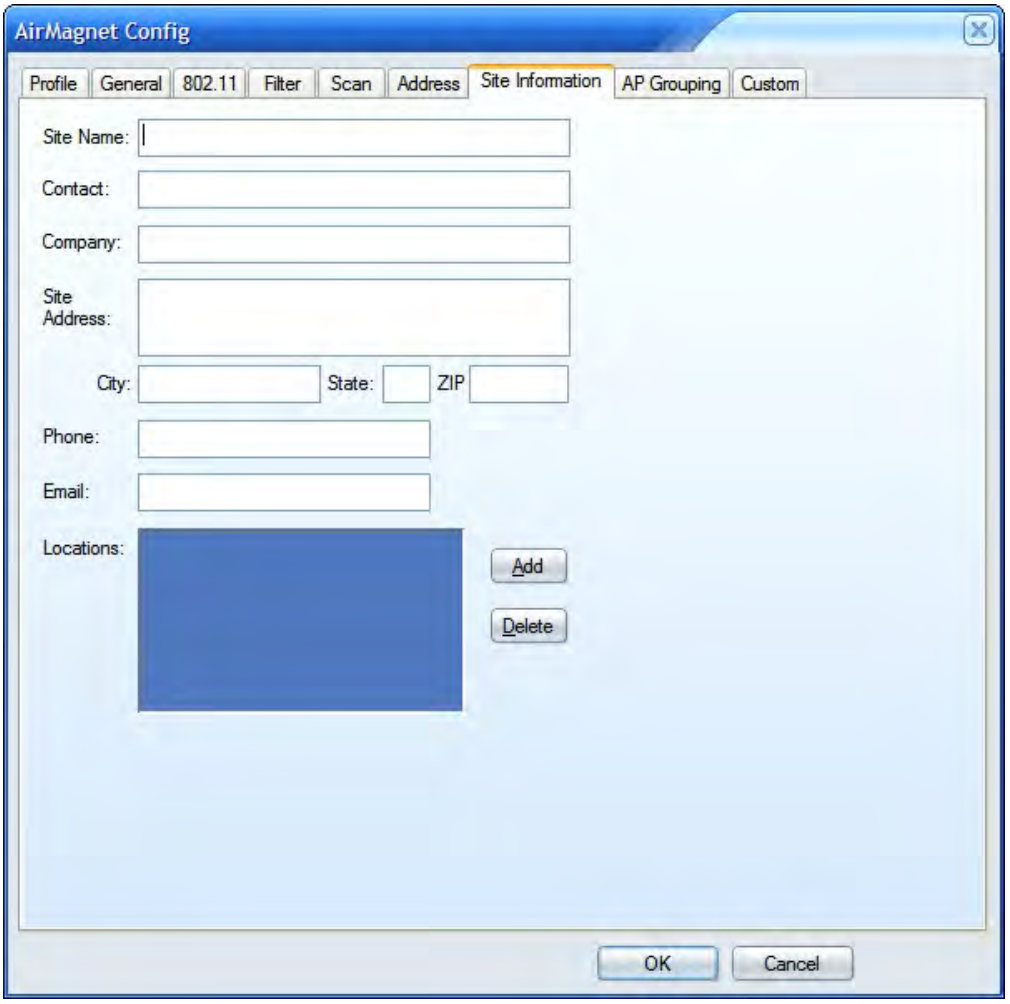
You can delete an entry (that is, a MAC address, or a MAC address—alias pair) from the address book.

To delete an entry from the address book:

1. Highlight the entry you wish to delete.
2. Click **Delete**.
3. Click **OK**.

Specifying Site Information

After all the system parameters have been configured, you may want to add some site-specific information to the profile as well. This is because AirMagnet Wi-Fi Analyzer is a mobile wireless network assurance tool which can be carried to different WLANs or different parts of the same WLAN. Since the network infrastructure differs from site to site or one part of the network to another, it will be very helpful if you can have some site-specific information included in profiles so that you can easily archive your site surveys and/or system profiles.



To add site information to the profile:

1. From the AirMagnet Configuration dialog box, click the **Site Information** tab.
2. Fill out the form by entering the information required.
3. Click **Add.** An entry "Location 1" will appear in the Location field.
4. Click **OK.**

AP Grouping

Configuring AP Grouping

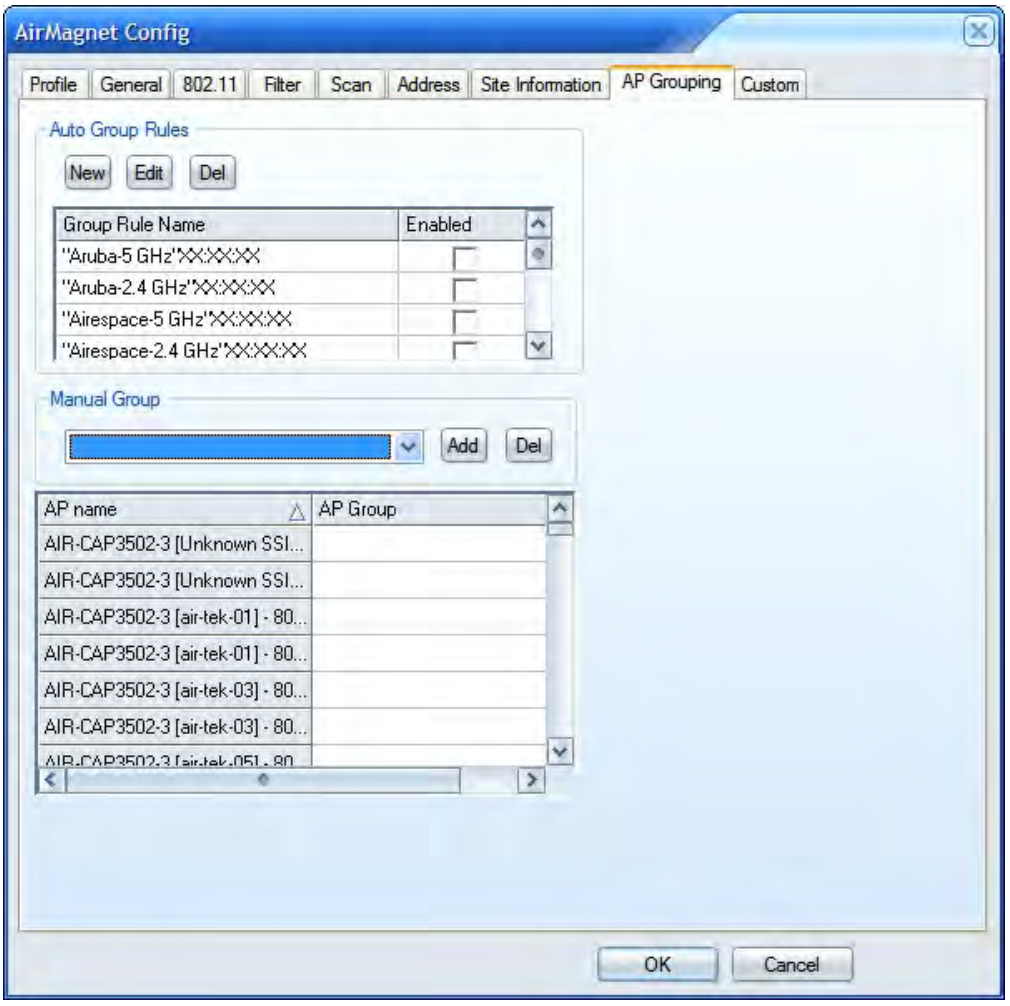
The AP Grouping tab allows you to set up specific names for single devices that utilize multiple VLANs under different SSIDs. This comes into play on many pages, where the separate SSIDs will show up and appear to be several different devices, when in reality they belong to the same single object. The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

You can configure AP grouping by any or all of the following means:

- Using Default Auto AP Grouping Rules
- Grouping APs Using Auto AP Grouping Rules
- Creating AP Groups Manually

Creating Auto APs Grouping Rules

AirMagnet WiFi Analyzer comes with several built-in “automatic” AP-grouping rules. Once enabled, these rules will enable AirMagnet WiFi Analyzer to automatically clump all devices meeting the criteria specified in a specific AP grouping rule under a single AP group. This is especially helpful if your organization uses devices from a specific vendor; AirMagnet WiFi Analyzer will be able to recognize those devices among all devices it has detected and group them accordingly.



To configure AP grouping:

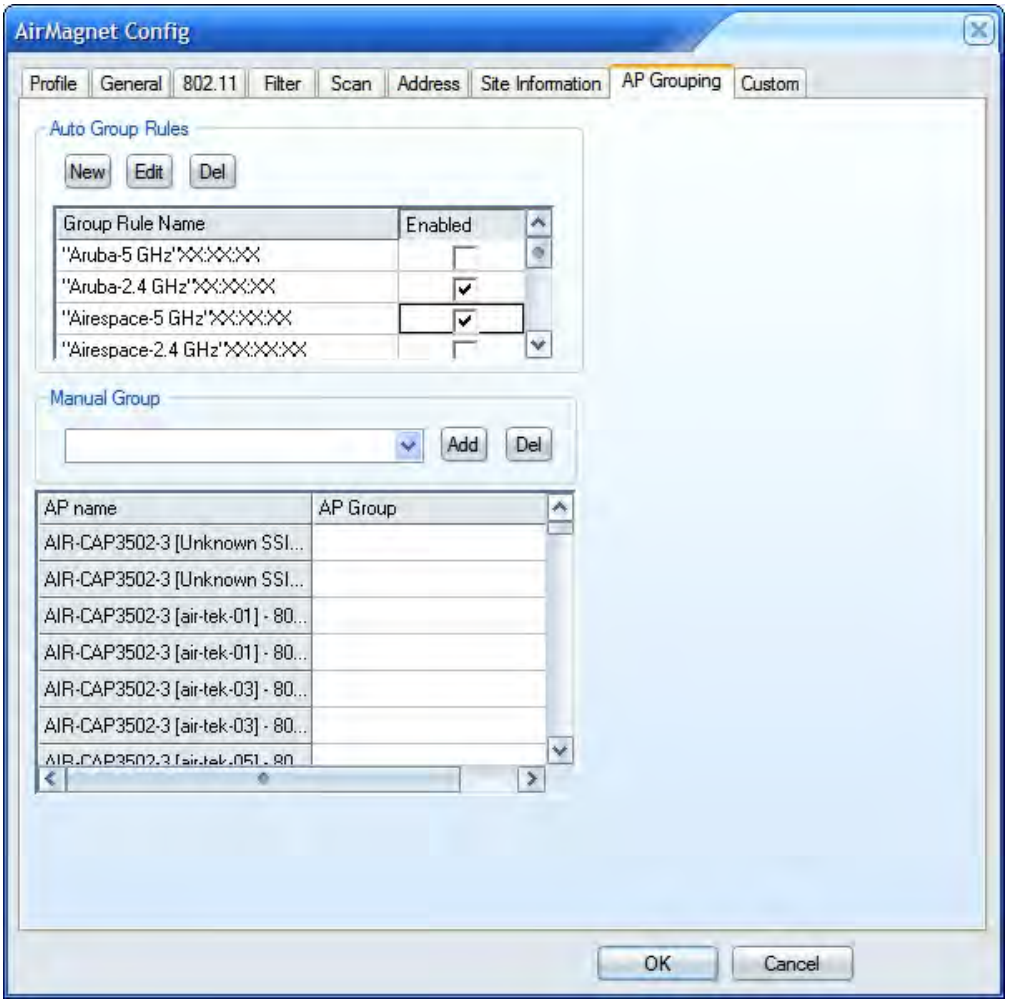
1. From the AirMagnet Configuration dialog box, click the **AP Grouping** tab.
2. Click **New.** The Auto Group AP Rule dialog box appears.
3. Make the entries and/or selections as described in the table below.

4. Click **OK.**

Entry/Selection	Description
Vendor ID	Specify the vendor ID of devices covered by the auto AP grouping rule.
Band	Specify the media type used by the devices.
MAC address last hex-digit starting	Select the last hex digit of MAC addresses you wish the AP auto grouping rule to start from.
Number of contiguous MAC address	Select the number of consecutive MAC addresses you wish to classify in the group.
Ascending	If selected, the rule will count up towards your specified maximum.
Descending	If selected, the rule will count down towards your specified maximum.

Applying Auto AP Grouping Rules

AirMagnet WiFi Analyzer comes with several built-in “automatic” AP-grouping rules to make it easier for the user to take advantage of this powerful management feature. These default auto AP grouping rules, as well as all those custom rules created by the user, are displayed in the Auto Group Rules section of the AP grouping dialog box. Once enabled, these rules will enable AirMagnet WiFi Analyzer to automatically clump all devices meeting the criteria specified in a specific AP grouping rule under a single AP group. This is especially helpful if your organization uses devices from a specific vendor; AirMagnet WiFi Analyzer will recognize those devices and group them accordingly.



To activate auto AP grouping rules

1. From the Auto Group Rules section, select the rule(s) by checking the corresponding check box(es).
2. Click **OK.**

Creating AP Groups Manually

AirMagnet WiFi Analyzer also provides the option for users create AP groups using whatever naming system they like. Once the groups are set up, all you have to do is to manually

assign the APs to the groups, one by one. Not only does it offer you the freedom and flexibility in naming our or AP groups, but also allows you to know exactly what APs you have placed in each of the groups.

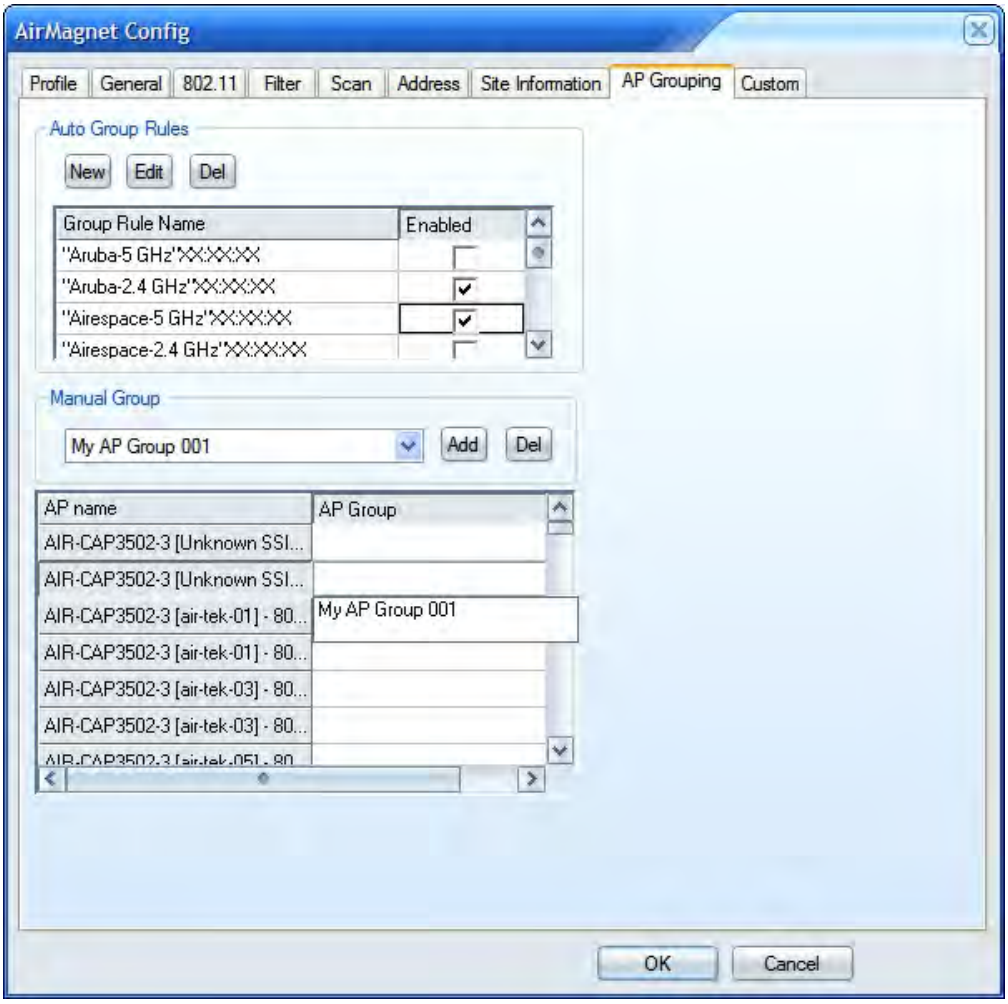
To manually create AP groups:

1. From the Manual Group section of the AP Grouping dialog box, click **Add.** The Manual Group dialog box appears.

2. Enter the name of the AP group to be created and click **OK.**
3. Repeat Steps 1 through 2 to create as many AP groups as needed.

Note: *The names of the AP groups you have created will appear in the AP Group Name of column in the Manual Group section when you click in that column.*

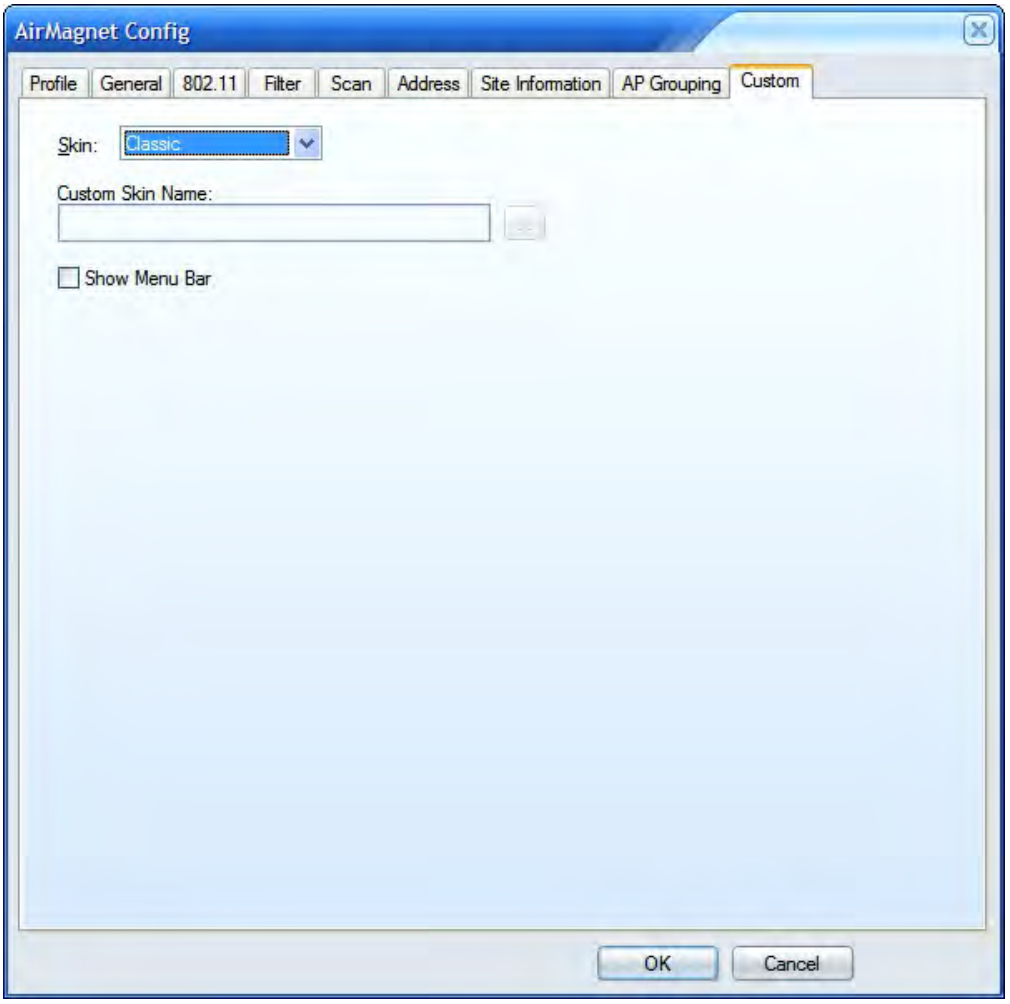
4. Assign APs to the AP groups by clicking in the AP Group column and select the AP group of interest.



5. Repeat Step 4 until all APs are assigned.
6. Click **OK.**

Customizing the User Interface

The Custom tab provides several options for the user to select or change AirMagnet WiFi Analyzer's appearance (color scheme).



To select or change UI skin color:

1. From the AirMagnet Configuration dialog box, click the **Custom** tab.
2. Click **Skin** down arrow and select from the drop-down list menu one of the options.
3. Optionally, check the **Show Menu Bar** check box if you want the menu bar to appear on top of the screen.
4. Click **OK.**

Note: *The aforementioned steps show how to choose or change UI skin color among the default options within AirMagnet WiFi Analyzer. You can also use your own skins as well. All you have to do is to click the square (Browse) button and browse to the location the custom skin file is located. Skins must be in the .msstyle format and can be downloaded from various sources on the Internet.*

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.

Connecting to a Remote System

AirMagnet WiFi Analyzer enables you to connect to remote systems to perform remote troubleshooting.

Note: *Connecting to a remote system is not supported in a Network Address Translation (NAT) environment.*

AirMagnet WiFi Analyzer Remote Operation Mode

You may set a computer running AirMagnet WiFi Pro to Remote Operation Mode. Once a computer is set to this mode, you can enable a remote connection to it from your local computer running AirMagnet WiFi Analyzer Pro. The local computer will switch to the remote adapter for data collection.

First, set the remote computer to Remote Operation Mode:

1. From the **File** menu, select **Operation Mode**.
2. Select **AirMagnet Remote WiFi Analyzer mode**.
3. Set a **Password** you will use later to connect to this remote computer.
4. Determine the IP address of the computer.

On the local computer, connect to the remote computer:

1. From the **File** menu, select **Connect to.**
2. Select AirMagnet Remote WiFi Analyzer
3. **Laptop/PC IP**, type the IP address of the remote computer.
4. **User Name**, type AirMagnetSensor

5. **Password**, type the password created in the **Remote Operation Mode** dialog.

Connecting to an AirMagnet SmartEdge Sensor

You may connect remotely to some models of AirMagnet SmartEdge Sensor.

Note: *This section pertains to setting up and configuring a new AirMagnet SmartEdge Sensor. Attempting to re-configure an existing AirMagnet SmartEdge Sensor is not supported. Contact your AirMagnet sales agent or Technical Support with any questions.*

Sensor Model	Description
AM/A5200	AIRMAGNET SENSOR, A/B/G/N, EXTERNAL ANTENNA
AM/A5205	AIRMAGNET SENSOR, A/B/G/N, INTERNAL ANTENNA
AM/A5220	AIRMAGNET SPECTRUM SENSOR, A/B/G/N, EXTERNAL ANTENNA
AM/A5225	AIRMAGNET SPECTRUM SENSOR, A/B/G/N, INTERNAL ANTENNA

The sensor must be configured for use with AirMagnet WiFi Analyzer Pro.

AirMagnet SmartEdge Sensor Configuration

1. Power on the AirMagnet SmartEdge Sensor (802.3af-compliant PoE adapter or 12v adapter)
2. Connect the Sensor Serial Console Port on the AirMagnet SmartEdge Sensor to the serial port of the computer using the supplied serial cable.
3. You will need to run a terminal emulator. (free or at-cost terminal emulator programs are available on the Web such as "PuTTY" or "SecureCRT")
4. Select the appropriate COM port to which the AirMagnet SmartEdge Sensor is connected. The default is COM1.
5. Make the following entries or selections for the terminal session:

Parameter	Setting
bits per second	115200
data bits	8
parity	no
stop bit	1
flow control	none

6. Continuing the terminal session, at the prompt, press **Enter**.
7. You will be prompted to enter the **Shared Secret Key**. The default key is "airmagnet".

After each of the following configuration settings, you are prompted whether to reboot. Unless directed to do so, choose **no (N)** until configuration settings are completed then reboot.

(For a list of configuration options, type: config>help).

8. Type: config>set enterprise enable

   This command sets the sensor for use with AirMagnet WiFi Analyzer.

9. When prompted to reboot the sensor, choose **yes (Y)**. After the sensor reboots, continue the configuration.
10. Type: config>set sensor

    This command sets a name and "shared secret key" for the SmartEdge Sensor (no spaces allowed in the name).

11. Type: config>set network

    This command sets the IP address parameters (IP address, subnet mask, and the default gateway), for example:

    DHCP Enabled (Y/N)? **Y**
    Obtain DNS server addresses automatically (Y/N)? **Y**
    The system is setting the following configuration:
    DHCP Enabled: Yes
    DNS Servers Addresses:Auto

12. Connect the AirMagnet SmartEdge Sensor to the corporate network using a straight-through RJ-45 Ethernet cable.
13. When prompted to reboot the sensor, choose **yes (Y)**. After the sensor reboots, continue the configuration.
14. Type: config>show sensor

    This command lists the configuration.

15. Type: config>show network

    This command lists the network configuration.

16. Type: config>logout

The sensor is available for use as a remote troubleshooting device.

Sensor Web Page

Sensor configuration information can be viewed and modified by opening the sensor web page.

Note: *The browser must have SSL 3.0 enabled. Before connecting to a sensor's web page, turn off the Computer's firewall or allow TCP port 443 and UDP frames in the firewall configuration.*

1. Open a browser and enter the sensor IP address: for example https://[IP address]
   - **User Name: AirMagnetSensor**
   - **Password:** the **Shared Secret Key**
2. Use the menu navigation tree on the left to explore the available sensor pages.

General Information: The menu options under this category provides status and log information about the sensor.

Diagnostic Information: The menu options under this category provides diagnostic tests and related information for troubleshooting a sensor that is malfunctioning. Contact Technical Support if you believe the sensor may be malfunctioning. See the diagnostic description on the far right of the diagnostic page.

Configuration: The menu options under this category provides sensor configuration options.

Sensor Setup

Parameter	Description
Sensor Name	You may change the default Sensor name “amsensor” to a unique a name in reference to its physical location.
Sensor Shared Secret Key	You may change the Sensor Shared Secret Key.
Log Level	Drop-down menu provides option for log viewing options.
Time Zone	Drop-down menu provides time zone options. Select the region that corresponds to the AirMagnet SmartEdge Sensor location.

Network Setup: Choose either DHCP or Static IP configuration

Parameter	Description
IP Configuration Method	Select Static or DHCP from the drop-down list. Note: If Static is selected, then specify the IP address, subnet mask, and gateway address; if DHCP is selected, the system will get the IP address, subnet mask, and gateway address automatically.
IP Address	Enter the IP address ONLY if Static is selected as the IP Configuration Method. See Above.
Subnet Mask	Enter the subnet mask ONLY if Static is selected as the IP Configuration Method. See Above.
Default Gateway	Enter the gateway IP address ONLY if Static is selected as the IP Configuration Method. See Above.
Domain Name	Enter the domain name of your enterprise network, e.g.,

	mydomain.com
DNS Server Address	Enter the DNS server address ONLY if Obtain DNS server address automatically is NOT checked.
Alternate DNS Address	Enter an alternate DNS server address ONLY if Obtain DNS server address automatically is NOT checked.
Alternate DNS Address (2)	Enter a secondary alternate DNS server address (if needed).
Telnet and SSH Server Options	Select enable if you choose to connect to the sensor using Telnet or SSH.

Factory Default: This command restores the sensor to its factory default setting. The sensor needs to be set to "Enterprise Enable" using the serial console configuration as described under "AirMagnet SmartEdge Sensor Configuration"

Restart Sensor: Use this option to reboot the sensor.

Logout: Sign out of the sensor web page session.

To connect to the AirMagnet SmartEdge Sensor:

Note: *Before connecting to the sensor, turn off computer's firewall or allow TCP port 443 and UDP frames in the firewall configuration. Also, WFA may upgrade the sensor to the current image and reboot the sensor during the remote connection. If this occurs, you will see a dialog box indicating the sensor upgrade process. This upgrade and reboot process may take about 2 mins. to process.*

1. Run AirMagnet WiFi Analyzer Pro
2. From the **File** menu, select **Connect to**
3. Select **AirMagnet Sensor**.

- **Sensor Name/IP:** the IP address of the AirMagnet sensor.
- **User Name: AirMagnetSensor**
- **Password:** the **Shared Secret Key**

Note: *When connected to a sensor, the WiFi Analyzer configuration will be used by the remote sensor.*

To Disconnect from the AirMagnet SmartEdge Sensor:

From the **File** menu, select **Disconnect**.

The following table lists features not available when connected to a remote sensor:

Item	Description
Wi-Fi Tools	All except the following tools are disabled: Diagnostic and 802.11n Tools
File>Configure	Scan tab: Country Code Channel is hidden 802.11 tab is disabled Profile tab is disabled
Live capture	Capture to disk is disabled
Roaming Analysis	Disabled
Compliance Reports	Disabled

Sensor Reset Button

Caution: There is a manual reset button located on the AirMagnet SmartEdge Sensor. Before using this button to reset the sensor, contact technical support for further instructions.

Managing Network Policies

About Network Policies

This section explains how to configure and manage wireless network security and performance policies. From the information 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.

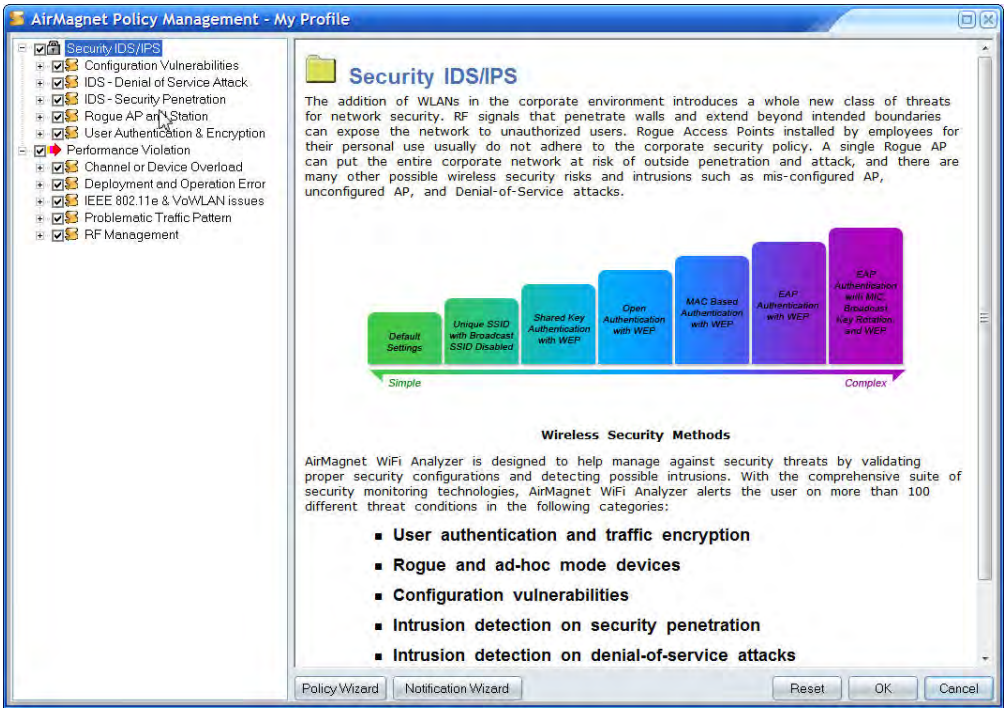
The security and performance alarms generated by the AirMagnet AirWISE expert engine have proved powerful in WLAN network management, especially for managing large-scale enterprise WLAN networks. AirMagnet uses a three-level policy structure that greatly facilitates WLAN event management and analysis. 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.

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.



As shown above, 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.

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.

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

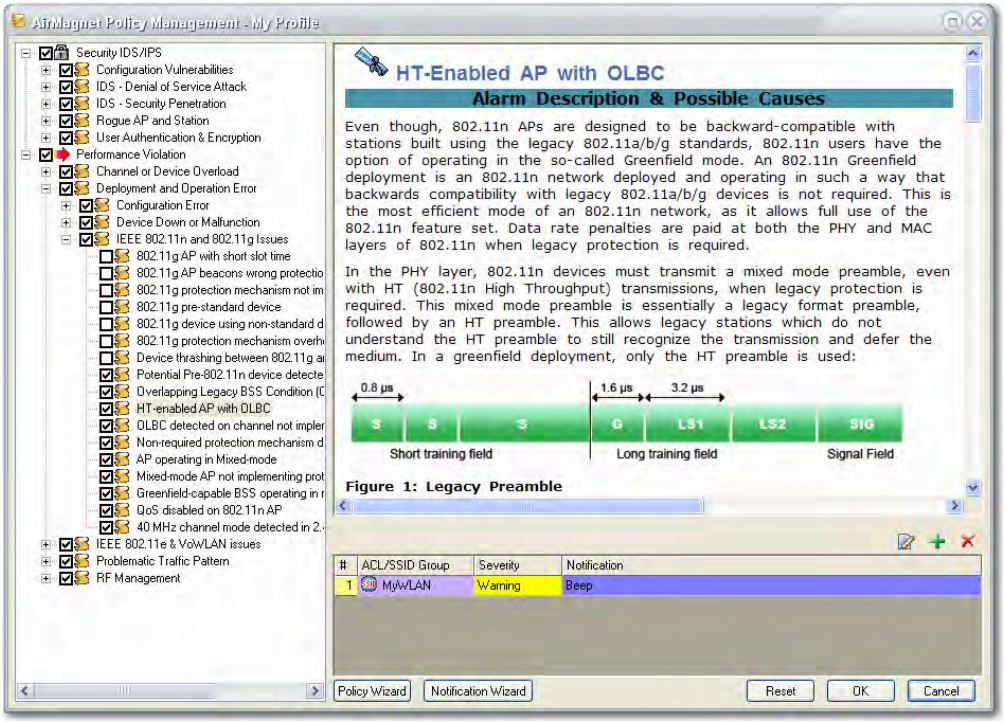
adding, changing, and/or deleting policy rules that contain alarms, notifications, and a number of other parameters.

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 Analyze's policy management procedures, these default policies come handy and offer some basic protection for the wireless network. However, to take full advantage of 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 explains the procedures involved in creating a policy rule.

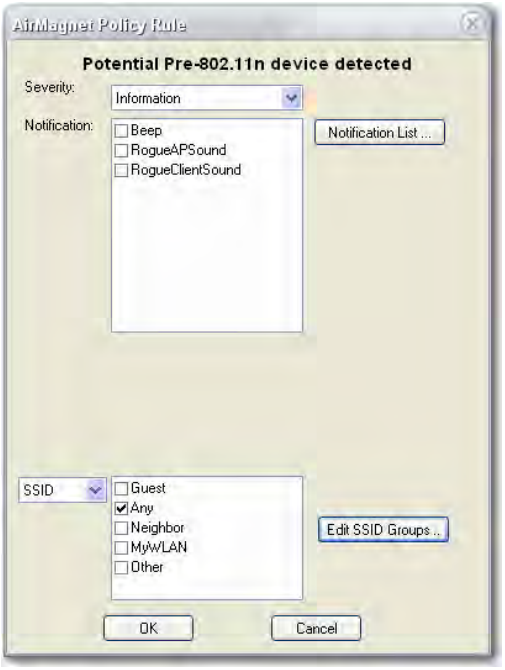
To create a new policy rule:

1. From the AirMagnet Policy Management screen, expand the Policy Tree and select a policy alarm of interest. The AirMagnet Policy Management screen refreshes.



Note: *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)** located in the lower right corner above the table**.** The AirMagnet Policy Rule dialog box appears.



3. From the AirMagnet Policy Rule dialog box, make the required entries and/or selection.
4. Click **OK** when completed.

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). ***Note:*** *If you need to add more notification options to the alarm, click* ***Notification List....*** *This opens the AirMagnet Policy Notification List dialog box where you can configure more notification options and add them to the list of available notifications. Refer to* *Assigning Notifications to Policy Alarms* *for details on how to configure and add notification options.*
ACL/SSID	Click the down arrow and select ACL or SSID.

	Note: • If you choose to use ACL, make sure that you have an ACL already configured. • If you choose to use SSID, select the SSID(s) from the list on the right. • You can 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.

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, select a policy rule of interest and click  **(Edit Policy Rule).** The AirMagnet Policy Rule dialog box appears.
2. Make the desired changes in the AirMagnet Policy Rule dialog box.
3. Click **OK** when completed.

Deleting Existing Policy Rules

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, highlight the policy rule of interest.
2. Click  (Delete Policy Rule).
3. A confirmation message will appear. Click **Yes**.

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, 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.
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.

Note: *By default, 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. However, you can configure the other advanced notification options that 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.*

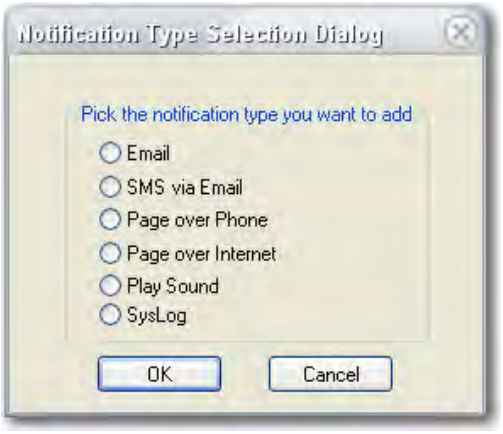
3. I you want to assign any of the available and applicable notification options to the alarm, check the corresponding check box(es) and click **OK**.

Note: *Once you click **OK**, the AirMagnet Policy Rule dialog box closes and the notification option(s) you have selected are added to the Notification field of the policy table on the AirMagnet Policy Management screen.*

4. If you want to configure and use some other notification options, then click **Notification List...** button. The AirMagnet Policy Notification List appears.

Note: *The AirMagnet Policy Notification List dialog box is where you 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.*

5. Click  **(Add New Notification).** The Notification Type Selection dialog box appears.



Note: *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. Refer to the table below for a summary of each option.*

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, and so on) 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.
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.
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 can 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 Rule**. The AirMagnet Policy Rule dialog box appears.
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.**

Note: *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 the **Notification List...** button. The AirMagnet Policy Notification List dialog box appears.
4. Highlight the notification option and click  **(Edit Notification).** The configuration dialog box for the notification option appears.

Note: *Since you are modifying the settings of an existing notification option, the name of the notification is grayed out. This means that the name of the name of the notification cannot be changed.*

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

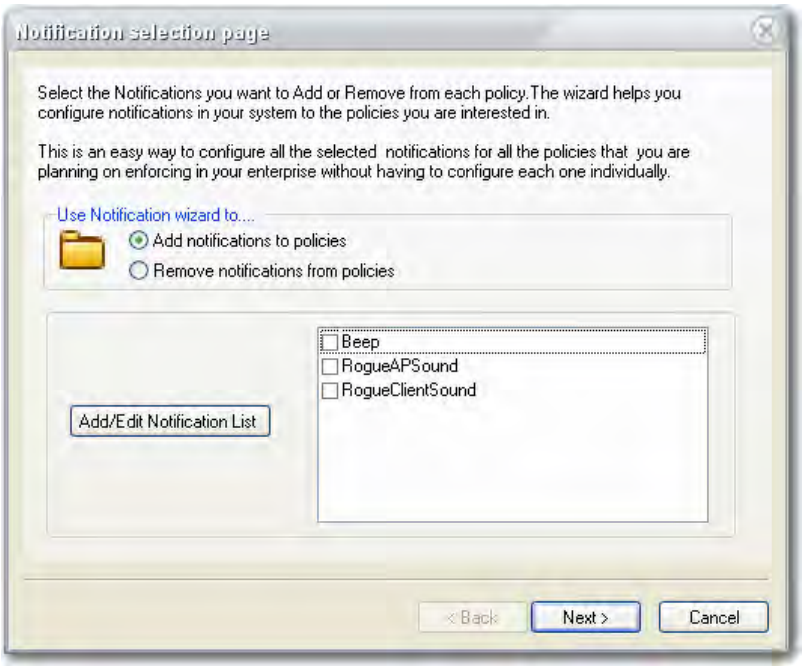
The AirMagnet Policy Rule dialog box contains all the notification options that have been configured. While you can assign or remove any of them to or from an alarm from the AirMagnet Policy Rule dialog box, you must delete the notification from the AirMagnet Policy Notification List dialog box if you 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.
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.

Note: *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 WiFi Analyzer.*

Assigning Notifications to Policy Alarms



To assign a notification to policies or alarms:

1. From the AirMagnet Policy Management screen, click the **Notification Wizard** button. The Notification Selection Page appears.
2. Check the **Add Notifications to Policies** radio button.
3. Select the notification(s) and click **Next**. The Policy Selection Page appears.

4. Select the policies and alarms to which you want the notification(s) to be applied.
5. Select a level of severity at which the notification is to be generated, and click **Next.** The Confirmation Page appears.
6. Click **Finish**. The selected notifications will be assigned to the policies and alarms.

By default, each alarm contains only one notification. For most alarms, the default notification is a beep, but for Rogue APs and clients, the default notification is a sound. You can add, change, or delete notifications as needed.

Assigning Policies to ACL or SSID Groups

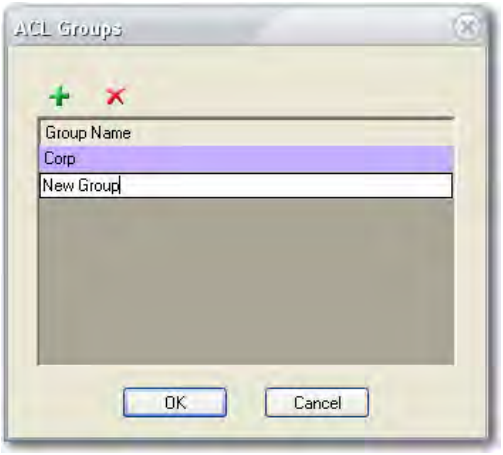
As mentioned previously, ACL and SSID groups are also an important part of AirMagnet network policy profiles and play a vital role in network security and performance management. Each ACL or SSID group contains information of specific wireless devices. When policies are assigned to ACL or SSID groups in a policy rule, it tells the program that only the devices that belong to the ACL or SSID groups are legitimate and that any device outside the designated ACL or SSID groups will be treated as rogue, 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:

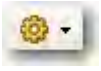


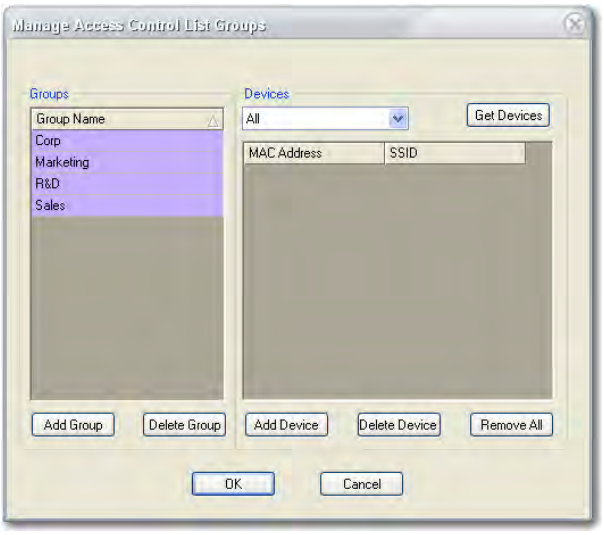
1. From the AirMagnet Policy Rule dialog box, click **Edit ACL Groups....** The ACL Groups dialog box appears.
2. From the ACL Groups dialog box, click  **(Add New ACL Group).** A new entry “New Group” appears in the table.
3. Highlight the entry and type a unique name over it, and click **OK.** The 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.

Note: *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:

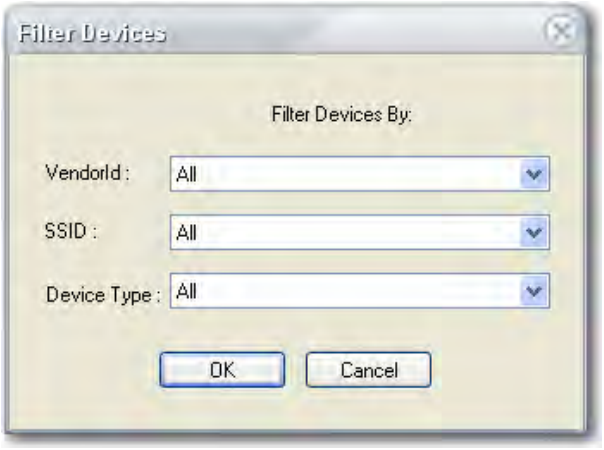
1. From the Start page, click  . The AirMagnet Config dialog box appears.
2. Click **Manage ACL Groups....** The Manage Access Control List dialog box appears.



Note: *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. Refer to the table below for descriptions of the buttons in the Manage Access Control List dialog.*

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 brings up the Filter Devices dialog and allows you to scan for the devices to add to the selected group.
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 deletes the selected ACL group.
Add Device	This button allows you to manually add a device by entering its MAC Address.
Delete Device	This button deletse 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 “QA”).
4. Click **Remove All** to clear the devices off the table.
5. Click **Get Devices**. The Filter Devices dialog box appears.



6. 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 the table below for a description of the 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 allows you to add only devices that use a specific SSID.
Device Type	This field lets you specify the device type you are interested in adding (AP, STA, or Ad-Hoc).

7. Click **OK** to close the Manage Access Control List Groups dialog box.
8. Click **OK** to close the AirMagnet Config dialog box. The “QA” 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.

To assign a policy to an existing SSID group:

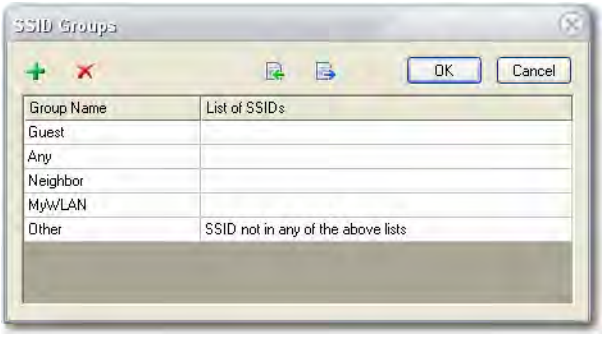
1. From the AirMagnet Policy Management screen, select a policy and click **Add Policy Rule**. The AirMagnet Policy Rule dialog box appears.
2. Select the SSID group(s) by checking the corresponding check box(es).
3. Click **OK.**

Modifying Existing SSID Groups

The existing SSID groups are useful 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, click **Edit SSID Groups...**. The SSID Groups dialog box appears.



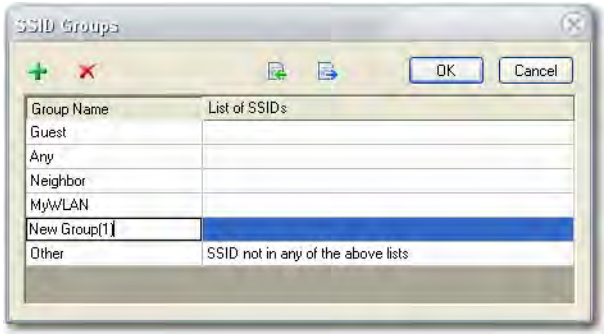
2. Click to highlight the name of the SSID group and type a unique name over it (if you want to rename it). Note that you may not rename the pre-generated groups.
3. Click to highlight the corresponding SSID List field and enter the SSIDs to be included in the SSID group. Entries are case-sensitive, and must be separated by commas (sample entry: SSID1, SSID2, and so on).
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 you to create SSID groups from scratch, if you choose to do so.

To create a new SSID group:

1. From the SSID Groups dialog box, click **(New SSID Group)**. A new entry marked “New Group” appears in the dialog box.



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, highlight the SSID.
2. Click **(Delete Selected SSID Group).**
3. Click **OK.**

Deleting Existing Notifications

To delete an existing notification:

1. From the *AirMagnet Policy Notification List* screen, highlight the entry.
2. Click **Delete Notification.** The *Confirmation* screen appears.
3. Click **Yes.**

Working with Policy Wizard

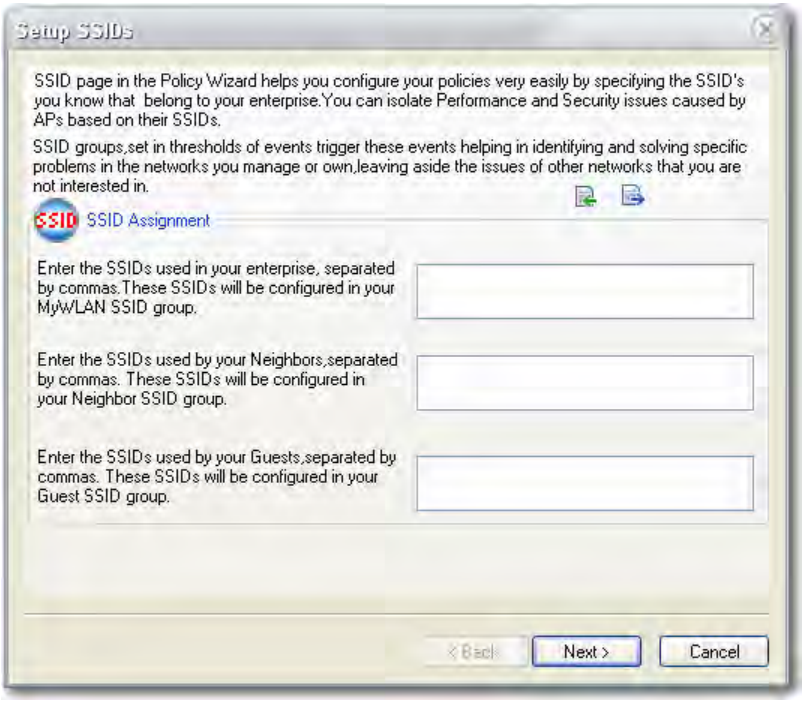
The Policy Wizard provides an easy way for novice users to configure WLAN security and performance policies. It allows you to configure your WLAN policies based on your

knowledge of your 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 Policy Wizard

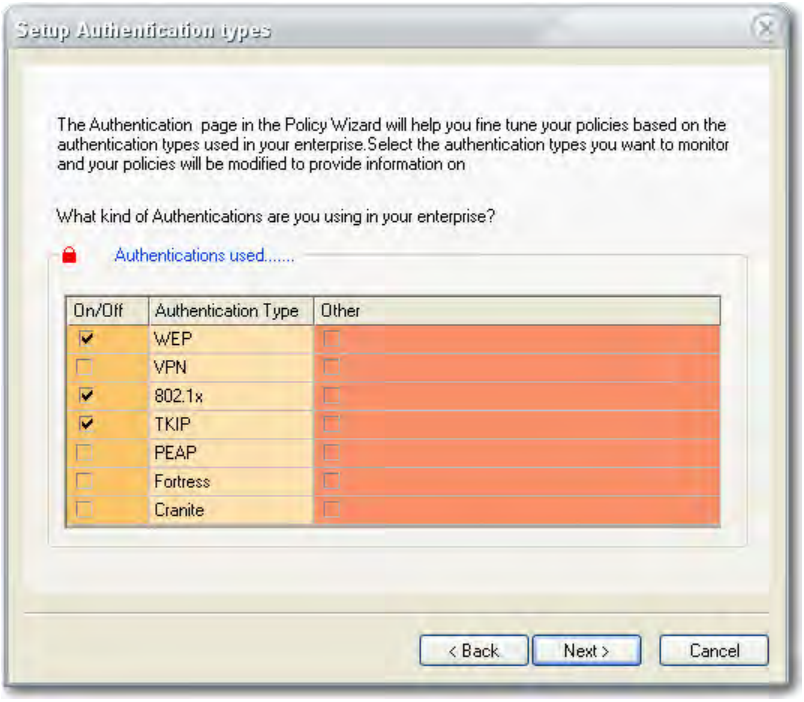
The Policy Wizard walks you through the process using just a few easy-to-follow screens which cover the following areas:

- **Setting up SSID Groups** - This option asks for the WLAN SSIDs used by your enterprise, your neighboring businesses, and your guests.
- **Setting up Authentication** - It allows you to configure policies based on the types of authentication used in your enterprise, your neighboring businesses, and your guests. In this case, the system will automatically notify you when the selected types of authentication 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.

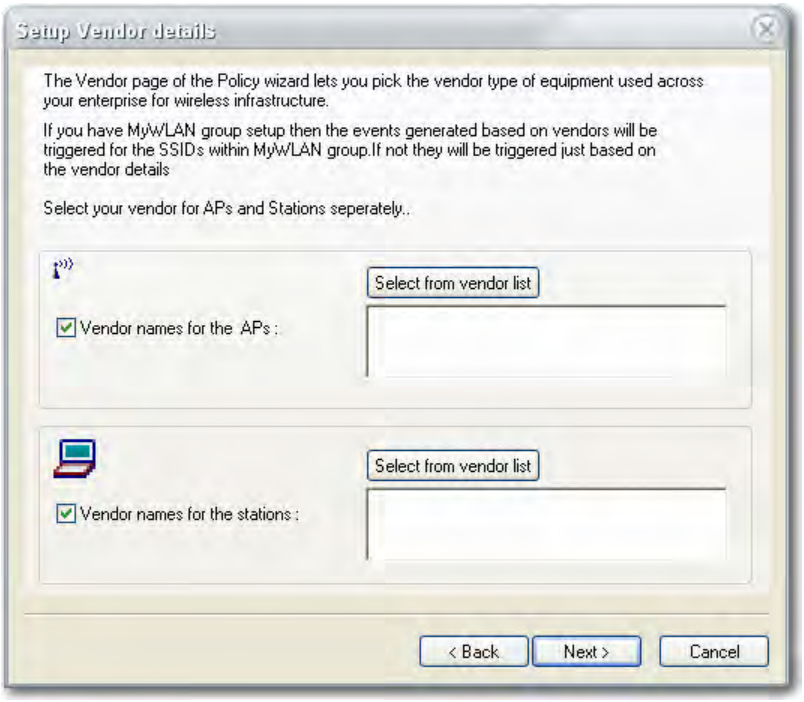


To configure policies using the Policy Wizard:

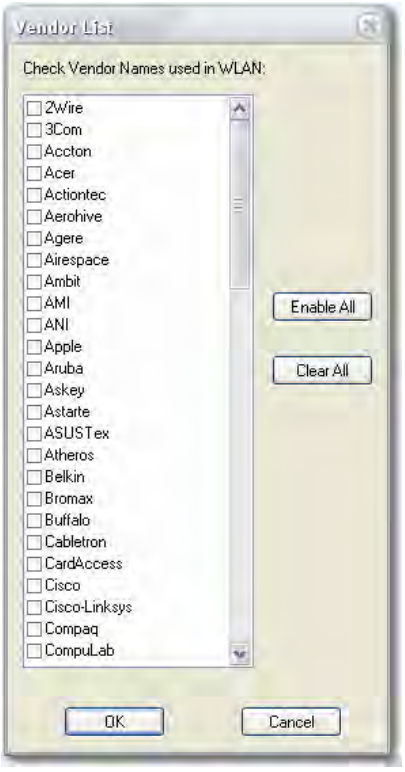
1. From the AirMagnet Policy Management screen, click the **Policy Wizard** button. The Setup SSIDs screen appears.
2. Enter the SSIDs used by your enterprise, neighbors and guests, and click **Next.** The Setup Authentication Types screen appears.



3. Select the type(s) of authentication for your network, and your neighbor, guest and other networks; and click **Next.** The Setup Vendor List screen appears.



4. Check the **Vendor Names for the APs** check box, and click the **Select from Vendor List** button. The Vendor List screen appears.



5. Select the vendors whose APs are used on your enterprise network, and click **OK.** The names of the selected vendors will appear in the AP section.
6. Repeat Steps 4 through 5 to configure the **Vendor List of Stations**.
7. Then click **Next.** The Confirmation screen appears.
8. Click **Finish**.

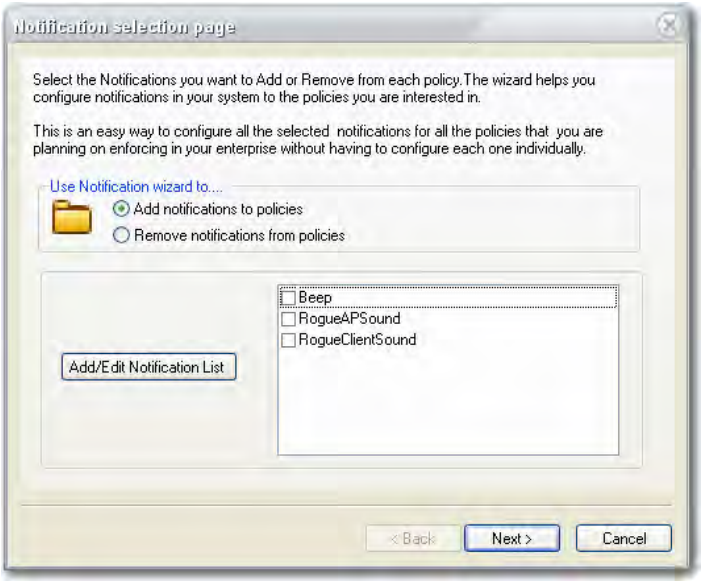
Working with Notification Wizard

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.

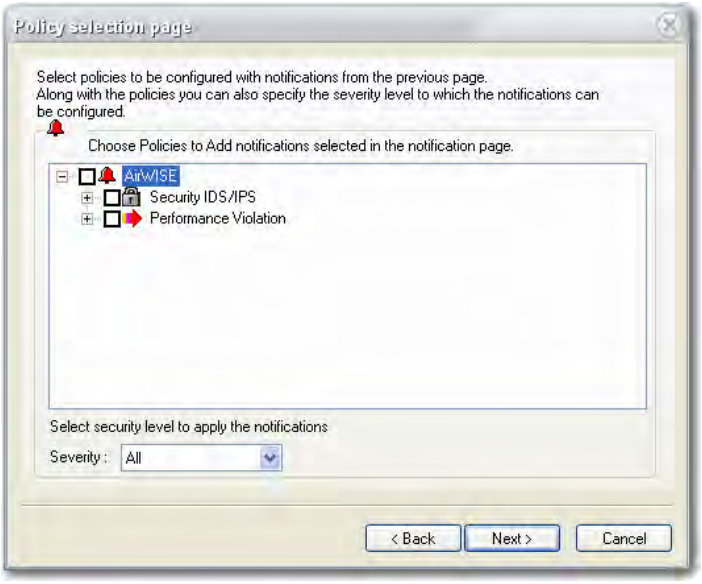
Assigning Notifications to Policy Alarms

To assign a notification to policies or alarms:

1. From the AirMagnet Policy Management screen, click the **Notification Wizard** button. The Notification Selection Page appears.



2. Check the **Add Notifications to Policies** radio button.
3. Select the notification(s) and click **Next**. The Policy Selection Page appears.



4. Select the policies and alarms to which you want the notification(s) to be applied.

5. Select a level of severity at which the notification is to be generated, and click **Next.** The Confirmation Page appears.

6. Click **Finish**. The selected notifications will be assigned to the policies and alarms.

By default, each alarm contains only one notification. For most alarms, the default notification is a beep, but for Rogue APs and clients, the default notification is a sound. You 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

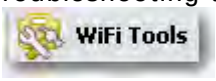
The following steps are suggested to illustrate how to expand the policy structure in the AirMagnet Policy Management screen:

1. Choose a policy group, for example, Security.
2. Select policy category in that policy group, for example, User Authentication and Encryption.
3. Select a subcategory of the selected policy category, for example, WPA-802.1x &TKIP.
4. Highlight a specific alarm under the policy subcategory, for example, 802.1x Rekey Timeout Too Long.

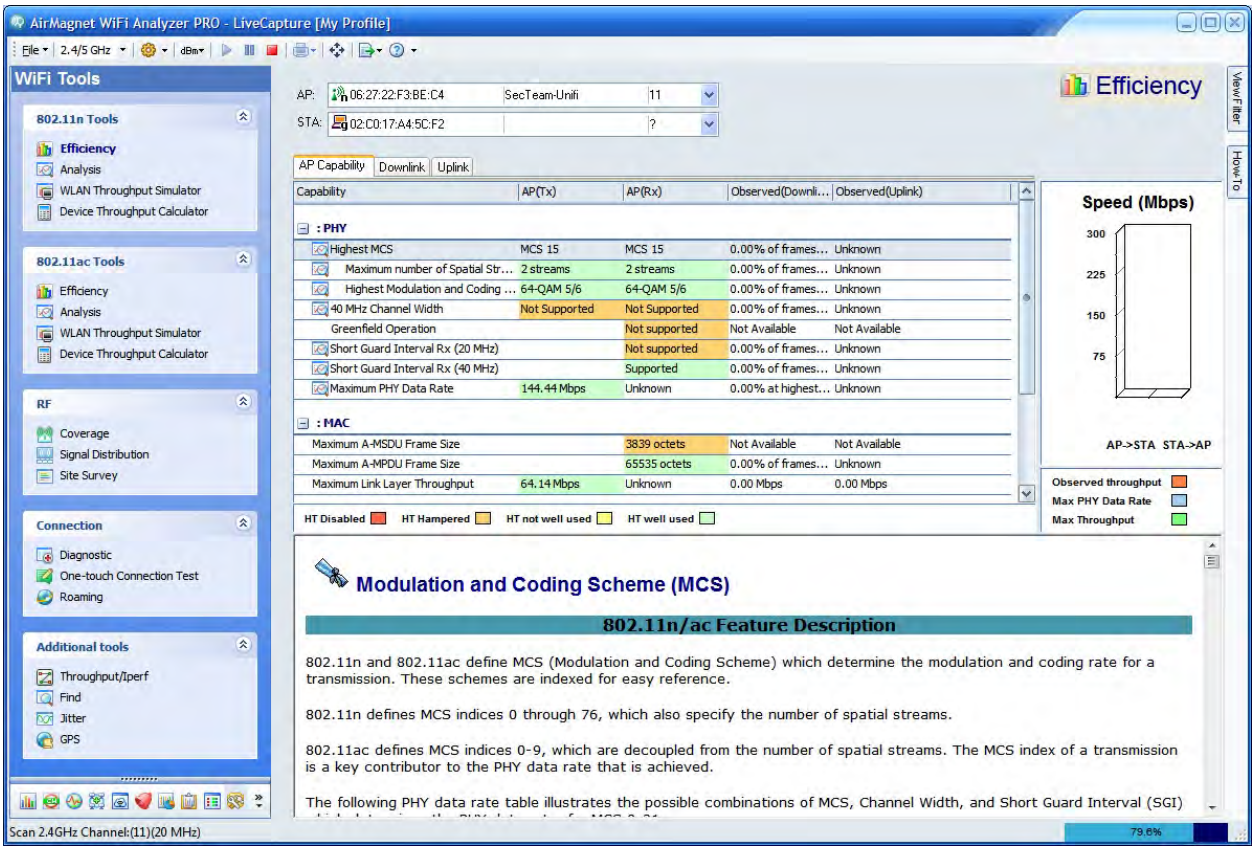
For detailed descriptions of AirMagnet WLAN policies, refer to the AirMagnet Wireless LAN Policy Reference Guide which is included on the software CD.

WiFi Tools Screen

About Wi-Fi Tools Screen

The WiFi Tools screen contains the tools for troubleshooting the 802.11 network. You can navigate to the WiFi Tools screen by clicking 

. The figure shows the WiFi Tools screen.



As shown on the screen, AirMagnet WiFi Analyzer offers the following tools:

- Measuring 802.11n and 802.11ac network efficiency
- Analyzing 802.11n and 802.11ac network issues (analysis)
- Simulating WLAN throughout for both 802.11n and 802.11ac
- Calculating device throughput for both 802.11n and 802.11ac
- Measuring WLAN or cell coverage
- Testing site RF signal distribution
- Conducting a site survey
- Performing WLAN diagnostics
- 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

80211n/ac Tools

About 802.11n/ac Tools

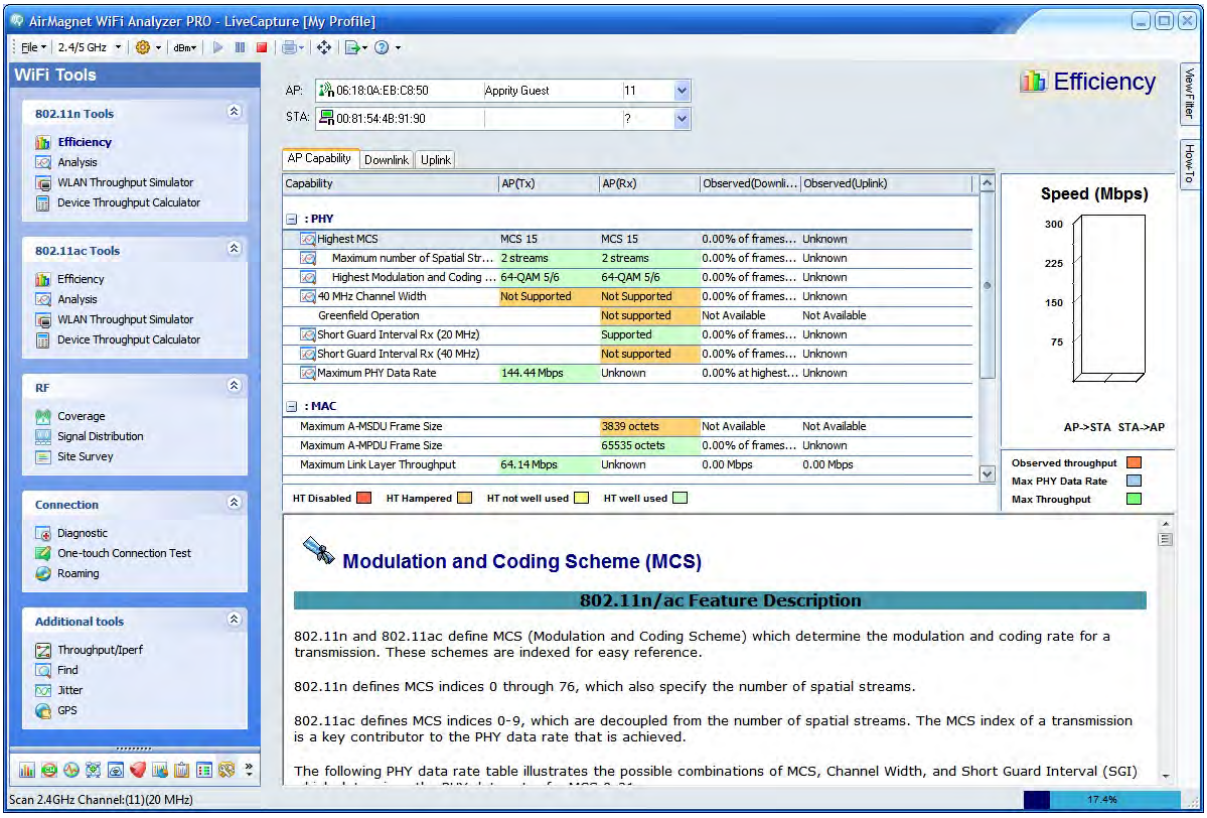
AirMagnet WiFi Analyzer comes with 802.11n/ac tools that allow you to analyze the performance of the 802.11n/ac wireless network – the next generation of wireless networking technology that offers unprecedented network throughput, range, and stability. The tools are focused on helping you understand and troubleshoot the most common 802.11n/ac-related issues you may encounter.

AirMagnet WiFi Analyzer provides the following 802.11n/ac-related tools:

- Efficiency
- Analysis
- WLAN Throughput Simulator
- Device Throughput Calculator

802.11n/ac Efficiency

The 802.11n and 802.11ac wireless network protocols 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 you need in order to take full advantage of the benefits of the 802.11n and 802.11ac network.



When you select Efficiency, the WiFi Tools screen displays all issues grouped in the categories listed below.

- **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 the network's backward compatibility with legacy 802.11 networks (that is, 802.11a/b/g).

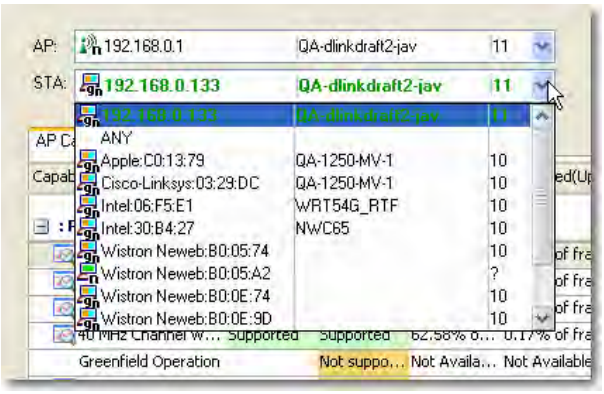
Note: *Double-clicking an entry refreshes the screen to the Analysis screen which shows detailed analysis of that entry (if applicable). Refer to Analyzing 802.11n/ac Network Efficiency.*

Analyzing 802.11n/ac Network Efficiency

The Efficiency tool allows you to see the network efficiency between any (chosen) pair of AP and STA, or AP alone.

To analyze the network efficiency between an AP and a STA:

1. From the Efficiency screen, select an AP and a STA.



Note: *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.*

2. 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 the table below.

Entry	Description
Tabs	Click any of the following tabs to view the pertinent data in the table.
▪ AP Capability ▪ Downlink ▪ Uplink	Displays data about the selected AP only. Displays data about the link from the selected AP to the selected STA. Displays data about the link from the selected STA to the selected AP.
Table Fields	
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 (that is, from the AP to the STA).
Observed (Uplink)	The level or state of a certain capability as observed from the uplink (that is, from the STA to the AP).
Color Legends	
HT or VHT Disabled	For the AP (Tx) and AP (Rx) columns, red color means the HT or VHT is disabled or not used.
HT or VHT Hampered	For the AP (Tx) and AP (Rx) columns, orange color means the HT or VHT is impaired.
HT or VHT not well used	For the AP (Tx) and AP (Rx) columns, yellow color means the HT or VHT is used for only 50~75%.
HT or VHT well used	For the AP (Tx) and AP (Rx) columns, red color means the HT or VHT is used almost to its full potential.

3. 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 the table below.

Data	Description
Left Bar Chart	Downlink (AP->STA) data rate.
Right Bar Chart	Uplink (STA->AP) data rate.
Bar Chart Color Legend	
▪ Light green	Maximum Throughput

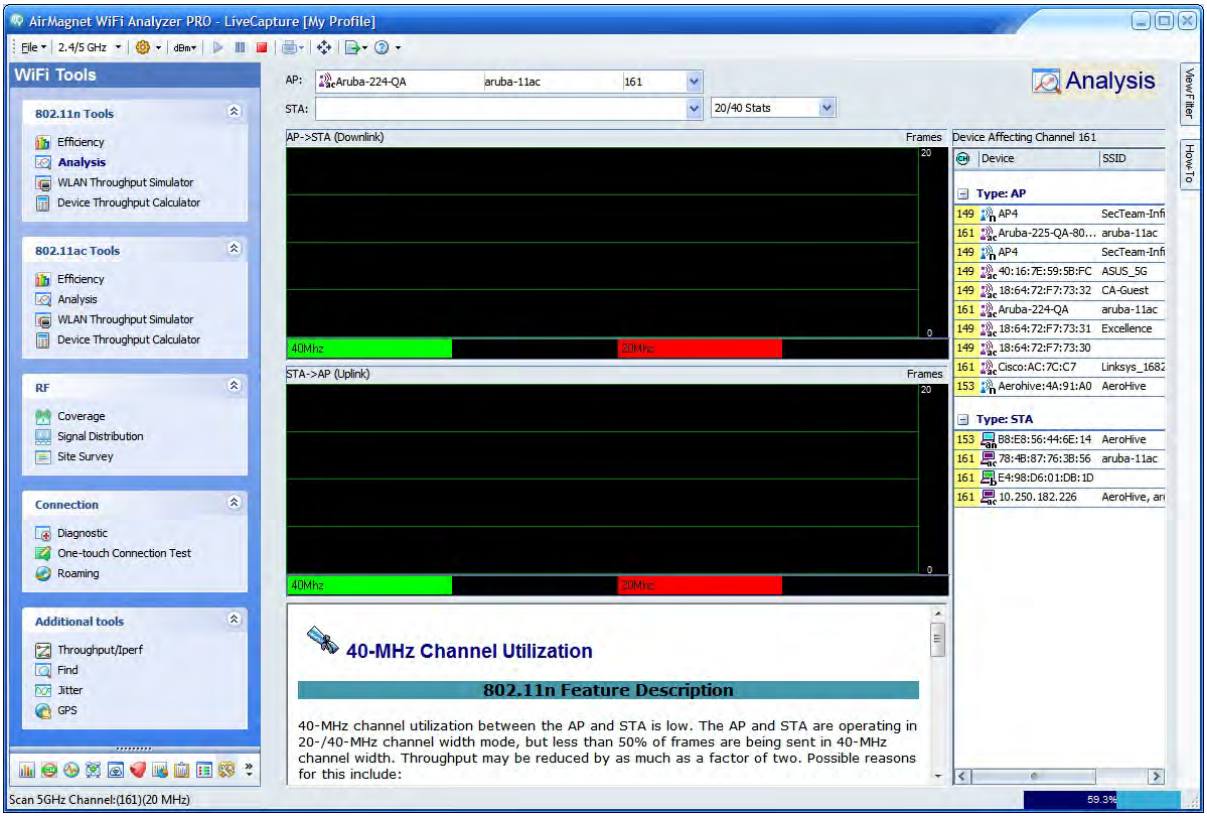
▪ Light blue	Maximum PHY Data Rate
▪ Brown	Observed Throughput

The Observed (Downlink) and Observed (Uplink) columns 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 (that is, 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 (that is, 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 (that is, 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 802.111n specification.

802.11n/ac Analysis

The Analysis screen provides detailed analysis (explanation) about a number of 802.11n or 802.11ac related issues. You can navigate to the Analysis tool screen by clicking Analysis under 802.11n Tools or 802.11ac Tools. The figure below illustrates the 802.11n Tools/Analysis screen.

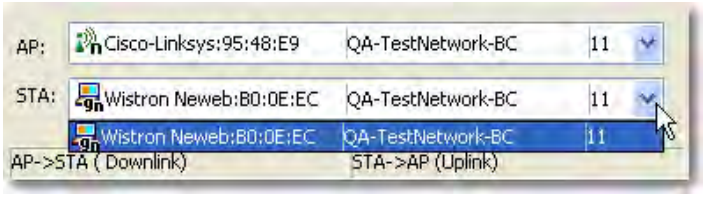


Analyzing 802.11n and 802.11ac Network Data

The Analysis tool allows you to see the following 802.11n and 802.11ac network data between any (chosen) pair of AP and STA, or AP alone:

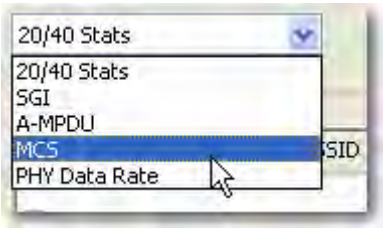
- 20/40/80 MHz Statistics
- Short Guard Interval (SGI)
- A-MPDU
- MCS
- PHY Data Rate

To analyze the network transaction between an AP and a STA:



1. From the WiFi Tools view, click **Analysis** in the 802.11n or 802.11ac Tools section
2. Select a AP and station.

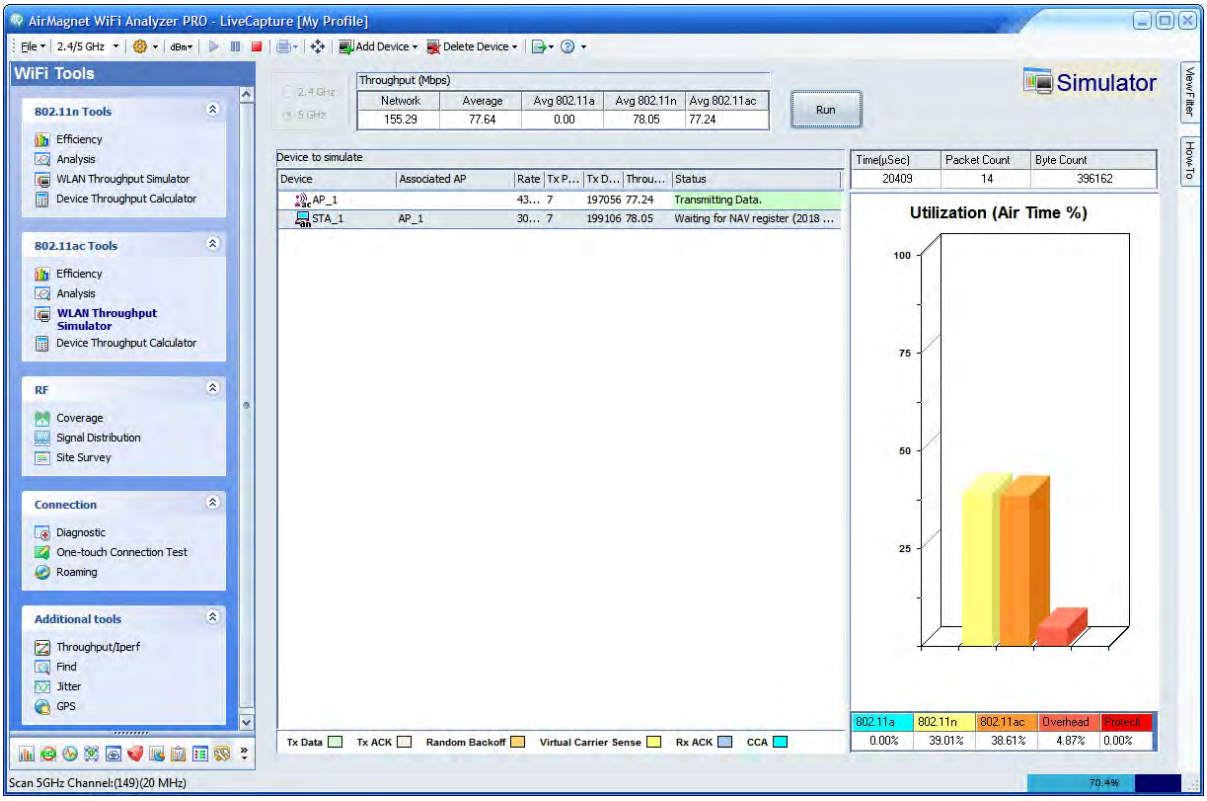
3. Select a data type of interest.



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.

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 you to add and configure up to fifty 802.11a, 802.11b, 802.11g 802.11n and/or 802.11ac 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.

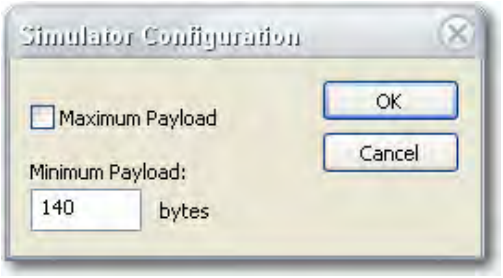


Configuring WLAN Throughput Simulator

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.



2. Check the `Maximum Payload` check box or specify a minimum packet size.
3. Click **OK**.

Note: *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. The 802.11ac Max payload is 1MB.*

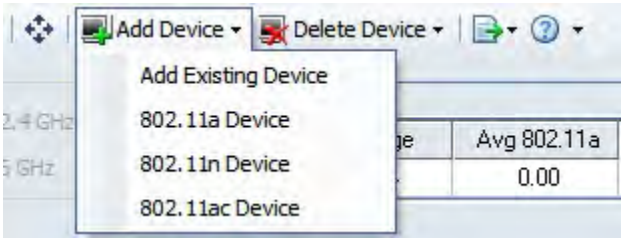
Simulating WLAN Throughput

The WLAN Throughput Simulator allows you 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 use the WLAN Throughput Simulator:

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 menu bar, click 

and select an option from the drop-down menu.

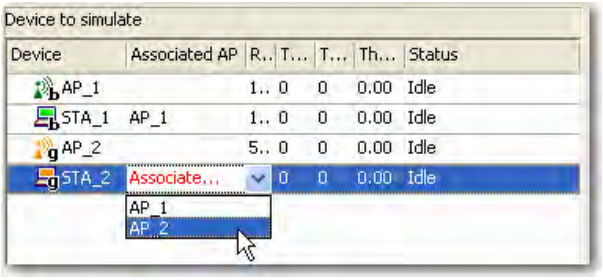


The table below explains all options in the Add Device drop-down menu.

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.
802.11ac Device	Adds 802.11ac APs and/or STAs. This option is only available for 802.11ac Tools.

4. Associate STAs with APs by clicking an STA and then the down arrow next to it to select an AP to create an association.

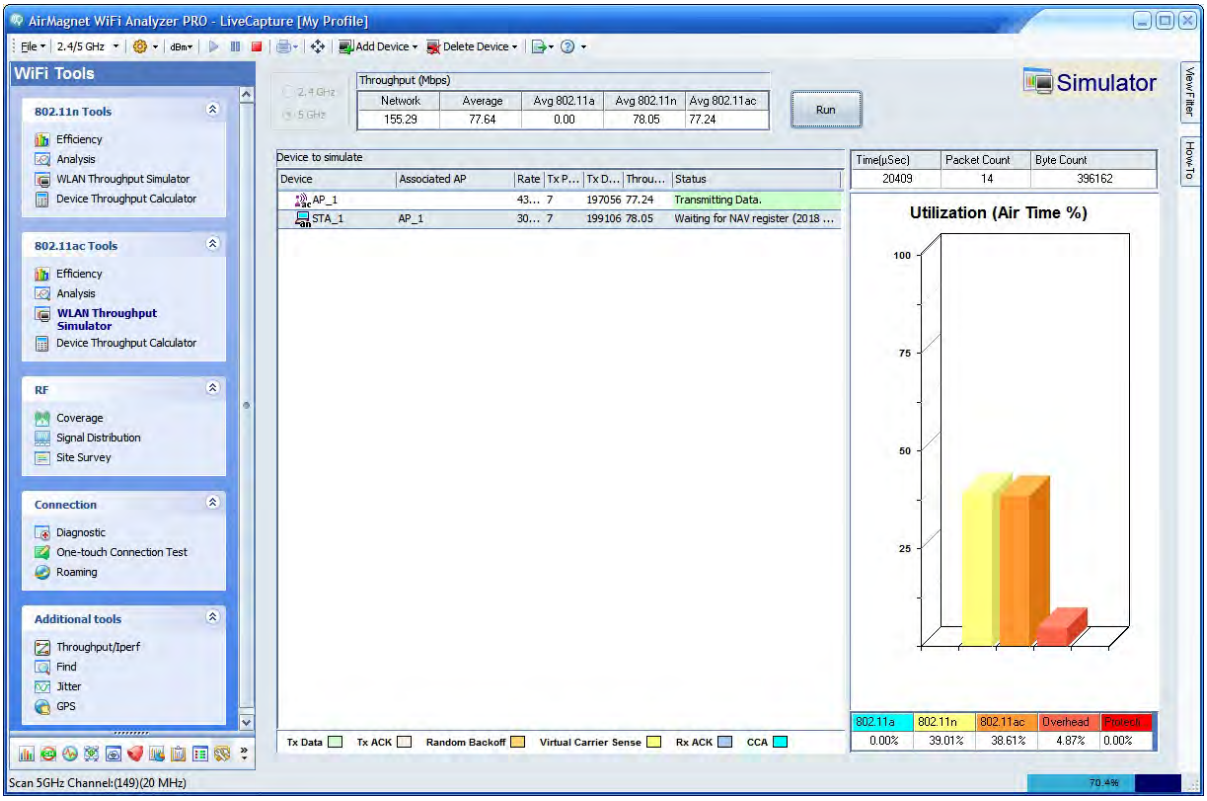


5. Repeat Step 3 to make sure that all APs and STAs are associated.

Note: *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.

Simulated WLAN Throughput Data



The table below explains the simulated WLAN data as shown on the WLAN Throughput Simulator screen.

Data Field	Description
Throughput (Mbps)	Shows WLAN throughput in Mbps in the following categories:
Network	The network throughput which is the combined, aggregate throughput of the wireless all media. Depending on whether you are using 802.11n or 802.11ac Tools, this may include 802.11a/b/g/n/ac, depending on the frequency band selected, that is, 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).

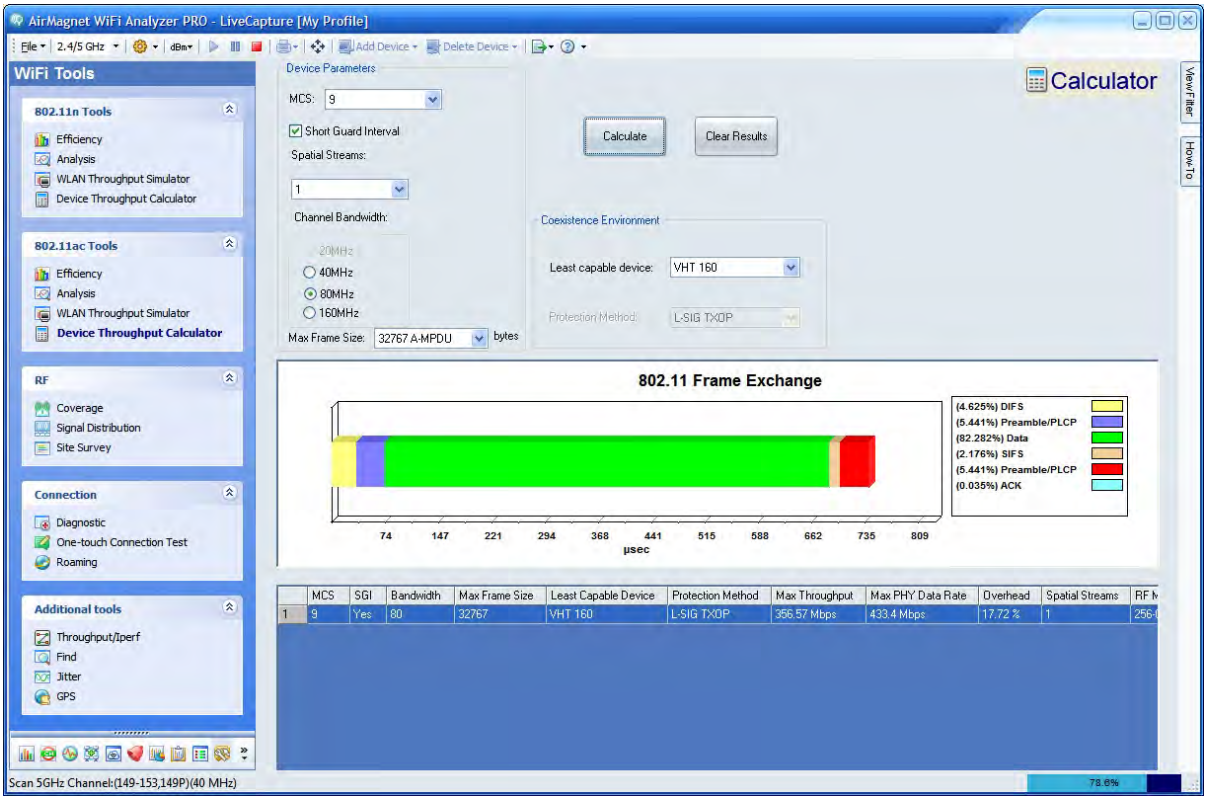
Avg 802.11b	The average node throughput for all 802.11b devices.
Avg 802.11g	The average node throughput for all 802.11g devices.
Avg 802.11n	The average node throughput for all 802.11n devices.
Avg 802.11ac	The average node throughput for all 802.11ac devices.
Device to Simulate	Shows information about each of the devices involved in the simulation.
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 any of the following: ▪ TX Data ▪ Tx ACK ▪ Random Backoff ▪ Virtual Carrier Sense
Time (µsec)	The simulation time (in µsec). ***Note:*** *The simulation engine runs at 1/1000th time scale, which means that every second of "real-time" represents one*

	millisecond of "simulation time".
Packet Count	The number of packets sent over the channel.
Byte Count	The number of bytes sent over the channel.

Note: *The WLAN Throughput Simulator will still use the required protection to transmit to the 802.11b stations even though it is configured for greenfield, which may or not be the right thing to do. One could argue that if one puts up a greenfield AP, it may still allow an 802.11b station to associate and then stop using greenfield. Until we see an AP which does not allow the association, this may be the closest to what will happen for real AP/STAs.*

Device Throughput Calculator

The Device Throughput Calculator is a utility for calculating a device's theoretical throughputs. Just click to specify the parameters such as MCS index, SGI, bandwidth, maximum 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. Refer to Calculating Device Throughput.



Calculating Device Throughput

The Device Throughput Calculator allows you 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 user the Device Throughput Calculator:

1. From the WiFi Tools screen, click **Device Throughput Calculator**.
2. On the Device Throughput Calculator screen, make the selections as described in the table below.

Parameter	Description
MCS	Click the down arrow and select an option from the drop-down list. 802.11n: 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. 802.11ac: MCS 1-9 is available from the drop-down.
Spatial Streams (802.11ac)	Click the down arrow and select an option from the drop-down list. This option is used in conjunction with MCS.
Short Guard Interval	If checked, Short Guard Interval (SGI) is enabled. ***Note:*** *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 the desired bandwidth: 20, 40, 80, 160.
Max Frame Size	Click the down arrow and select an option from the drop-down list.
Block ACK (802.11n)	If checked, Block Acknowledgement is enabled.

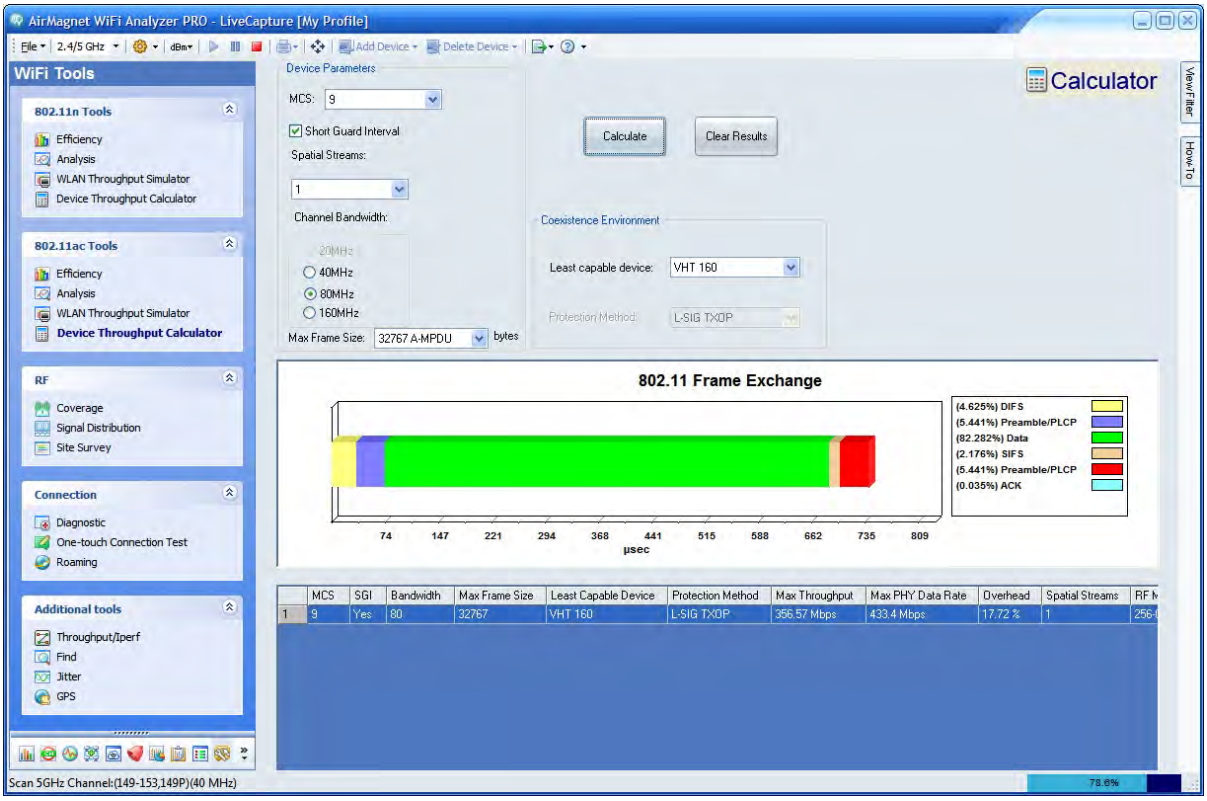
Least Capable Device	Click the down arrow and select an option from the drop-down list: ▪ VHT 160 ▪ VHT 80 ▪ VHT 40 ▪ VHT 20 ▪ HT 40 Mixed Mode ▪ HT 20 Mixed Mode ▪ 802.11a
Protection Method	Click the down arrow and select an option from the drop-down list: ▪ CTS-to-Self ▪ RTS/CTS ▪ L-SGI TXOP ***Note:*** *None of these protection methods applies to HT 40 Greenfield.*

3. Click **Calculate**. 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.

Note: *AirMagnet WiFi Analyzer generates a calculation 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. Click here for a sample screen that shows calculation results.*

Calculated Device Throughput Data

AirMagnet WiFi Analyzer calculates device throughput data based on the parameters the user has selected and display the results in the lower half of the screen. The screen shows two types of information: 802.11 Frame Exchange in the graph and throughput data in the table - as shown in the figure below.



The table below briefly explains the 802.11 frame exchange shown in the graph.

Data	Description
DIFS	DCF Interframe Space.
Preamble / PLCP	Preamble/Physical Layer Convergence Procedure.
Data	Data Frame.
SIFS	Short Interframe Space.
Preamble / PLCP	Preamble/Physical Layer Convergence Procedure.
ACK	Acknowledgement Frame.

RF Tools

About RF Tools

AirMagnet WiFi Analyzer provides RF tools that assist network administrators to learn and understand the RF conditions on or around their WLAN site in terms of RF coverage, signal distribution, and signal strength and noise level, and so on. The real-life RF data obtained through these tools help them make well-informed decisions regarding their WLAN deployment and enhancement.

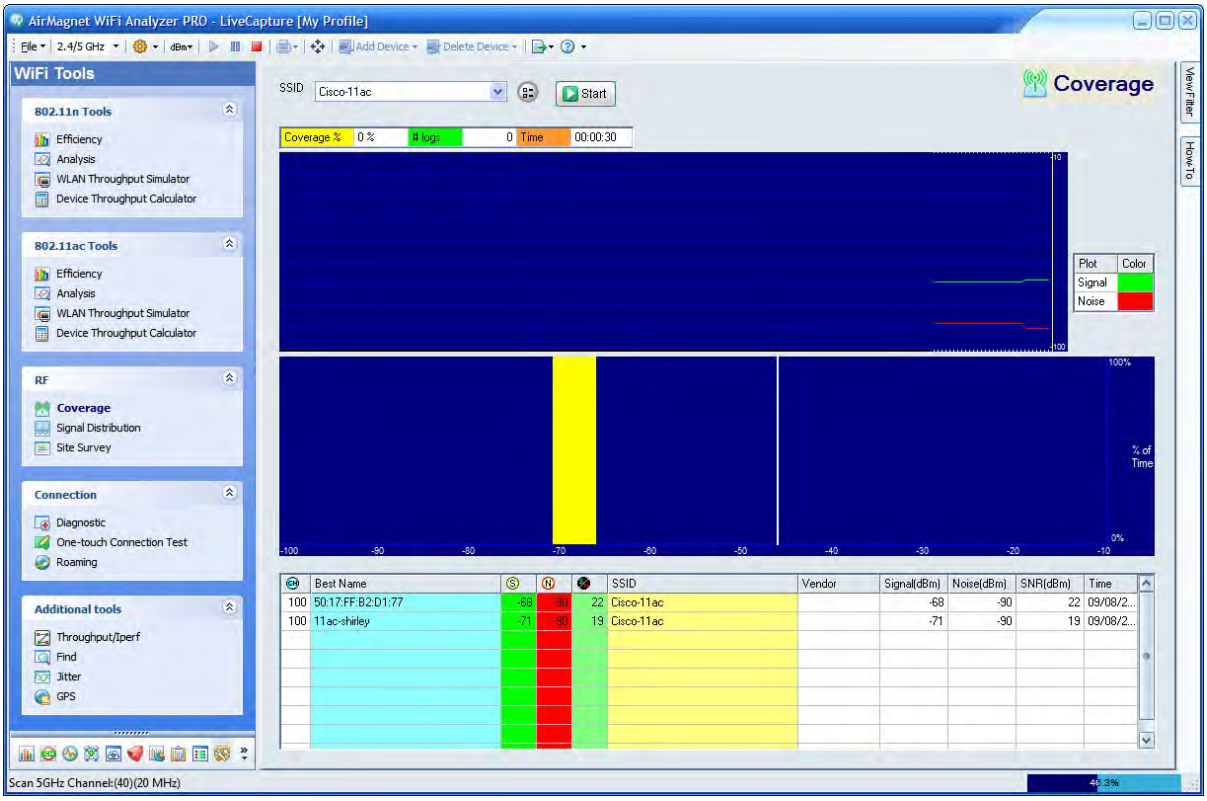
Three tools fall within this category:

- 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. The figure below shows the Coverage tool screen. Refer also to Configuring Coverage Tool and Measuring WLAN Site Coverage.

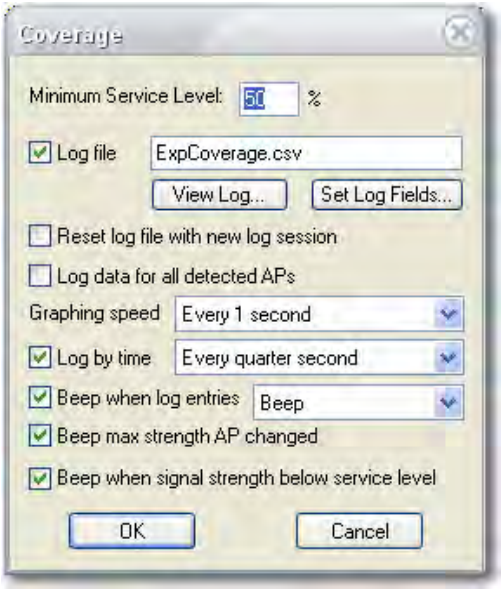


Configuring the Coverage Tool

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.

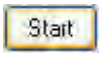
To configure signal coverage test settings:

1. From the **WiFi Tools>Coverage** screen, click  **(Configure).**
2. Make the desired selections and click **OK.**



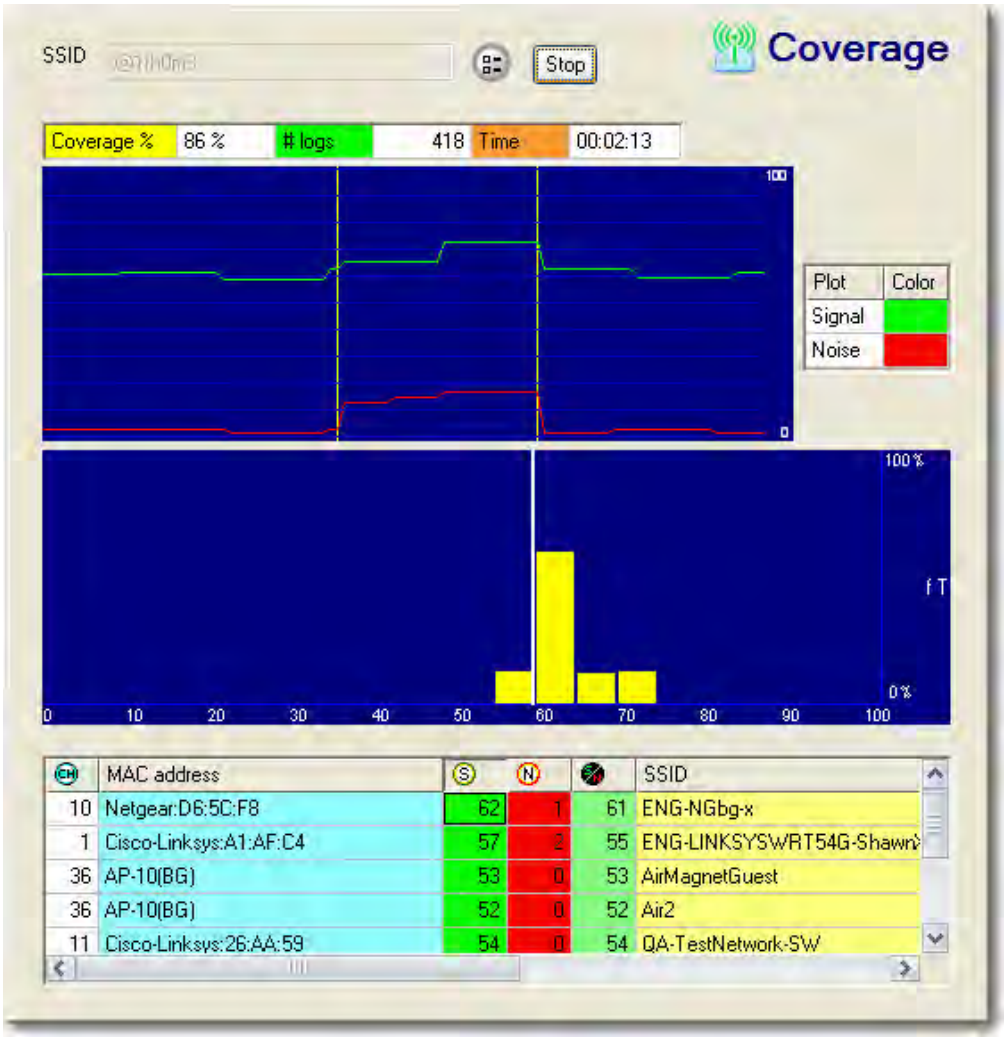
Measuring WLAN Site Coverage

To measure the site RF signal coverage:

1. From the top of the Coverage tool screen, click the down arrow and select an SSID from the drop-down list.
2. Click 

. Data will start to appear on the screen.
3. Click 

to end the coverage test.



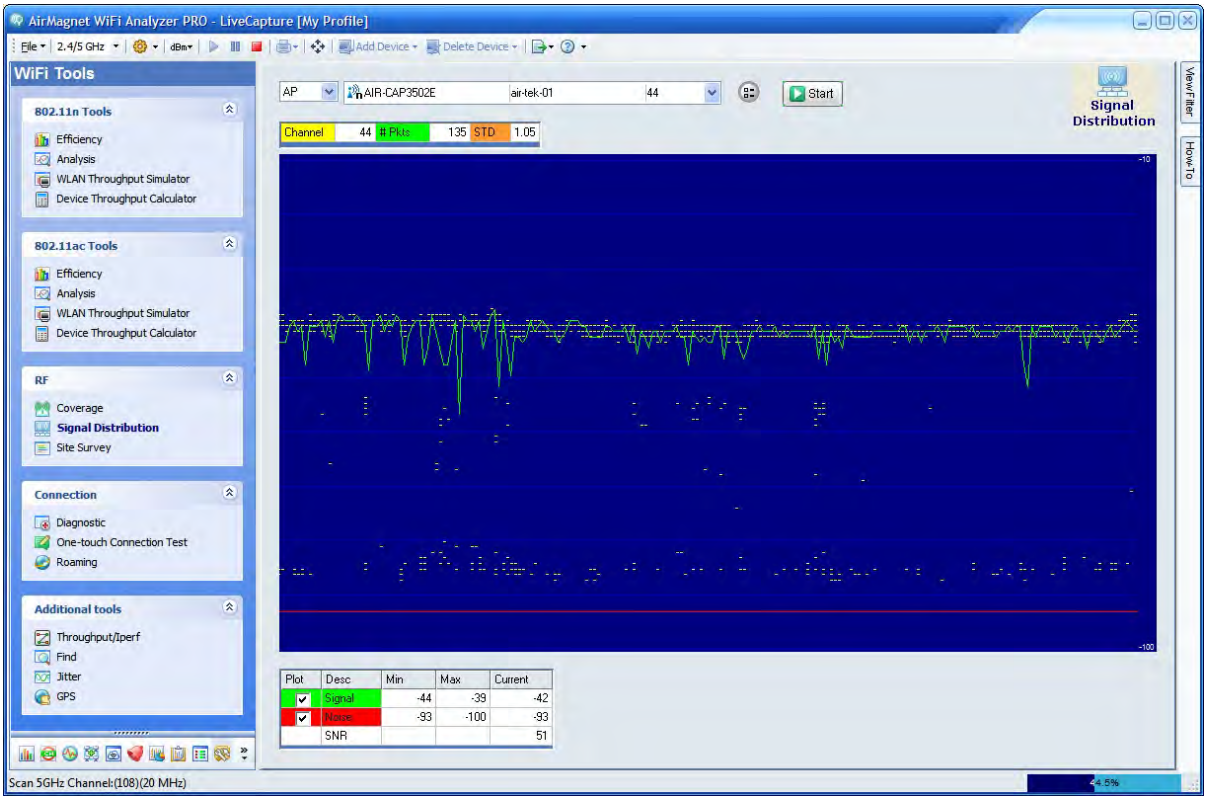
The Coverage tool screen provides a complete picture of the RF signal coverage for the selected SSID. The tool also shows the amount of traffic that is above the specified Minimum Service Level which is represented by the white vertical line in the bar graph. The bars to the right of the white line represent 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 take AirMagnet WiFi Analyzer and roam through the coverage area. 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 signal multi-path. It provides an easy way to monitor WLAN RF signal distribution patterns and to visualize issues that would otherwise be difficult to see and analyze. The example below shows the

Signal Distribution tool screen. Refer also to Configuring Signal Distribution Tool and Testing WLAN Site Signal Distribution.



Configuring Signal Distribution Tool

To configure the Signal Distribution tool settings:

1. From the **WiFi Tools>Signal Distribution** screen, click  **(Logging Options)**.
2. Make the desired selections and click **OK.**

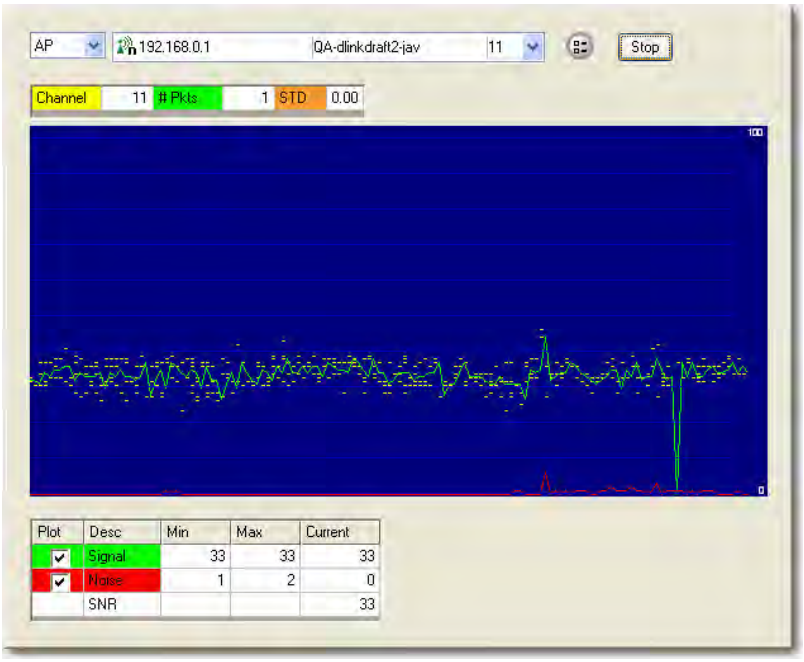
Testing WLAN Site Signal Distribution

To conduct a signal distribution test:

1. From the **Tools>Signal Dist** screen, select AP or STA, and select a specific AP or STA on the right.
2. Click 

. Signal distribution data start to appear on the screen.
3. Click 

to end the test.

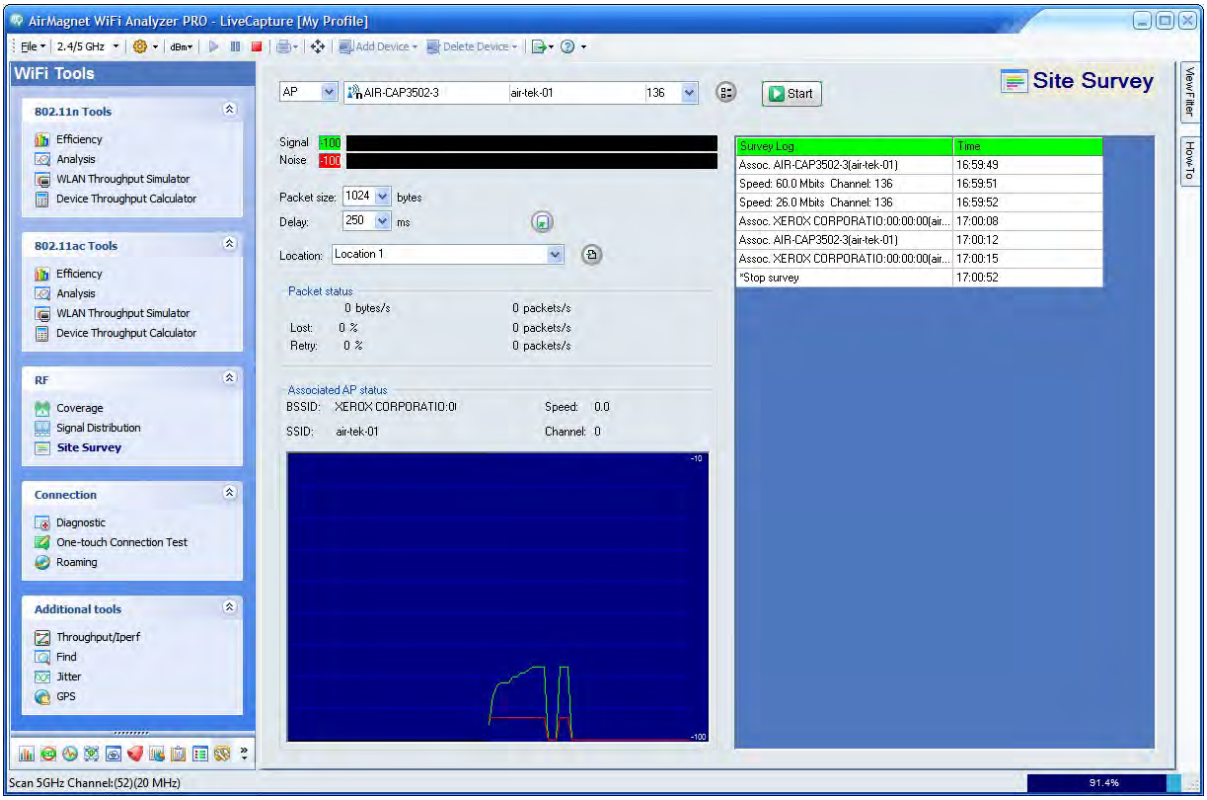


Note: *The cluster of yellow dots shown in the example above represents the RF signal per packet being seen from the current location. In case of good signal distribution, the dots should be all close together within a narrow range. It means that the site RF signals are consistent in strength with little 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

The Site Survey provides 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, and so on directly from within AirMagnet WiFi Analyzer. The example below shows AirMagnet WiFi Analyzer's

Site Survey tool screen. Refer also to Configuring Site Survey Tool and Conducting a WLAN Site Survey.



AirMagnet WiFi Analyzer's built-in Site Survey tool 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, and so on.

Configuring Site Survey Tool

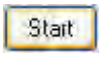
To configure the Site Survey tool:

1. From the Site Survey tool screen, click  **(Logging Options)**.

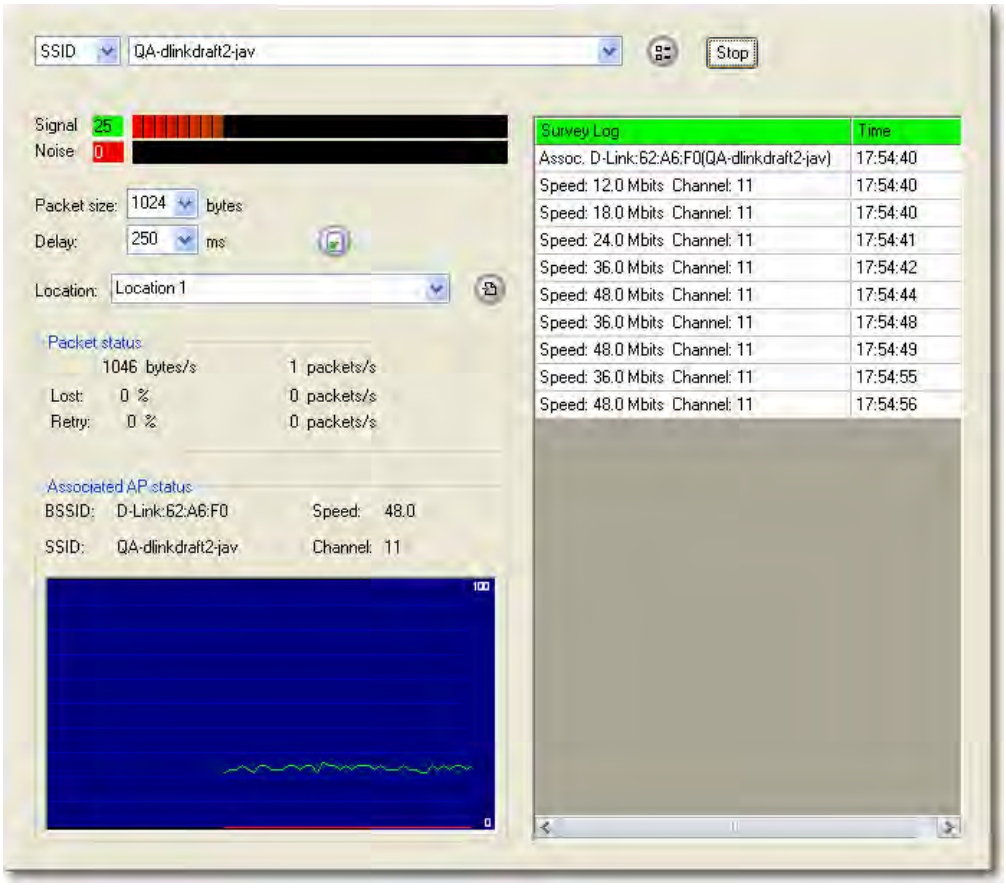
2. Specify a path for exporting the survey file.
3. Name the file in a way that is unique to the location of the survey.
4. Uncheck **Trigger by event.**
5. Make the other selections as you desire.
6. Click **OK.**

Conducting a 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 screen, select **AP** or **SSID** and then the specific AP or SSID you want to associate with.
3. Click 

. Live data starts to appear on the screen**.**



3. Click 

to end the survey.

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.

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 causes your computer to roam once it reaches a specific minimum signal strength, whereas configuring roaming based on speed causes 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.

Note: *You can find a list of adapters that support this feature at https://www.netally.com/wp-content/uploads/2019/12/AMM-Preferred-Adapters.pdf. Locate the desired adapter and click* ***More details****. Refer to the column labeled "Roaming Control for Active Surveys."*

Connection

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.

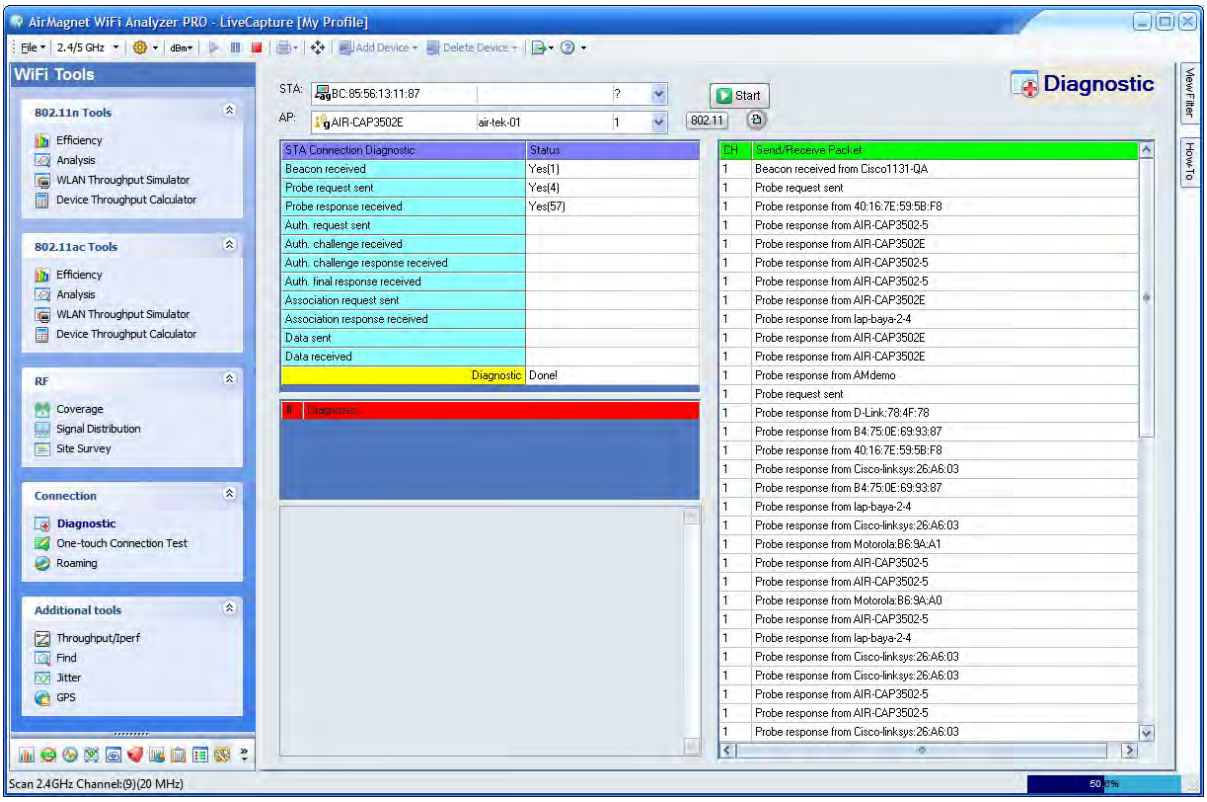
The following are the connection tools:

- **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.

Diagnostic Tool

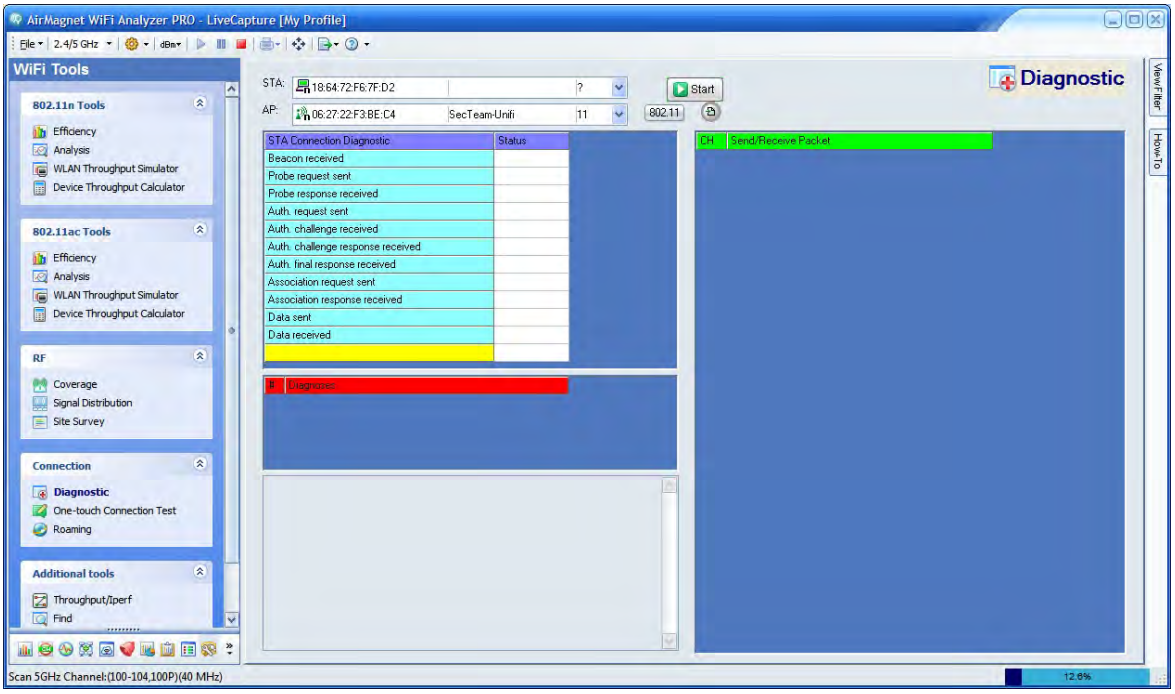
Without intelligent tools, the process of troubleshooting a problem connection between a client station and an AP can be an incredible drain on professional resources. AirMagnet WiFi Analyzer's Diagnostic tool identifies mismatched configurations, such as SSIDs, WEP keys, transmission rates, preamble, 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. The figure below shows the Diagnostic tool screen. Refer also to Diagnosing Network Connectivity Issues.



Diagnosing Network Connectivity Issues

To diagnose a client station connection problem:

1. Locate the client 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 a laptop PC (with AirMagnet WiFi Analyzer running on it) next to the client station.
4. From the **WiFi Tools** screen, click the **Diagnostic** tool.

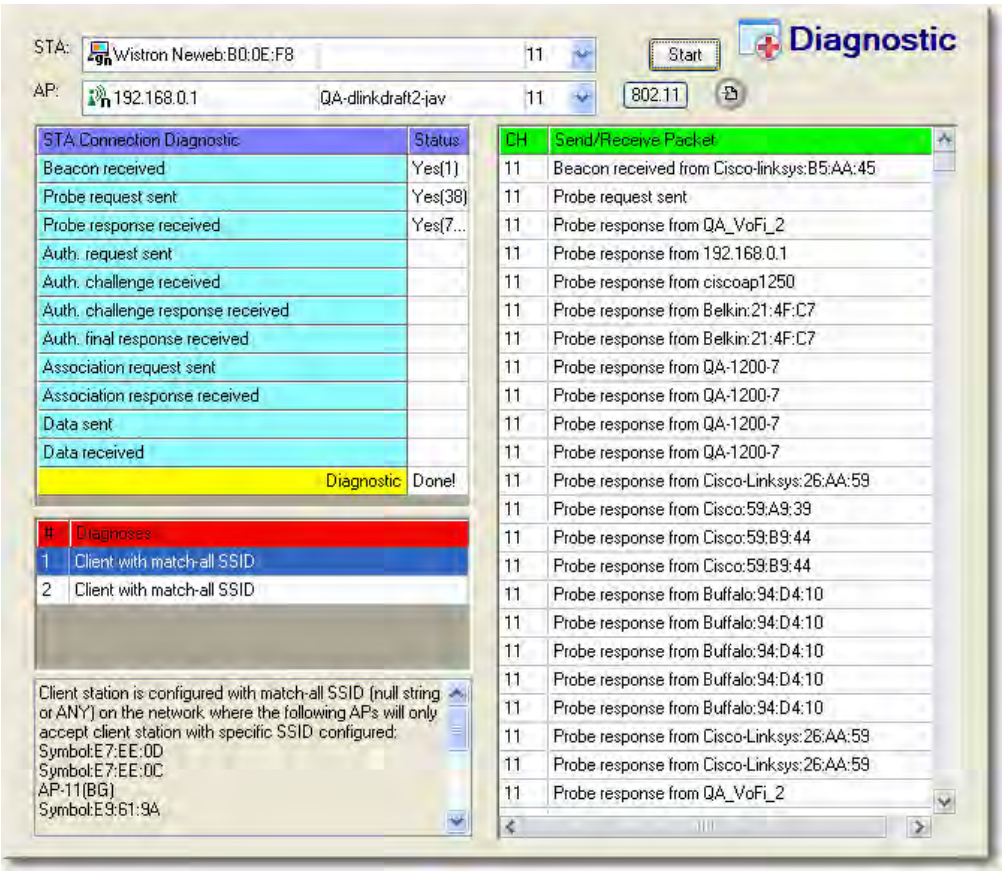


5. For **STA,** select the client station MAC address from the STA drop-down list.
6. For **AP**, select the AP that the client is supposed to connect with from the AP drop-down list.

Note: *You can select ANY if you are not sure which AP to use, but the accuracy of the diagnosis will be reduced.*

7. Click 

. The Diagnostic tool screen shows the progress in association with the AP.



Note: *The diagnostic test automatically ends once it is 100% completed. However, if you want to stop a diagnostic test that is still in progress, just click* Stop.

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 802.1X to display 802.1x information.

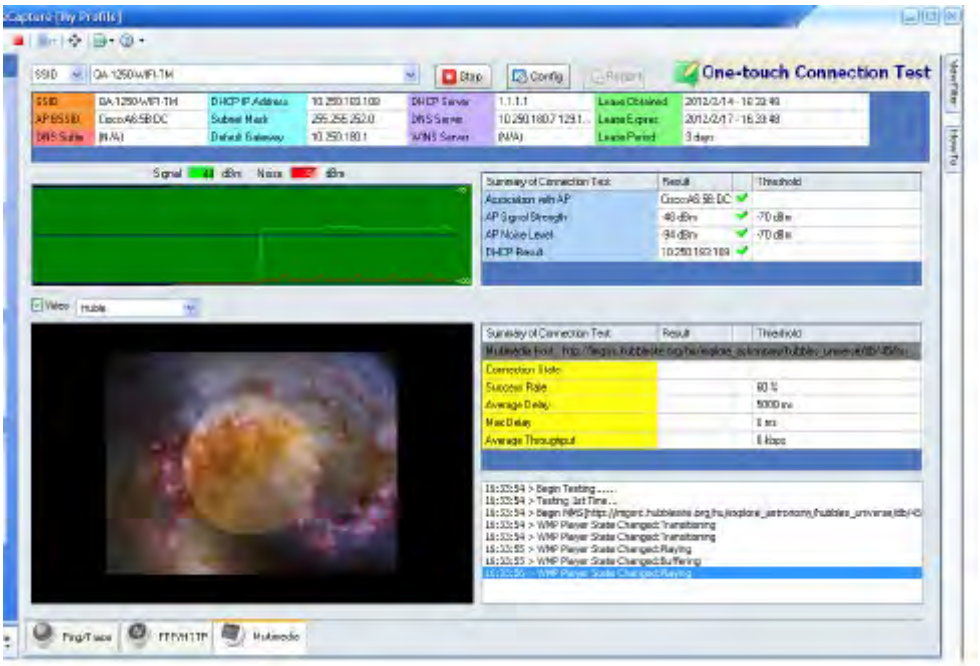
11. Click **(Export)** to export the log data.

One Touch Connection Test Tool

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 tool enables you to easily conduct a number of end-to-end connectivity tests from one user interface.

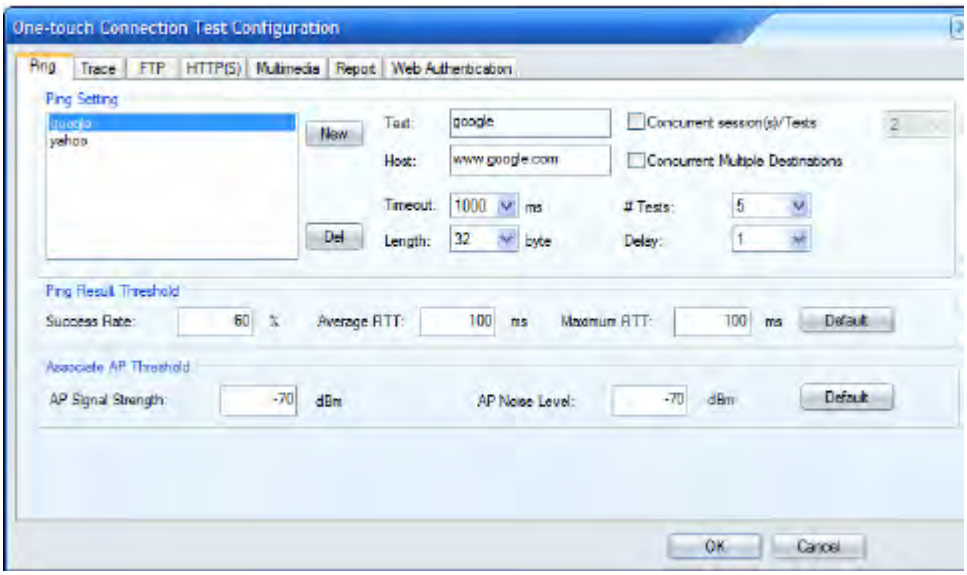
AirMagnet WiFi Analyzer provides the following uniquely integrated active tools to address these anomalies:

- Ping
- Trace
- FTP
- HTTP
- Multimedia



Configuration

You can configure the One-Touch Connection Test tool by clicking **Config** at the top of the screen.



Generate Report

To generate a One Touch Connection report, you must choose the report option before starting a test. Click the **Report** Tab in the Configuration dialog and check **Create One-Touch Connection Test Report**.

Use the **Report Options** to add information to the report such as Report Name, Location, Tester Name, Page Header and Page Footer.

When the One-Touch Connection Test is started, the tests will run and gather information. Once the test is complete, tyou can view the report by clicking **Report**.

Report formats: PDF, HTML, RTF, XLS and XML.

Concurrent Sessions/Tests and Multiple Destinations

For the Ping Test, FTP Test and HTTP(S) Test you can choose to run both concurrent (simultaneous) tests of the same destination as well as concurrent tests of multiple destinations.

Concurrent Sessions / Tests: Check this option to run concurrent sessions against the selected Test (for example, Host). Use the drop-down to the right to set the number of concurrent sessions to run (1-10). Use this option in combination with the Concurrent Multiple Destinations option.

Concurrent Multiple Destinations: If you have created multiple tests (hosts), you can choose to run them all concurrently. To do this, check Multiple Concurrent Destinations. This option may be used in combination with the Concurrent Sessions/Tests option.

Ping Configuration

1. Click **Config**.

2. Click the **Ping** tab.
3. Click **New** and type a test name. Click **OK**.
4. With the test name selected, type the web address (for example www.domainName.com) in the **Host** text box.
5. Change any other default settings as desired.

Option	Description
Timeout	Length of time in milliseconds before the ping test will abort.
Length	Frame length in bytes.
# Tests	Number of consecutive times to run the test.
Delay	Delay time between tests.
Success Rate	Percentage echo reply back needs to be successful.
Average RTT	Average round trip time.
Maximum RTT	Maximum round trip time.
AP Signal Strength	Signal strength of the associated AP.
AP Noise Level	Noise level in dBm.

Trace Configuration

Use the Trace option to isolate the routing path and locate breakage.

1. Click **Config**.
2. Click the **Trace** tab.
3. Click **New** and type a test name. Click **OK**.
4. With the test name selected, type the web address (for example www.domainName.com) in the Host text box.
5. Change any other default settings as desired.

Option	Description
# Tests	Number of consecutive times to run the test.
Success Rate	Percentage echo reply back to be successful.
Average Delay	The average round trip delay in communicating with the host in milliseconds.
Maximum Delay	Maximum round trip delay in communicating with the host in milliseconds.

FTP Configuration

The FTP tool allows you to connect to a specified FTP server and transfer a selected file upload and download as many times as set in the configuration.

1. Click **Config**.
2. Click the **FTP** tab.
3. Click **New** and type a test name. Click **OK**.
4. With the test name selected, configure the FTP server information.
5. Adjust any default settings as desired.

Option	Description
Server	IP address of the FTP host.
Port	Port number for the FTP host.
# Tests	Number of times to run the test.
User	FTP host username.
Password	FTP host password.

Local File	The absolute path to a file to use to upload and download from the FTP site.
Upload Success Rate	Percentage upload success rate for the number of times the test will be run.
Upload Average Throughput	Average required speed in kilobits-per-second for the test to be successful.
Upload Average Delay	Average upload connection delay requirement for test to be successful.
Upload Maximum Delay	Maximum upload connection delay requirement for test to be successful.
Download Success Rate	Percentage download success rate for the number of times the test will be run.
Download Average Throughput	Average required speed in kilobits-per-second for the test to be successful.
Download Average Delay	Average download connection delay requirement for test to be successful.
Download Maximum Delay	Maximum download connection delay requirement for test to be successful.

HTTP(s) Configuration

The HTTP tool functions much like the FTP tool, testing HTTP upload/download instead of FTP. It allows you to connect to a specified HTTP server and transfer a selected file back and forth as many times as required to verify connectivity.

1. Click **Config**.
2. Click the **HTTP** tab.

3. Click **New** and type a test name. Click **OK**.
4. With the test name selected, type an URL and image or file name (or copy and paste the URL from a browser).
5. Adjust any default settings as desired.

Option	Description
# Tests	Number of consecutive times to run the test.
Download Success Rate	Percentage download success rate for the number of times the test will be run.
Download Average Throughput	Average required speed in kilobits-per-second for the test to be successful.
Download Average Delay	Average download connection delay requirement for test to be successful.
Download Maximum Delay	Maximum download connection delay requirement for test to be successful.

Multimedia configuration

The Multimedia option enables you to test connectivity to media such as a movie or audio file.

1. Click **Config**.
2. Click the **Multimedia** tab.
3. Click **New** and type a test name. Click **OK**.
4. With the test name selected, type an URL ending in a media file name (or copy and paste the URL from a browser).
5. Adjust any default settings as desired.

Option	Description
# Tests	Number of consecutive times to run the test.

Duration	Time in milliseconds to run the test.
Timeout	Length of time in milliseconds before the test will abort.
Success Rate	Percentage success rate for the number of times the test will be run.
Play Average Delay	The average delay in communicating with the host in milliseconds.
Max Delay	Maximum delay in communicating with the host in milliseconds.
Average Throughput	Average required speed in kilobits-per-second for the test to be successful.
Frame Skipped	Retrieves the total number of frames skipped during playback.
Lost Packets	Retrieves the number of packets lost. This method retrieves streaming media packets only, and will equal zero when using the HTTP protocol, which is lossless. Packets may be lost for a number of reasons, such as the type and quality of the network connection. Each time playback is stopped and restarted, the value retrieved from this method is reset to zero. The value is not reset if playback is paused. This method retrieves valid information only during run time when the URL for playback is set.
Bandwidth	Retrieves the current bandwidth of the media item. This option is only applicable for streaming media.

Supported multimedia formats:

ASF AIF AIFCAIFF AU

AVI MID MPE MPEG MPG

MPv2 MP2 MP3 M1V SND

WAV

Windows Media files with a *.wm* file name extension

Windows Media Audio (*WMA*)

Windows Media Video (*WMV*)

The following protocols are currently supported by Windows Media Player:

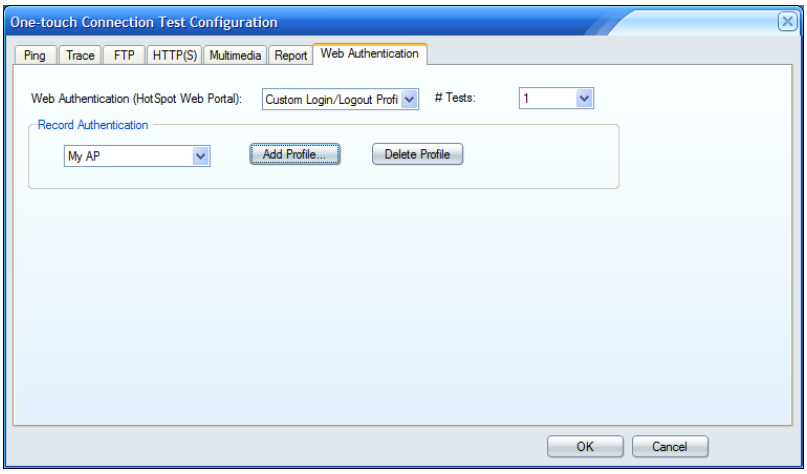
Protocol	Description
HTTP	Hypertext Transfer Protocol. Includes HTTP with fast cache and multicast.
RTSP	Real Time Streaming Protocol. Includes RTSP with fast cache.
RTSPU RTSP	Used with User Datagram Protocol (UDP). Includes RTSPU with fast cache.
RTSPT RTSP	Used with Transmission Control Protocol (TCP). Includes RTSPT with fast cache.
MMS	Microsoft Media Server protocol.
MMSU	MMS used with UDP.
MMST	MMS used with TCP.
WMPCD	A protocol used by Windows Media Player to provide access to

	compact discs.
WMPDVD	A protocol used by Windows Media Player to provide access to DVD-ROM discs.

Web Authentication Configuration

The Web Authentication tool lets you test authentication in the case where an AP automatically redirects to a web site that requires authentication such a login and logout.

1. From **One Touch Connection Tool** view, Click **Config**.
2. Select the **Web Authentication** tab.
3. Choose an option from the drop-down:
   - **None:** This is the default for not using web authentication test.
   - **Manual Test:** Select this option when authentication requires non-password, manual intervention such as checking a box to agree to terms.
   - **Custom Login/Logout Profile:** Select this option to create a profile for a web site that implements password protection.
4. If you selected the **Custom Login/Logout Profile** option, you will need to create a login/logout profile.



5. Click **Add Profile**. Type a profile name and click **OK**.
6. Select an AP/SSID from the drop-down and click **Connect**. An association with the AP will be established.

Note: *For any password protected AP/SSID, you will need to have set up the profile in the main WiFi Analyzer Configuration under the 802.11 tab.*

7. Click **Next**. This will open the web page.
8. Click **Start Record**. Login to the web page. Click **Stop Record**. Click **Next**.

9. Click **Start Record**. Logout of the web page. Click **Stop Record**. Click **Finish**.

To complete the Web Authentication configuration, select the number of times to run this test from the **# Tests** drop-down.

Running a One Touch Connection Test

Once you have configured one or more tests, run the tests. One or more tests can be run consecutively.

1. Click the tab on the navigation bar for the desired test(s): Ping/Trace, FTP/HTTP or Multimedia.
2. Check the desired test(s) to be run.
3. Click **Start**.

The test(s) will run and populate the One Touch Connection view with test results.

Note: *If the computer's firewall is enabled, it may block one or more tests from running. In this case, a message may be displayed indicating the firewall is on. Stop the test (click Stop) and disable the firewall.*

While the tests are running, the related tab on the navigation bar will blink.

4. To cancel the test, click **Stop**.

One Touch Connection Results

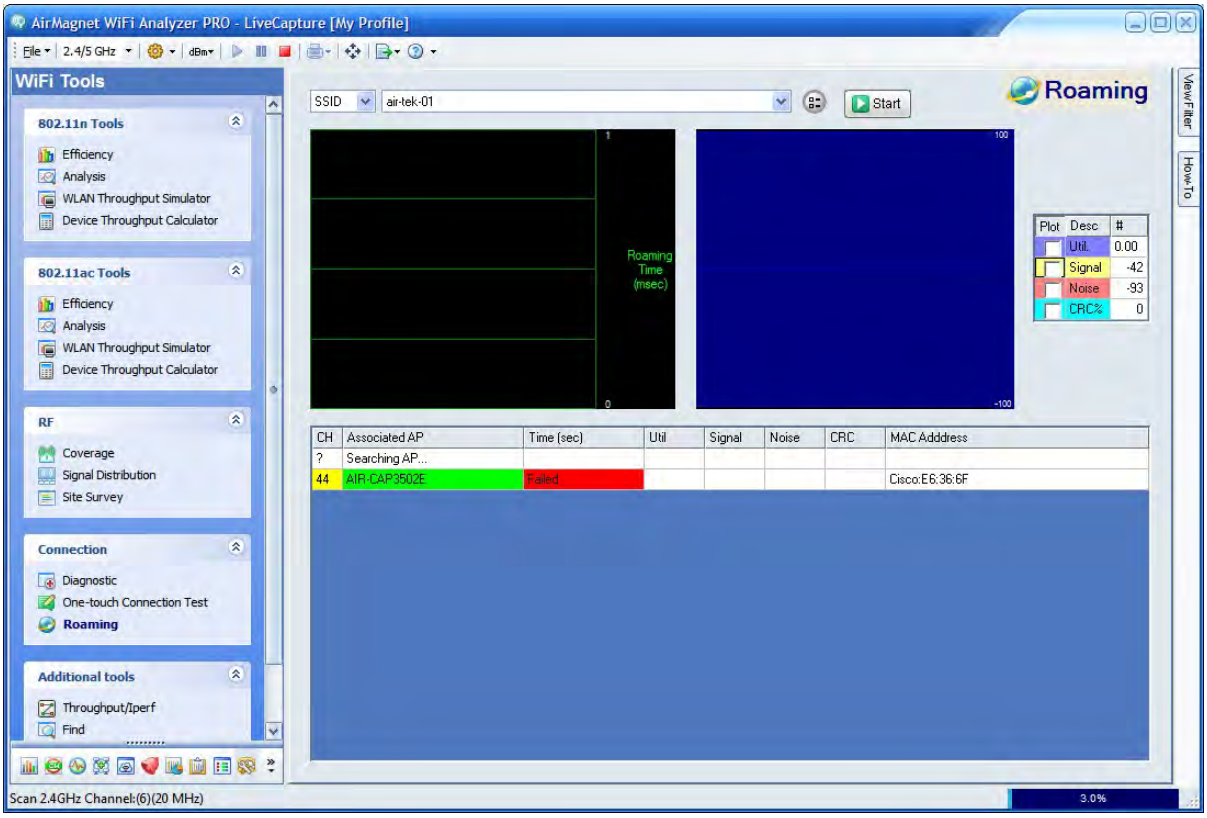
When the test is finished, the results are posted in the **One Touch Connection Test** view. Click the associated tabs on the navigation bar to view results.

If you had checked the "Create One-Touch Connection Test Report," the Report button is available. Click **Report** to generate the report.

One Touch Connection Test Results

Roaming Tool

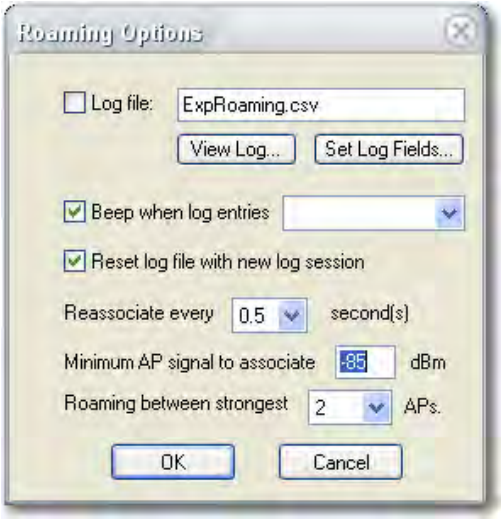
The Roaming tool is another utility for troubleshooting VoWLAN installations. A key component of VoWLAN QoS is its ability to allow stations to roam between APs without dropping calls. If roam time is too long, the chances that calls will be dropped increases considerably. With AirMagnet WiFi Analyzer's Roaming tool, you 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. Refer to Configuring Roaming Tool and Conducting Roaming Tests.



Configuring Roaming Tool

To measure roaming connectivity:

1. From the **Roaming** tool screen. click **(Configure)**.



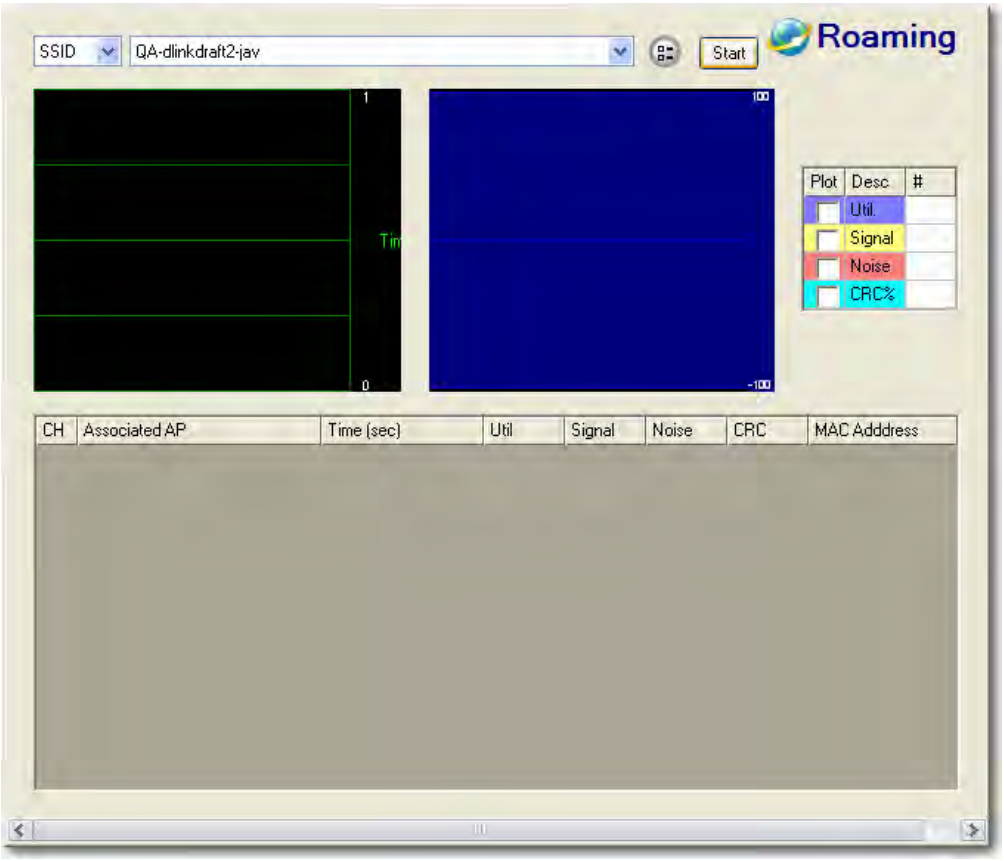
2. From the Roaming Options dialog box, make the desired selections.
3. Click **OK.**

Conducting Roaming Tests

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 Start.

Data will start to appear on the screen.



3. Click Stop to end the roaming test.

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, you 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 Tools

Throughput/Iperf

AirMagnet WiFi Analyzer integrates with Iperf – a free, open-source software tool for network performance analysis. The integration allows you 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 WiFi Analyzer's integration with Iperf, you must download and install Iperf Version 1.7.0, which has been tested and verified to be working with this AirMagnet WiFi Analyzer 8.0 and later releases. Refer to Install Iperf Software and Analyzing Bandwidth and Throughput.

Installing Iperf Software

AirMagnet Survey's integration with the open-source Iperf software provides you with a means of recording both upload and download transmit rates during an active survey. Although this requires some additional configuration when compared to active surveys, the ability to view both upload and download speed information can be invaluable when analyzing the wireless network environment.

During an Iperf survey, the laptop which is being used to conduct the survey transmits custom Iperf data packets to a user-configured Iperf server. The server's responses allow Survey to record the station's download speed from the current location.

In order to conduct an active Iperf survey, you must download and unzip the Iperf server software on a separate device. You may locate Iperf software by means of internet search on the term "iperf 1.7". Iperf integration is designed to operate with Iperf Server version 1.7.0.

Note: *We recommend that you create an Iperf folder in the root directory to contain the files (that is, C:\Iperf).*

Starting the Iperf Server

After you have downloaded and extracted the Iperf server software, you must launch the application before starting an Iperf survey.

1. Click ***Start>Run…*** to open the Run dialog box.
2. Type *cmd* and click ***OK*** to open the Windows command-line interface.
3. Navigate to the Iperf folder (for example, *C:\Iperf*), type 'Iperf -s' and press **Enter**. A message appears describing the TCP port in use by the server.

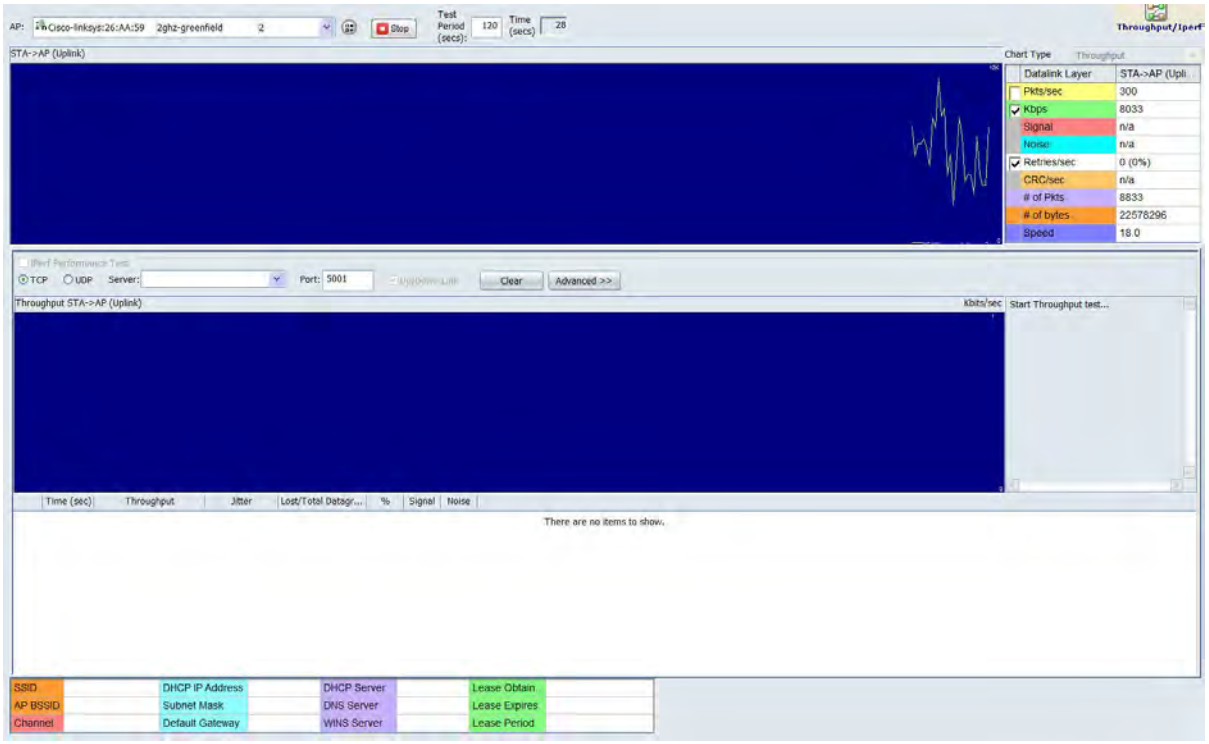
Note: *In the command to start the Iperf server, the '-s' parameter stands for 'server' and the '-p 5001' part tells the server to listen on port 5001. By default, AirMagnet Survey uses 5001 as the port for its transmissions during an active Iperf survey. If the Iperf server port is changed, you must change the port used by the Survey application as well.*

Once the Iperf server status message appears, the system is actively listening for Iperf transmission messages. The system is now ready for conducting an active Iperf survey.

Analyzing Network Bandwidth and Throughput with Iperf

To analyze network bandwidth and throughput with Iperf:

1. From WiFi Tools screen, click **Throughput / Iperf.** The Throughput/Iperf screen appears.
2. Select an AP.
3. Specify the length of the **Test Period**, for example, 120.
4. Select a **Chart Type**, for example, PHY Data Rate.
5. Make sure to check the **Iperf Performance Tes**t check box.
6. Select TCP or UDP and specify the Server and Port.
7. Check the Up/Downlink check box.
8. Click Start. Data starts appearing on the screen, as shown in the example below.



Notes:

- The test ends automatically once the specified test period is timed out. You can also stop a live test at any time by clicking Stop.
- The example 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

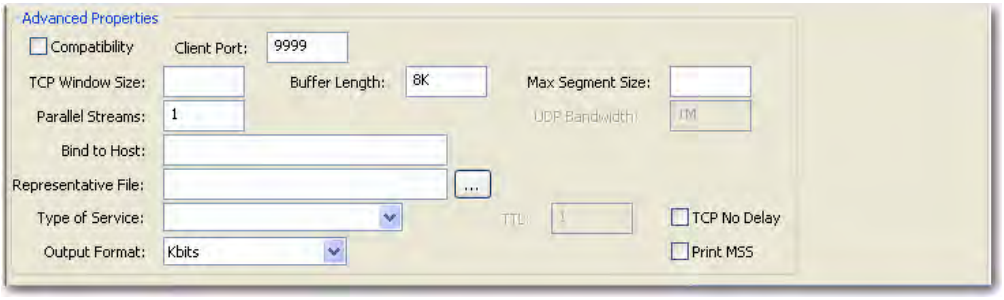
rate; for the uplink, 100% of the throughput (696 Kbps) is using 108-Mbps data rate.

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 is 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 and later Magnet 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.

Advanced Iperf Properties

The following screen shows the advanced properties on Iperf.



The table below describes the advance properties on Iperf tool.

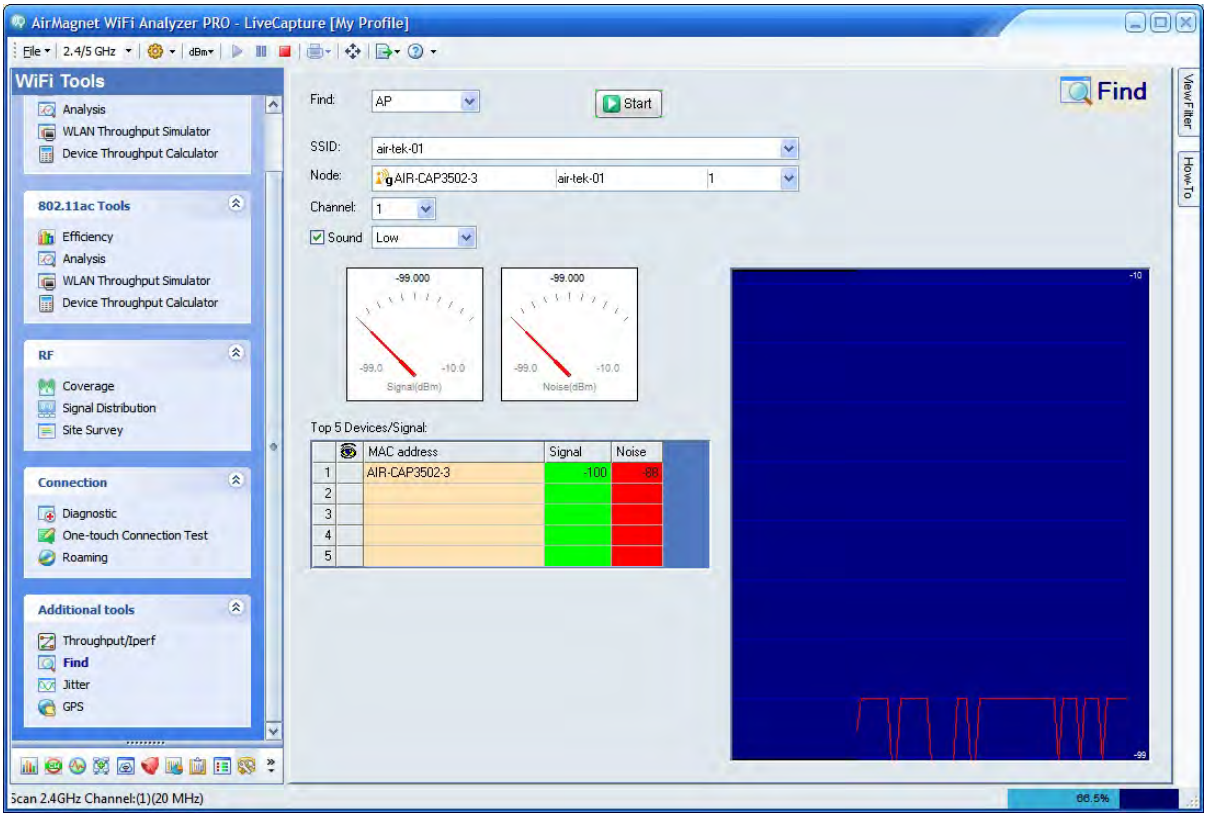
Property	Description
Compatibility	This option, if selected, allows for backward compatibility with older version of Iperf.
Client Port	The port through which the Iperf server connects to the client. It defaults to the port used to connect to the Iperf server from the client.
TCP Window Size	Sets the 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 us 1. ***Note:*** *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.
Bind to Host	One of this host computer'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: ▪ 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.

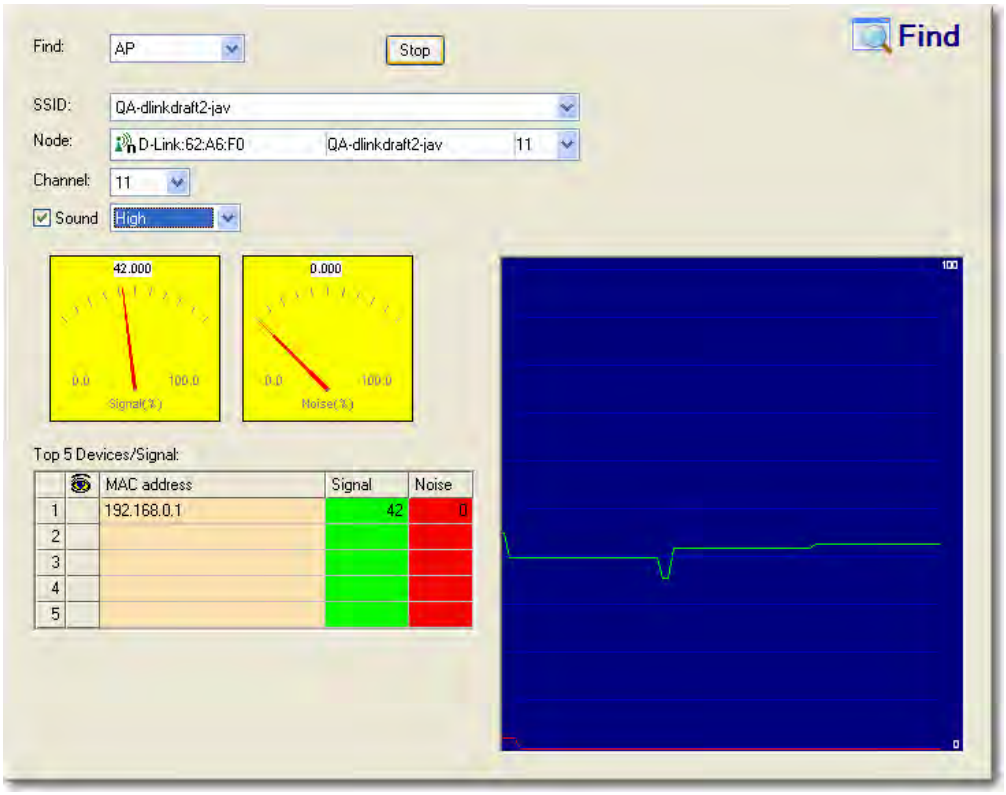
TCP No Delay	If selected, this sets the TCP no delay option, disabling Naggle's algorithm. Normally this is only disabled for interactive applications such as telnet.
Output Format	Click the down arrow and select from the drop-down list menu the format in which bandwidth numbers are to be printed. The supported formats are: ▪ Adaptive Bits ▪ Adaptive Bytes ▪ Bits ▪ Bytes ▪ Kbits ▪ Kbytes ▪ Mbits ▪ Mbytes
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, and so on). 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 you locate the physical location of any devices that have been detected. This can be easily done using AirMagnet WiFi Analyzer's Find tool. The figure below shows the Find tool screen. Refer also to Locating Rogue Devices.



Locating Rogue Devices



To locate a rogue device:

1. From the AirWISE screen, look for alarms under **Rogue AP and Station**.

2. Identify a rogue device (AP or station) and take down its vendor name (followed with the first three digits of its MAC address) and SSID.

3. From the **Find** tool screen, select **AP** or **STA.**

Note: *This must match the type of device you have selected from the AirWISE screen in Step 2.*

4. Select the SSID of the rogue device you have recorded.

5. Select the node device, if applicable.

6. Choose the channel the rogue device is on, if applicable.

7. Click 

. 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.

8. In the Top 5 Devices/Signal pane, click the box next to the device you wish to locate.

9. Turn on the audio and set the volume to High. This will make it even easier to locate the rogue device.

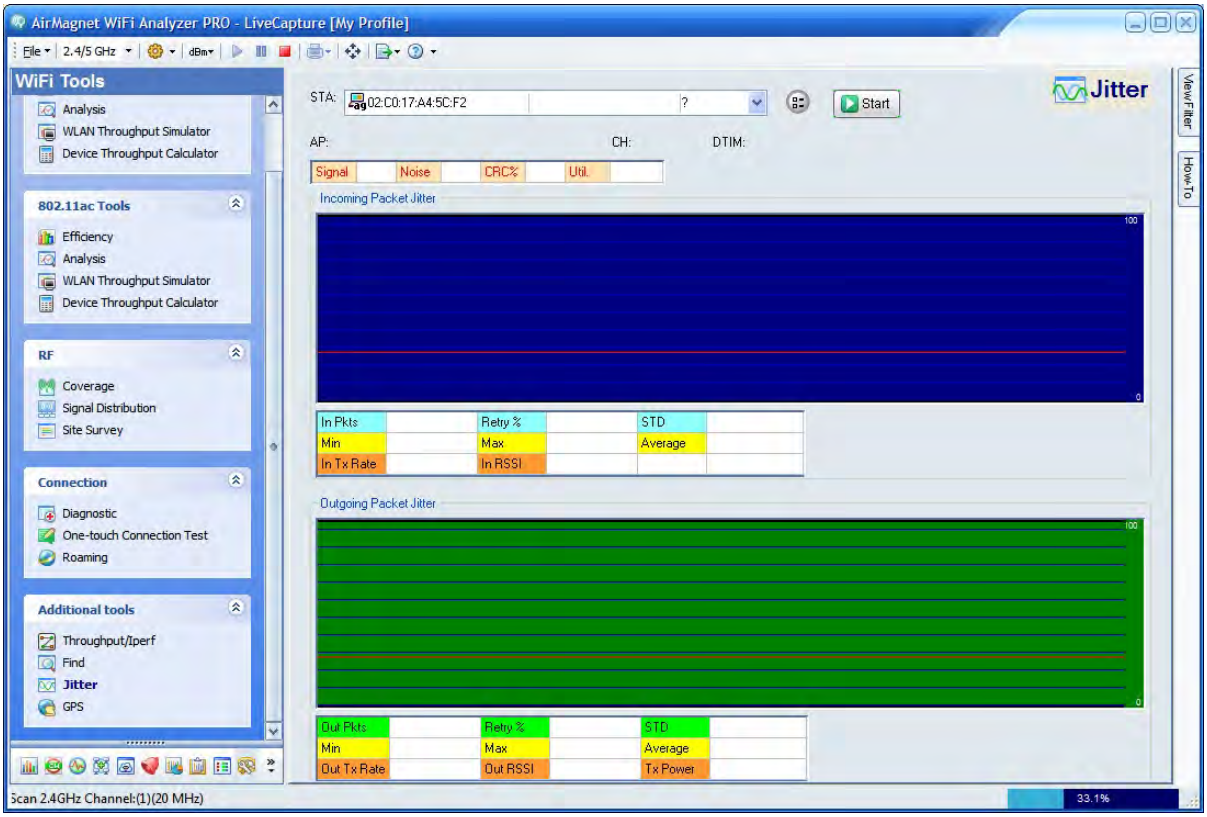
10. Look at the signal meter and walk in the direction where the signal gets stronger as you walk until you have physically located the device.

11. Click 

to end the operation.

Jitter Tool

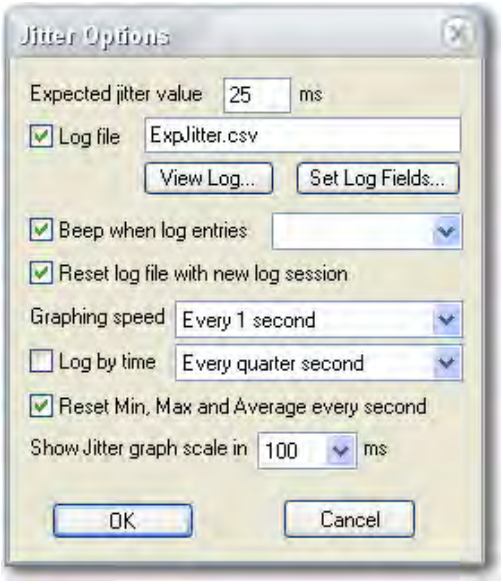
Jitter refers to unwanted variations in the frequency or phase of a digital or analog signal. VoWLAN phones and systems are designed to accommodate a certain amount of jitter in the network. However, if the jitter value gets too high, the quality of calls or network connections may suffer. AirMagnet WiFi Analyzer's Jitter tool enables network administrators to easily test the jitter value on a VoWLAN to ensure the QoS for voice traffic. The figure below shows AirMagnet WiFi Analyzer's Jitter tool screen. Refer to **Configuring Jitter Tool** and **Conducting Jitter Tests**.



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 Options:



1. From the **WiFi Tools>Jitter** screen, Click **(Configure)**.

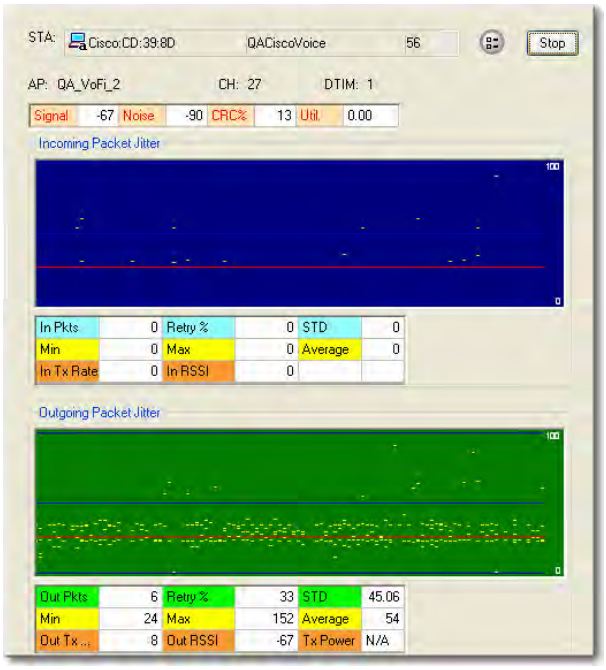
2. Make the desired selections and click **OK.**

Conducting Jitter Tests

To measure RF signal jitter on the network:

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. Click Start. The jitter data start to appear on the screen as shown here.



3. Click  to end the test. See the table below for information shown on the Jitter tool screen.

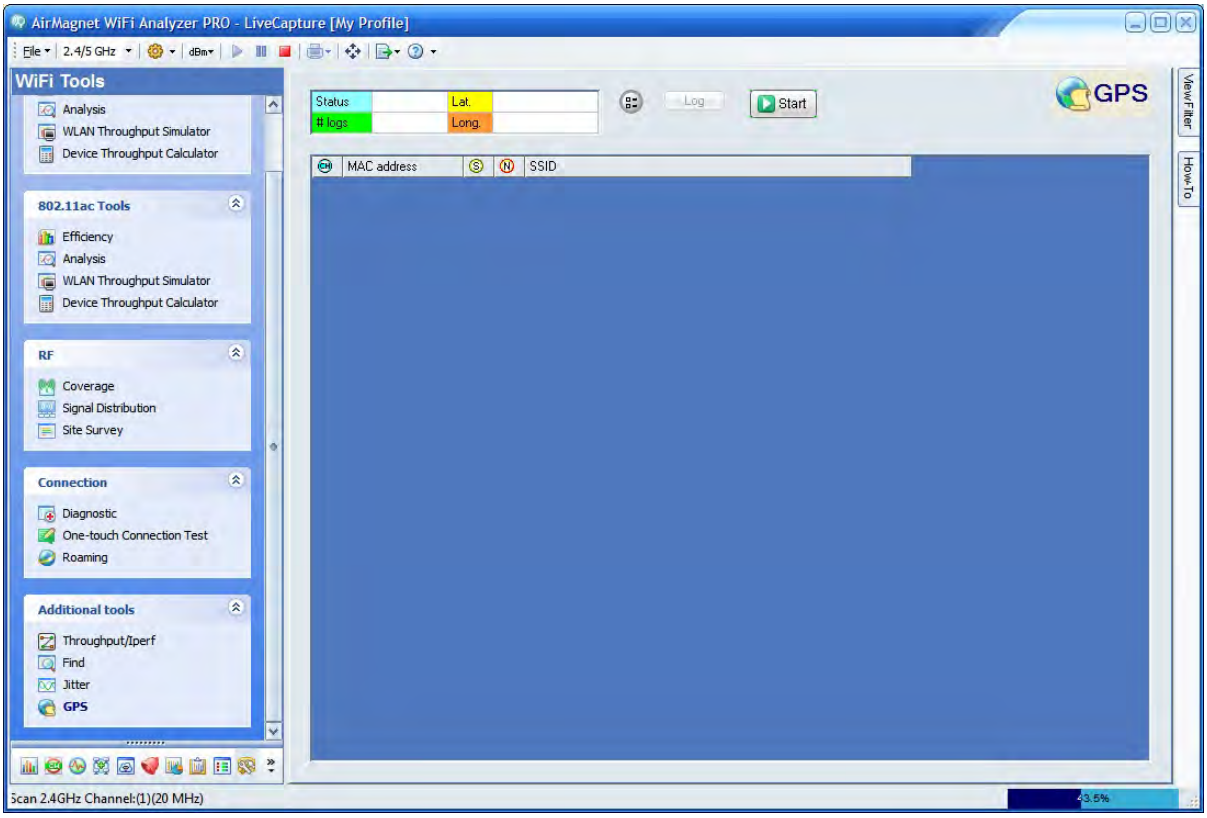
Parameter	Description
AP	The AP the station is associating with. Automatically detected.
CH	The channel the AP is operating on. Automatically detected.
Util	Channel utilization rate.
Noise	Noise level in dBm.
CRC%	CRC error rate.
DTIM	DTIM configuration on the AP.
In Pkts	Incoming packets from the AP.

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

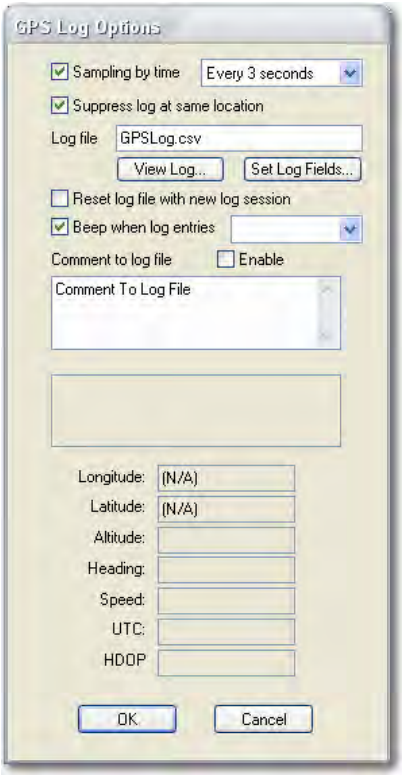
The GPS tool allows you to find the exact location of a device that AirMagnet WiFi Analyzer has detected on the network. The figure below illustrates AirMagnet WiFi Analyzer's GPS tool screen. Refer also to Configuring GPS Settings, Configuring GPS Options, and Using GPS Tool.

Note: *Prior to using the GPS tool, you must complete GPS configuration on the AirMagnet Configuration screen (**File>Configure>Profile**) and have a GPS device already connected to your laptop PC.*



Configuring GPS Options

In order to properly use the GPS and AirMagnet WiFi Analyzer integration, you need to configure GPS tool.



To configure the GBS tool:

1. From the GPS screen, click  **(GPS Options)**.

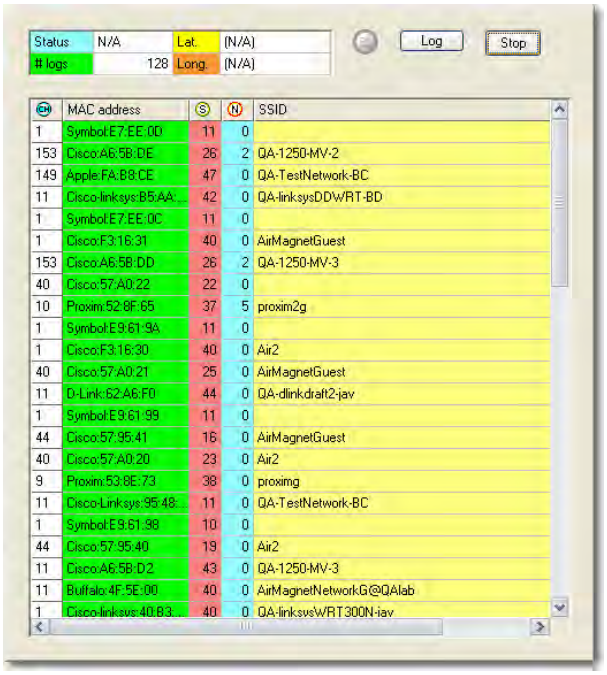
2. Make the desired selections in the dialog box.

3. Click **OK.**

Using GPS Tool

To collect GPS data:

1. From the GPS tool screen, click  . Data will start to appear on the screen. Refer to the example below.



2. Click  to end the operation.

Managing Data Files

About Managing Data Files

This section 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.

- 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

To expand the policy structure in the AirMagnet Policy Management screen:

1. Choose a policy group, for example, Security.
2. Select policy category in that policy group, for example, User Authentication and Encryption.
3. Select a subcategory of the selected policy category, for example, WPA-802.1x & TKIP.
4. Highlight a specific alarm under the policy subcategory, for example, 802.1x Rekey Timeout Too Long.

For detailed descriptions of AirMagnet WLAN policies, refer to the AirMagnet Wireless LAN Policy Reference Guide which is included on the software CD.

AirMagnet-Supported File Formats

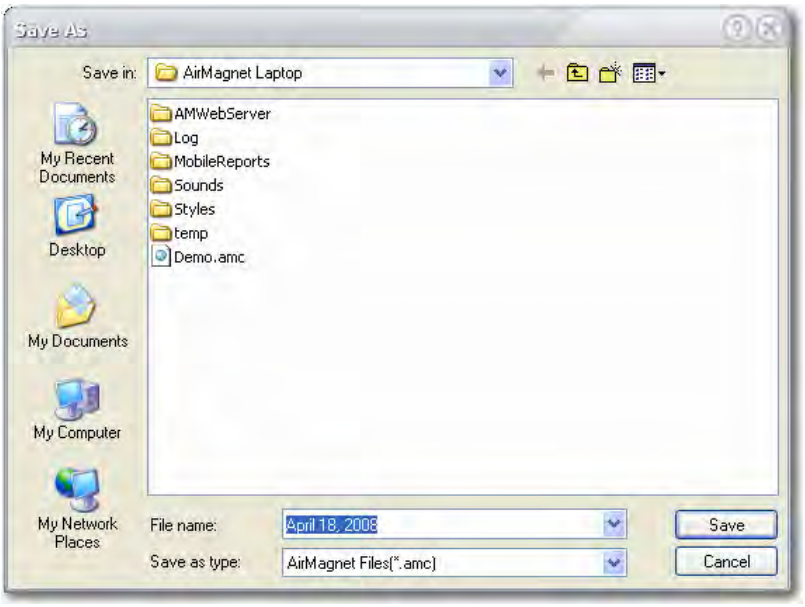
AirMagnet WiFi Analyzer supports the following file formats:

- ***.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.
- ***.ecp*** — 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.



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 Wi-Fi Analyzer* on your PC, using the date and time when the file is save 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**.

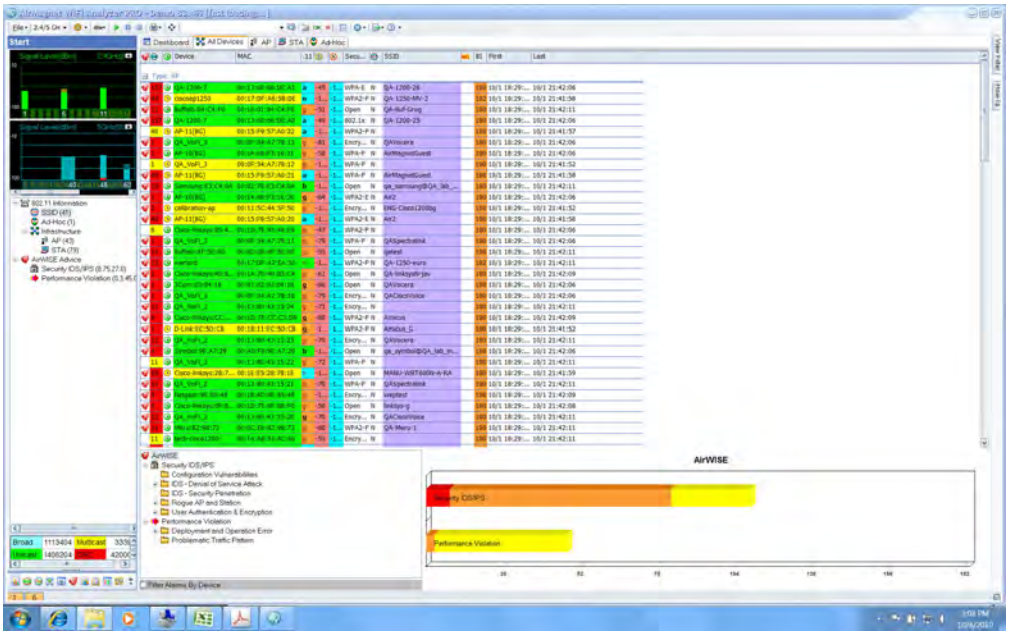
Opening a Saved File

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 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. 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.

To open a capture file:

1. Click **File>Open....** The *Open* screen appears.
2. Select the file, and click **Open.** The file data start to appear on the screen.



3. Wait until the value on top of the screen become 100% (meaning the data is completely loaded).
4. The live capture function is suspended while and after the file is (being) opened. To resume live capture, click  .

Note: *The figure above 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*

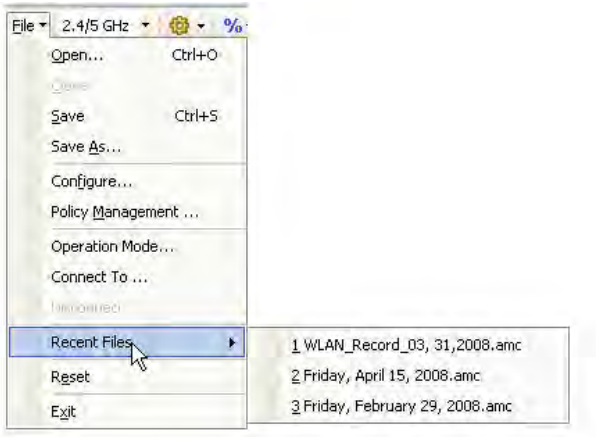
Capture File option when opening the trace file, the file loads instantly and you can see a lot more data as shown in the following figure.

Viewing Recently Opened Capture 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.



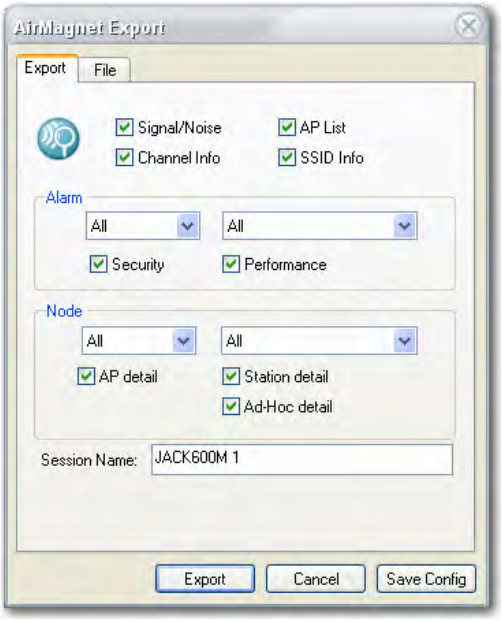
2. From the drop-down list menu, select a file to open it.

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 the database files:

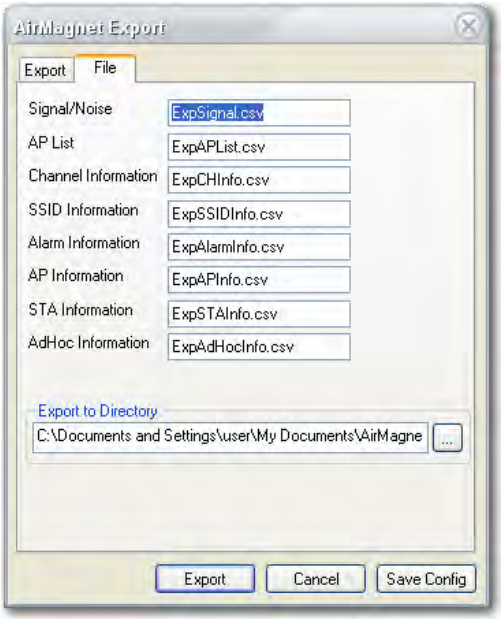
1. Click  **(Import/Export)** and select Export.... The *Export* screen appears.



2. Overwrite the **Session Name** with a name unique to the site where the data are collected.

Note: *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 opens another screen where you can modify the names of the files.

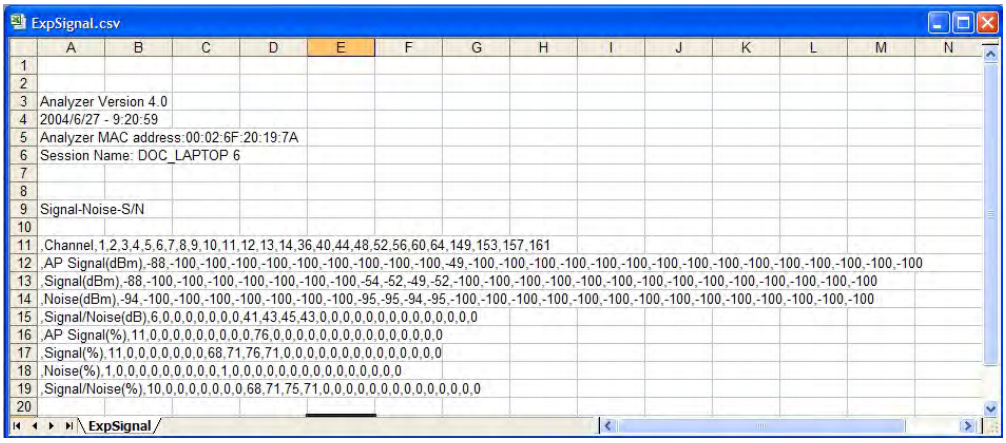


5. Rename the files, if you want to.
6. Specify a file path.

7. Click **Export**.

Note: *The file extension cannot be changed.*

.csv files can be opened in Microsoft Excel. The following figure shows a sample *.csv* file.

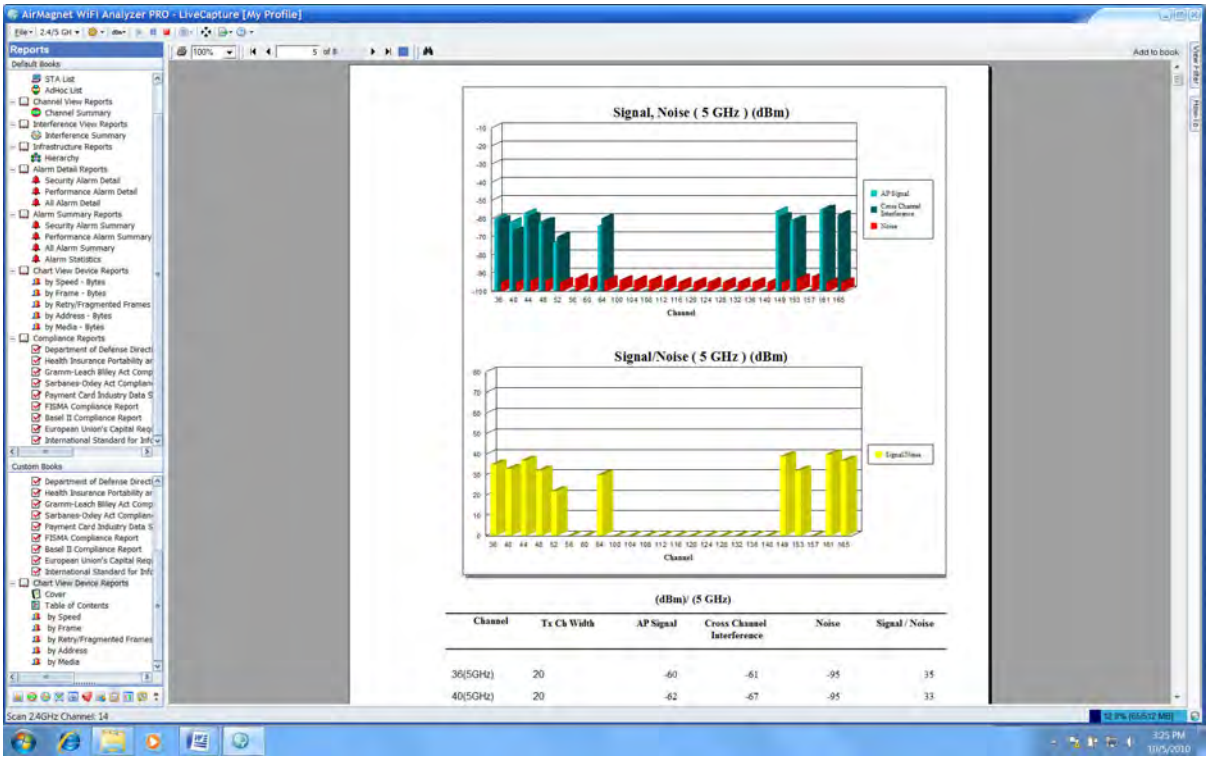


Reports Screen

About Reports Screen

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 user-selected reports. It provides a convenient way for organizing, sharing, and archiving data that are collected on your network. You can navigate to the Reports screen just by clicking 

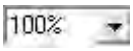
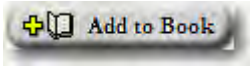
on the navigation bar. The figure below shows AirMagnet WiFi Analyzer's Reports screen.



Reports Screen Menu and Tool Options

The following table describes the menu and tools in the Reports screen:

Icon	Tool Name	Description

	Print	Prints the currently opened report.
	View Ratio	Allows you to set or change the view ratio of the report on the screen.
	To First Page (of a report)	Moves to the first page.
	To Previous Page	Moves to the previous page.
	Current Page of Total Number of Pages	Indicates the current page as well as the total number of pages of a report.
	To Next Page	Moves to the next page.
	To Last Page	Moves to the last page.
	Stop Loading	Stops Loading the selected report. ***Note:*** *This tool is used to abort an attempt to open a report.*
	Search Text	Opens the Search dialog box where you can key in the text to be searched for through the currently opened report.
	Add Report to Book	Adds the currently opened report to a (custom) report book.

Custom Books

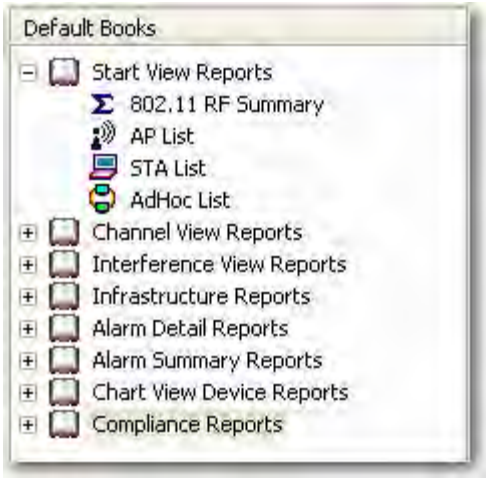
This section is located in the lower left-hand part of the Reports screen. It displays all custom report books that you have compiled. It also provides the tools for creating and managing custom report books.

You can perform the following tasks from this part of the Reports screen:

- Creating a Report Book
- Adding Reports to Book
- Modifying Book Properties
- Modifying Report Contents
- Deleting a Report or Report Book
- Modifying Book Properties
- Modifying Book Contents

Default Books

This section is located in the upper left-hand part of the Reports screen. It lists all reports that AirMagnet WiFi Analyzer automatically generated. The reports are based on data shown on some of the major screens.



Default Books has the following reports:

Start View Reports - Contains the reports based on data shown on the **Start** screen. You can directly access these same reports from the Start screen by clicking **(View Reports)** and selecting any of these reports from the list menu.

Channel View Reports - Contains the report based on data shown on the **Channel** screen. You can access this same report directly from the Channel screen by clicking and selecting either **Selected Channel** or **All Channels** from the list menu.

I**nterference View Reports** - Contains the report based on data shown on the **Interference** screen. You can access this same report directly from the Interference screen by clicking and selecting **Interference** from the list menu.

Infrastructure Reports - Contains the report based on data shown on the **Infrastructure** screen. You can access these same reports directly from the Infrastructure screen by clicking and selecting either **Selected Device** or **Hierarchy Summary** from the list menu.

Alarm Detail Reports - Contains reports based on alarm detail data shown on the **AirWISE** screen. You can access these reports from the AirWISE screen by clicking and selecting **Alarm Detail** and then any of the options from the list menu.

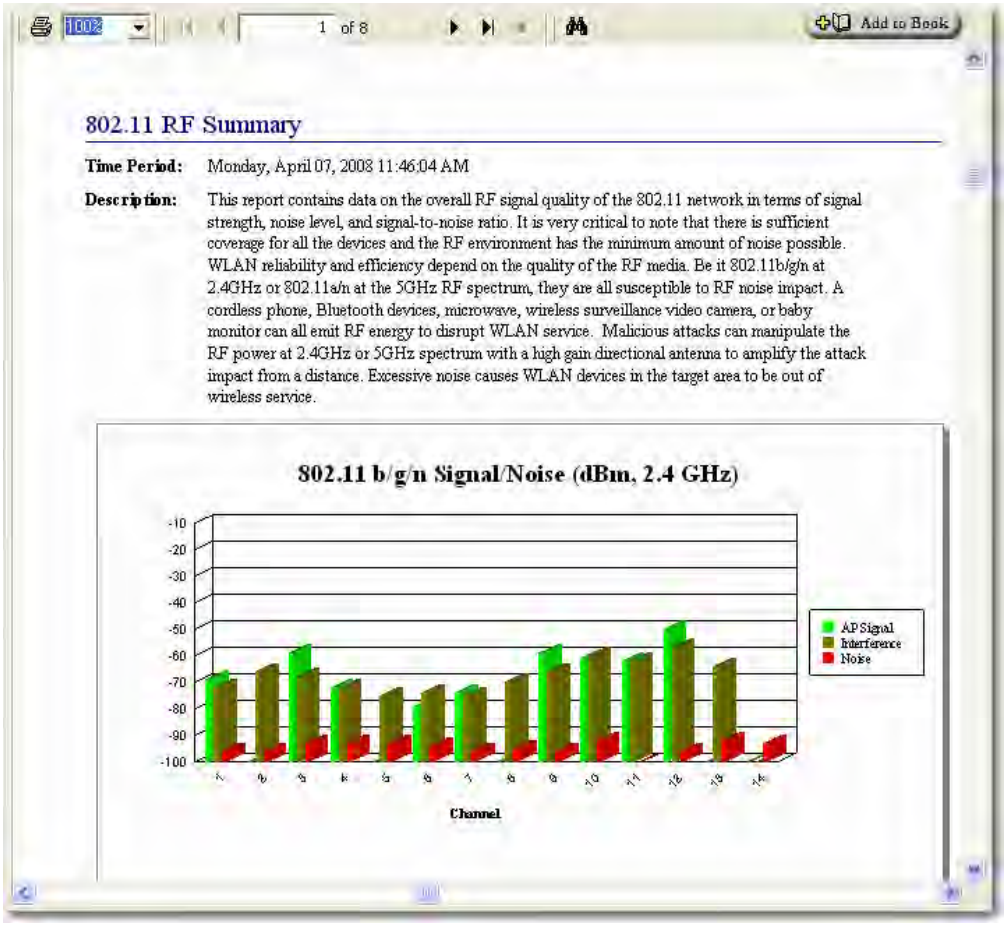
Alarm Summary Reports - Contains the reports based on alarm summary data shown on the **AirWISE** screen. You can access these reports from the AirWISE screen by clicking and selecting **Alarm Summary** and then any of the options from the list menu.

Chart View Device Reports - Contains the reports based on device data captured on your network.

Compliance Reports - contains the reports based on regulatory compliance status of your network.

Report Pane

The right-hand side of the Reports screen is the report pane which displays the content of the report being selected. The illustration below shows the report pane. It provides a number of tools for viewing the report. Refer to Reports Screen Menu and Tool Options.



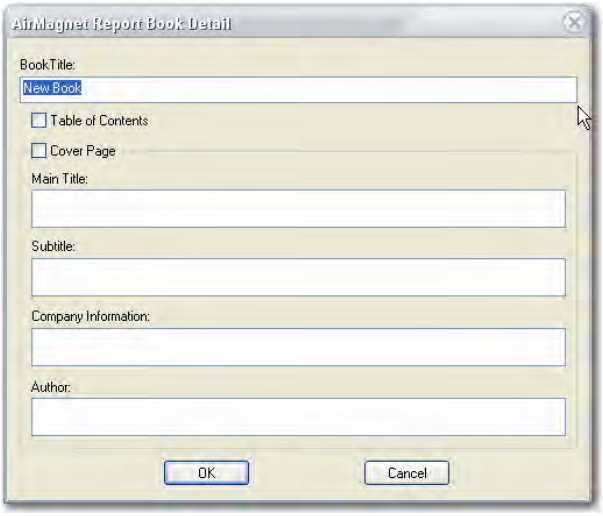
Creating a Report Book

You can create a report book using a custom cover page, table of contents, and reports of your own choice. It is a good way to categorize, share, and archive data that are captured on your network.

To create a report book:

1. Right-click the Custom Books section to bring up the right-click menu.

2. From the right-click menu, click **New Book....** The **AirMagnet Report Book Detail** dialog box appears.



3. In the AirMagnet Report Book Detail dialog box, make the entries and/or selections as described in the table below.

Entry/Selection	Description
Book Title	The title of the report book shown in the Custom Books section.
Table of Contents	If selected (checked), a table of contents will be automatically created. The table of contents is based on the reports that are added to the book, with each report forming an individual chapter. The number of entries in the table of contents equals to the number of reports added to the report book.
Cover Page	If selected (checked), a cover page will be automatically added to the report book. The cover page contains information as described

	below.
Main Title	The main title appears on the top of the cover page.
Subtitle	The subtitle appears below the main title on the cover page. It should help explain the main title.
Company Information	The information of the business entity that own the wireless network.
Author	The name of the person who created the report book.

4. Click **OK**. The book title (with its cover page and table of contents) appears in the Custom Books section.

Note: *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.*

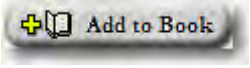
Adding Reports to a Book

There 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 adds 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, click to 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 

.

Adding Default Reports toa 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:

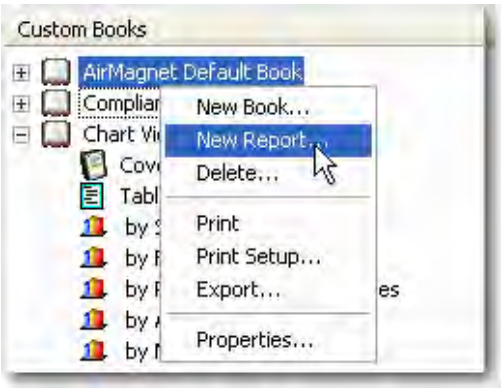
1. From the Default Books section, select a report of interest and drag and drop it directly to the book.
2. Repeat Step 1 until all relevant reports are added to the book.

Adding Custom Reports to a Book

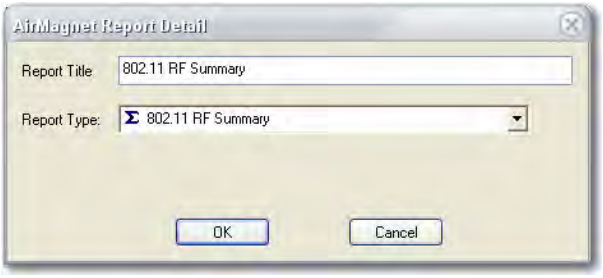
This section describes the procedures for adding custom reports to a report book. It differs from the other methods in that it allows you to custom the reports before adding them to the report book.

To add a custom report to a report book:

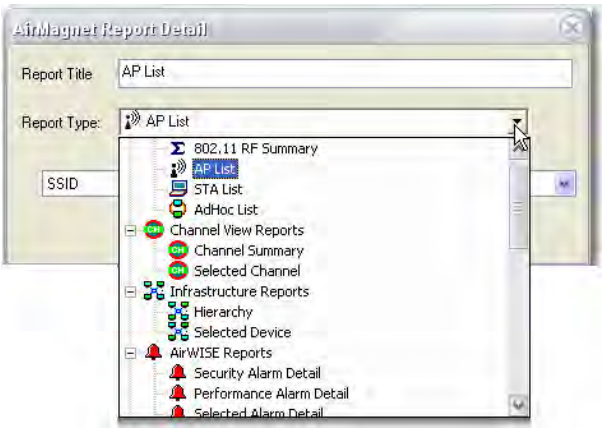
1. In the Custom Books section, right-click the title of the book of interest. The right-click menu appears.



2. From the right-click menu, select **New Report....** The **AirMagnet Report Detail** dialog box appears.



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.



Note: *From here on, the dialog box may look different depending on the report you select. Some reports 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.

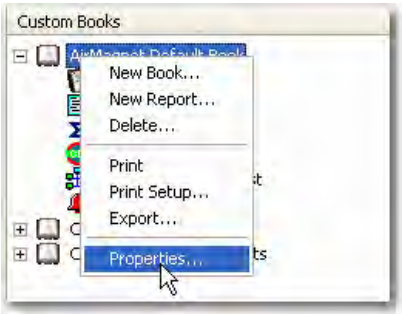
Modifying Book Properties

Modifying the properties of a report book means making changes to the information on its cover page.

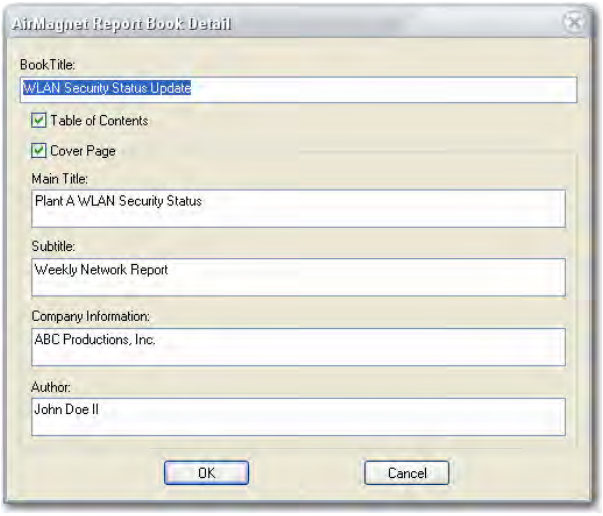
Note: *This applies only to report books in the Custom Books section.*

To modify the properties of a report book:

1. From the Custom Books section, right-click the report book of interest.



2. From the right-click menu, select **Properties....** The **AirMagnet Report Book Detail** dialog box appears.



3. Make the desired changes and click **OK.**

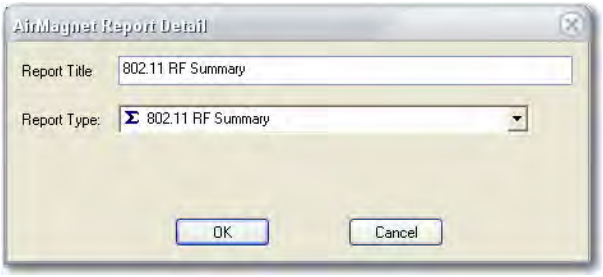
Modifying Book Contents

Modifying the content of a report book means making changes to data contained in the report by using different filters.

To modify the content 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.



3. Make the desired changes and click **OK.**

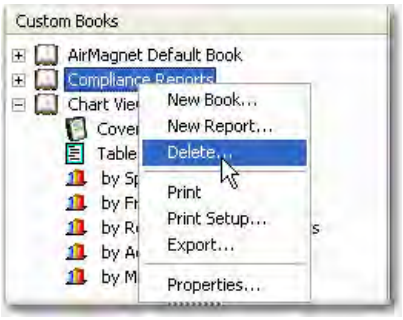
Delete a Report or Report Book

The Custom Books section can become overcrowded as more report books are created. To clean up this part of the user interface, you may want to delete those reports or report books that are out of date.

Note: *You can only delete reports or report books in the Custom Books section; nothing can be deleted from the Default Books section.*

To delete a report of report book:

1. In the Custom Books section, right-click the report or report book. The right-click menu appears.



2. From the right-click menu, select **Delete....** A confirmation message appears.
3. Click **Yes.**

Printing a Report

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).**

Note: *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.*

To print a report (Custom Books only):

3. From the Custom Books section, right-click the report of interest.

4. From the right-click menu, click **Print.**

Note: *The right-click menu is available only in the Custom Books section of the Reports screen.*

Exporting a Report

The reports or report books in the Custom Books section of the Reports screen can be exported in any of the file formats:

- Adobe PDF
- HTML
- MS Word
- XML

To export a custom report or report book:

1. From the Custom Books section, right right-click the entry of interest.

2. From the right-click menu, select **Export....** The Export dialog box appears.

3. From the Export dialog box, select a file format, specify a export path, and click **OK.**

Viewing a Report

You can view any report shown in either the Default Books or the Custom Books section of the list of reports simply by clicking a report of interest. Refer to Report Pane.

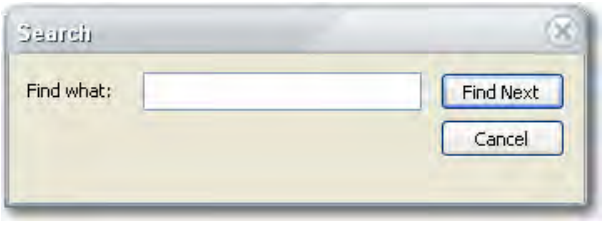
Note: *The time it takes for a report to open in the report window varies depending on the size of the report.*

Using the Report Search Tool

You can conduct text-based searches through a report using  (Search Text), which allows 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.



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. To continue searching, click **Find Next** until you reach the end of the report.

Compliance Reports

Compliance reports provide you with an easy-to-view summary of your network's compliance with various industry standards.

Note: *The PCI Compliance Reports and HIPAA Compliance Report can be used as introductory Executive Summaries for their respective reports or they can be used as stand-alone Executive Summary reports.*

Disclaimer

Please note that AirMagnet's customers are responsible for ensuring their own compliance with applicable laws and regulations. While the AirMagnet Policy Compliance Reports provide information about the law and are designed to help you satisfy government regulations, such information is not legal advice, and it is your sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant law or regulation.

Important Disclaimer: NetAlly does not represent or warrant that its services, products or any other information it provides to a customer will ensure that you are in compliance with any law or regulation.

Types of Compliance Reports

Department of Defense Directive 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.

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.

Gramm-Leach Bliley Act

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.

Sarbanes-Oxley Act

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.

Payment Card Industry Data Security Standard (PCI)

The Payment Card Industry Data Security Standard (PCI) version 3.0 is intended to supersede Version 2. AirMagnet includes both PCI 2.0 and 3.0 compliance reports.

These compliance reports provide information to assist an assessor in determining whether the organization complies with PCI DSS requirements standard applicable to wireless networks and devices operating in the unregulated radio frequencies (2.4 to 5 GHz).

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.

EU CRD/CAD3

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.

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 organizations 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 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.

FISMA

FISMA (Federal Information Security Management Act) 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:

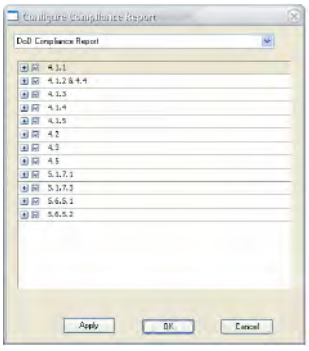
- All information in the Federal government except information marked as classified.
- All information systems except those operating as national security systems.
- Any organization that is a government agency, sells hardware and/or software to a government agency, or supports the information or information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

Customizing Compliance Reports

If the data reported by the existing compliance reports provided by AirMagnet don't match the requirements of your corporate network, you may customize the information used by each type of compliance report. The ability to configure specific report information can help you to tailor Enterprise's reporting abilities to the needs of the company.

To customize compliance report data:

1. From the Console's **Reports** screen, click  (Config Compliance Report). The Configure Compliance Report dialog box appears.



2. Use the drop-down box at the top of the window to select the compliance report to be customized. The lower pane displays all the sections in the selected report.
3. Use the "+" (expand) option to expand each section. This will reveal the alarms reported on a section-by-section basis.
4. Uncheck the alarms that should not be included in the report.
5. Click **Apply** to save the changes, and click **OK** to close the dialog box.

49 GHz Band

About 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 (that is, 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. On the other hand, secondary operations 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, you must use one of the following 4.9-GHz wireless network adapters:

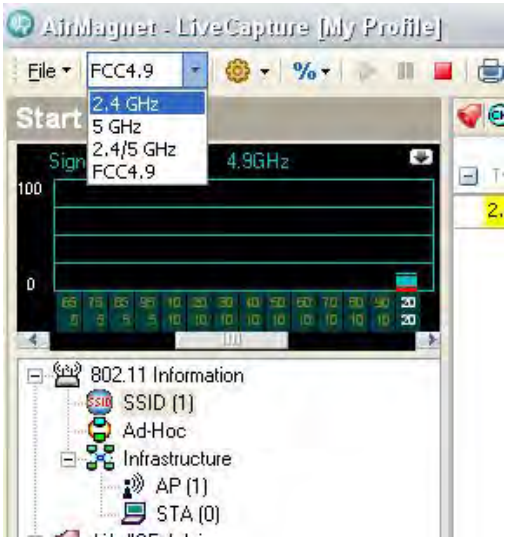
- Linksys Wireless A+G Notebook Adapter WPC55AG version 1.3
- Ubiquiti SR4C 4.9 GHz

- TRENDnet TEW-501PC ag

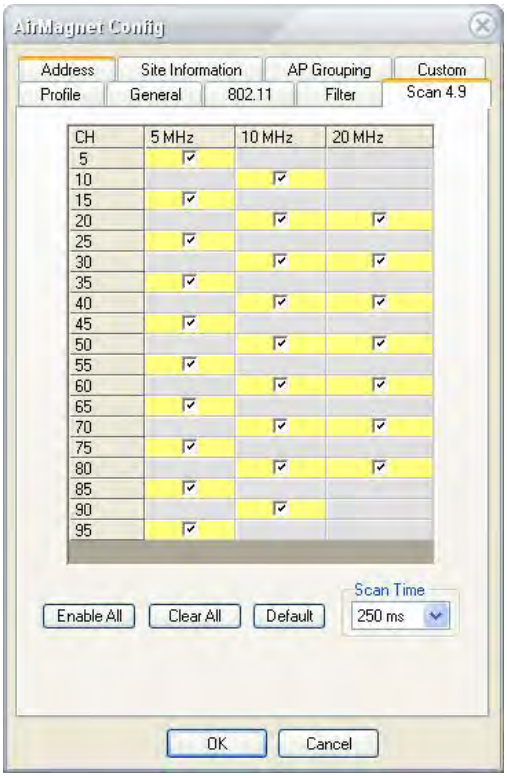
Setting AirMagnet WiFi Analyzer in 4.9-GHz Mode

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 menu bar, click the Band button and select FCC 4.9 from the drop-down list. See the figure below.



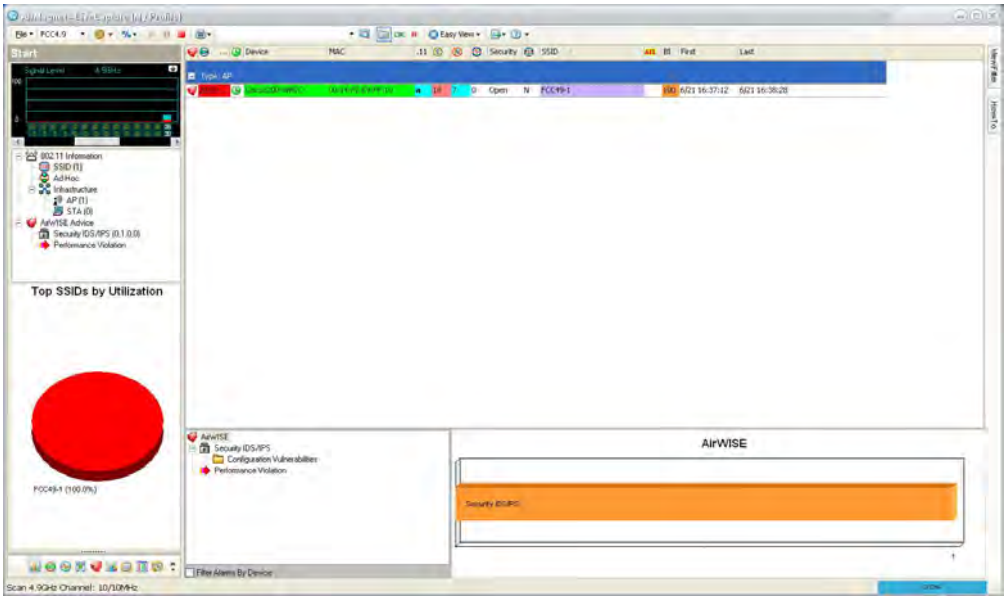
4. Click **File>Configure...>Scan 4.9**. Refer to the figure below.



Note: *The figure above 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**.

Note: *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. The figure below shows the Start screen in 4.9-GHz mode.*


Top SSIDs by Utilization
AirWISE

Solving 802.11n Issues

About Solving 802.11n Issues

This section discusses how to use AirMagnet WiFi Analyzer to monitor, troubleshoot, and resolve 802.11n-related issues on the network.

- 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 sse to support legacy devices?
- How will associated legacy devices decrease 802.11n device throughput?
- How many legacy APs can be added to an 802.11nnetwork?
- How will 802.11n STAs affect an existing 802.11a network?

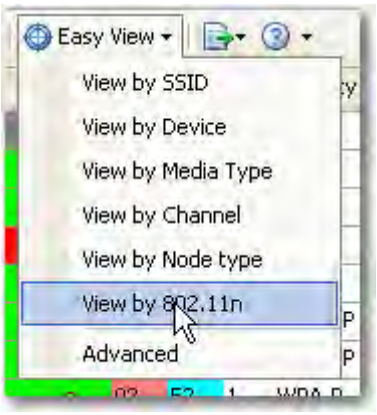
How to Find Out 802.11n Features on an AP?

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.

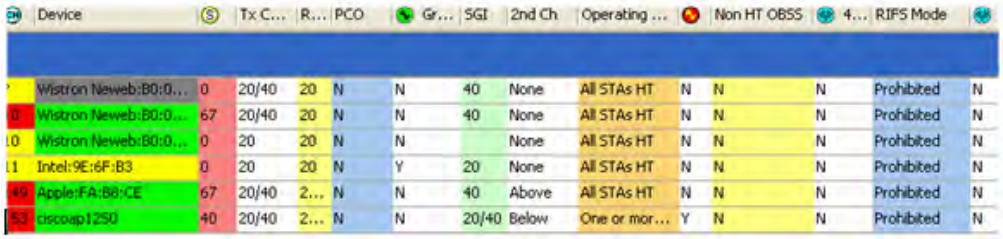
To find out the 802.11n features used on an AP:

1. Open the Start screen.
2. From the men ubar, click 

and select View by 802.11n from the drop-down menu.



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.



Note: *To make it easy to know all 802.11n features 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:

- 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

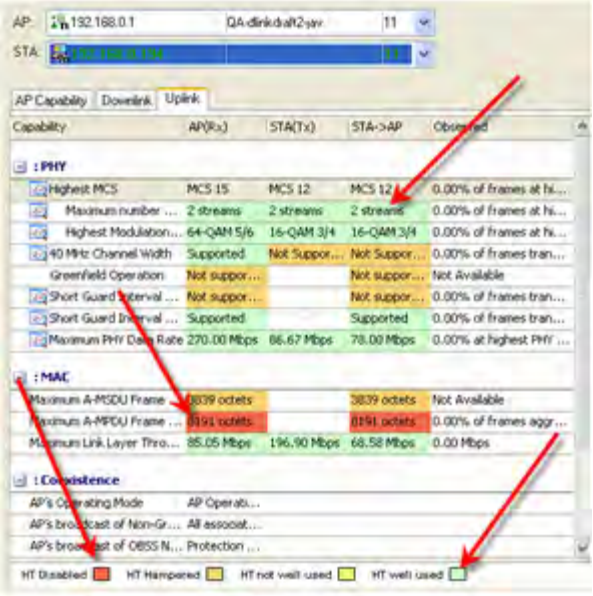
Note: *You can get a quick definition or explanation of any of these terms simply by enabling Bubble Help by clicking*  *in the menu bar. Once the Bubble Help is enabled, you can simply mouse over the name of any of the column to get a tool tip for it.*

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 you 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.



3. From the Efficiency screen, select an AP or STA of interest.

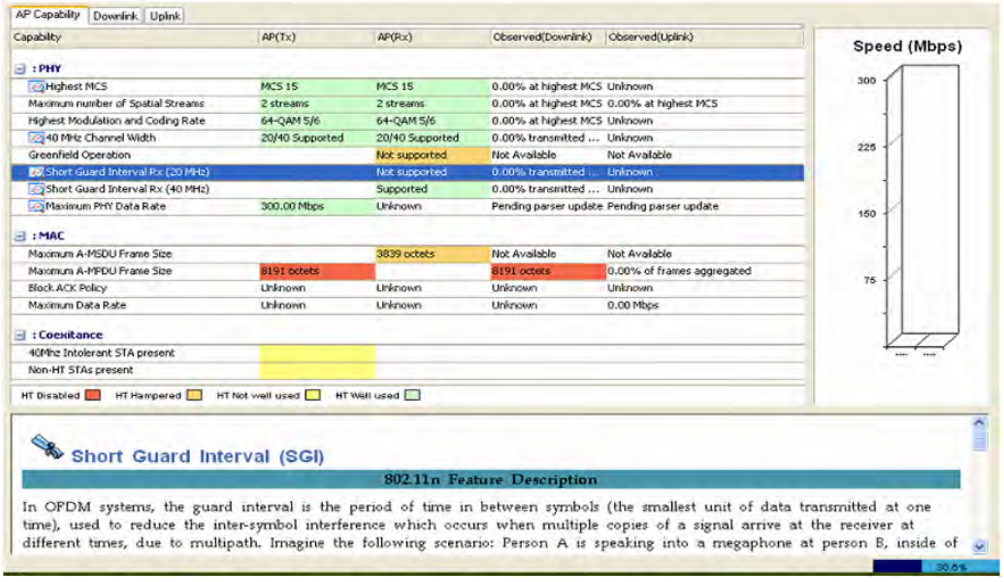
Note: *The Efficiency screen provides detailed description of all 802.11n features in three categories: PHY, MAC, and Coexistence. For instructions on how to use the Efficiency screen, refer to Analyzing 802.11n Network Efficiency.*

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.

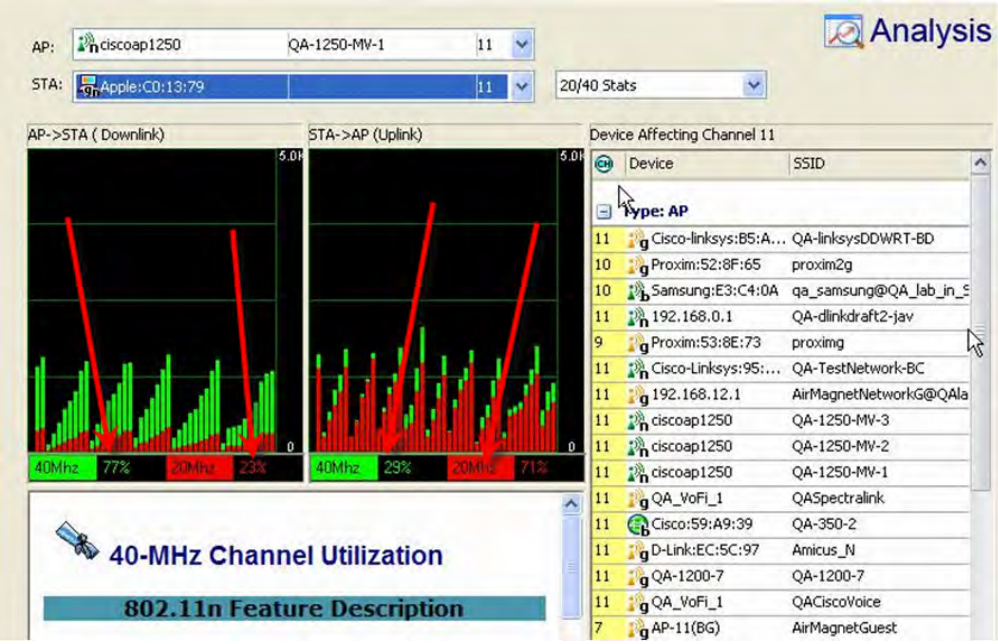


How Much Traffic Is Sent Using 40-MHZ Channel Width?

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.



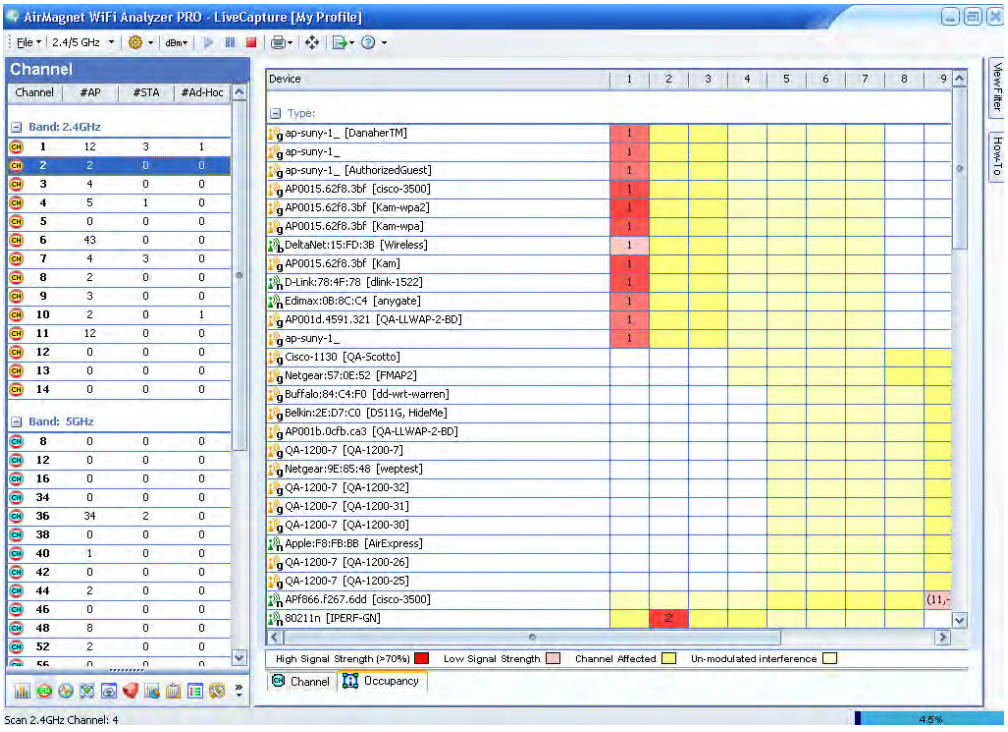
Note: *The Analysis screen displays the percentage (%) of 20- or 40-MHz traffic between the selected AP and STA. It also provides statistics on SGI, A-MPDU, MCS Index, PHY Data Rate Analysis, and so on. For more information, refer to About 802.11n Tools.*

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. Click the **Occupancy** tab.



Note: *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 provides vital information needed for making well-informed decision when planning for new network deployments or enhancement of existing installations.*

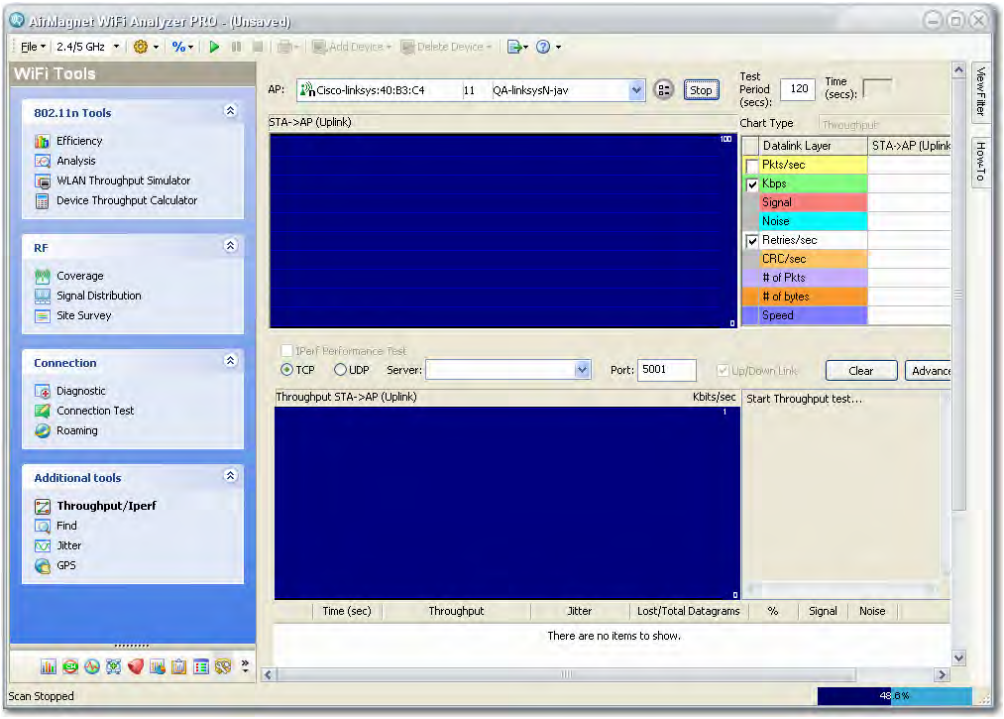
The occupancy status of all the available channels shown on the Channel/Occupancy screen help you easily decide which channels to choose for new APs to be deployed on a congested network. As a rule of thumb, you should choose the unused channels and avoid the congested ones.

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, for example, 120.
3. Select a Chart Type, efor example, 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 Start.



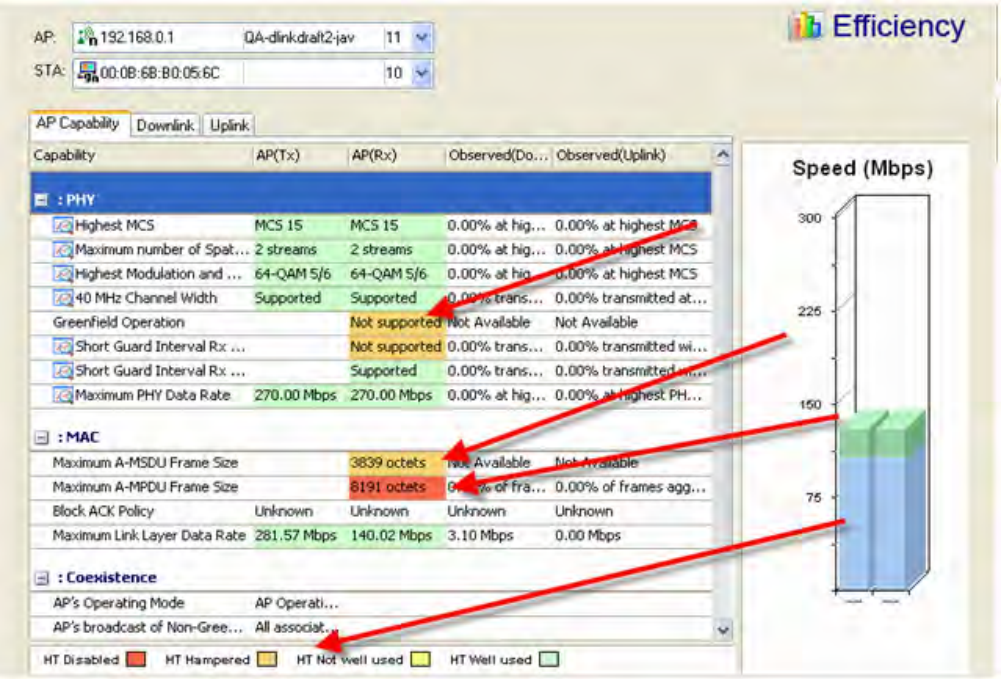
Note: *The Throughput/Iperf screen shows both the up and downlink throughput for the selected AP. It allows you to test the network performance using either the TCP or the UDP protocol. It shows various factors such as signal strength, noise level, retries, and CRC errors that may impact your network throughput. For more information, refer to* *Analyzing Network Bandwidth and Throughput with Iperf*.

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.

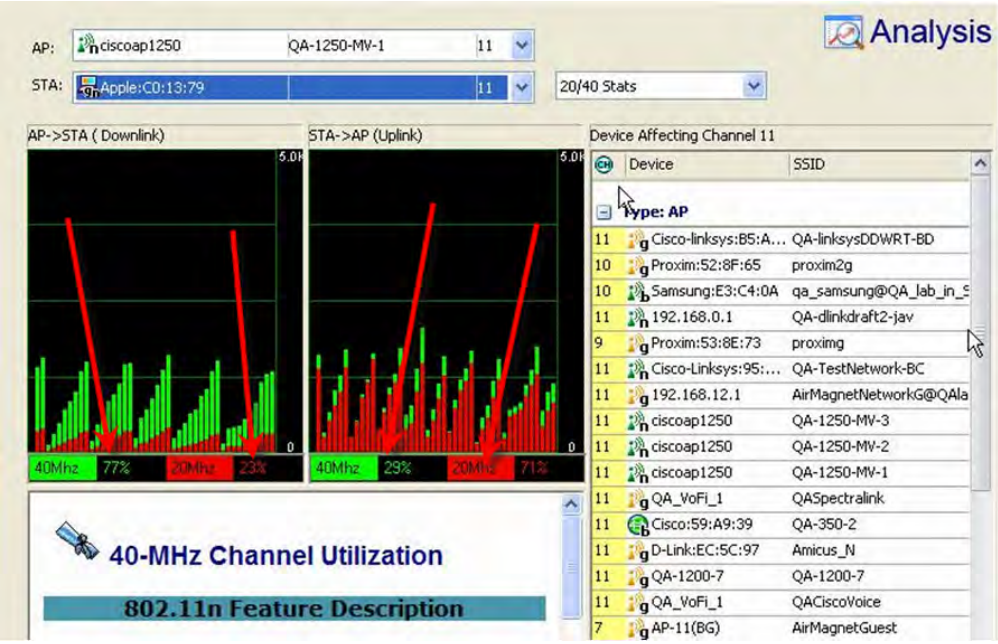
To find out why you are not getting the expected throughput from an AP:

1. Open the **Efficiency** screen.



Note: *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, refer to [802.11n Efficiency](#).*

2. Open the **Analysis** screen.
3. Select an AP and a STA.
4. Select 20/40 Stats.



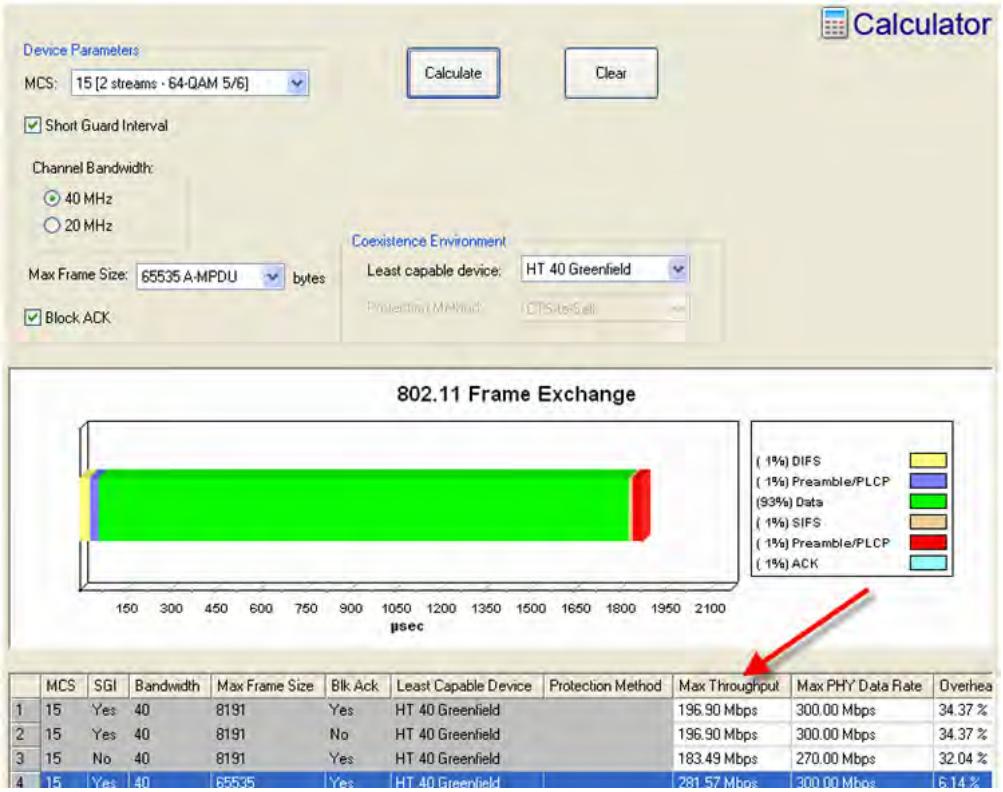
The view indicates the percentage of traffic being sent at 20 MHz and at 40 MHz. It can detect if utilization at higher MCS rate is low. It also indicate low signal-to-noise ratio in noisy RF environments or over greater distance between AP and STA.

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:

1. Open AirMagnet WiFi Analyzer's Device Throughput **Calculator** screen.
2. Set the parameters you want to use on the AP and click Calculate.
3. Repeat Step 1, using different parameters.



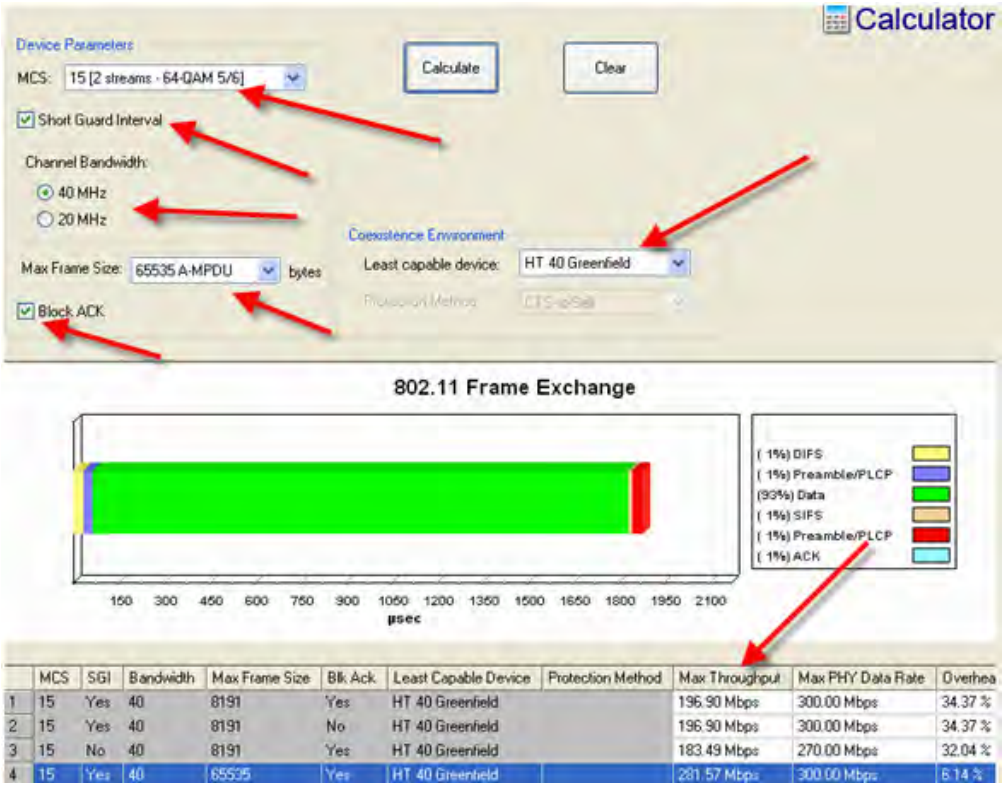
Each time you click **Calculate**, AirMagnet WiFi Analyzer calculates the theoretical throughput level you can expect from an AP using the same parameters. This can help you set realistic expectations for a newly deployed AP because the calculations are based on parameters you specified on the AP. The 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 the following figure.

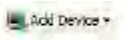


All the fields highlighted in the previous figure are considered very important for the 802.11n network and must be taken into consideration when purchasing or configuring 802.11n AP. They help you make informed decisions to maximize throughput of your 802.11n devices or networks.

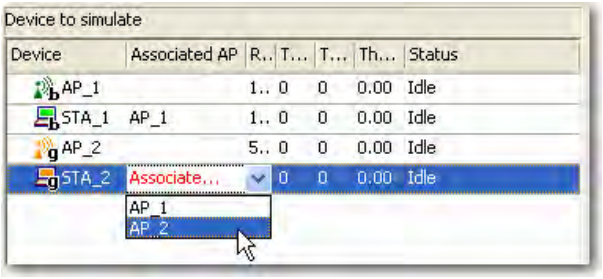
What Change in Network Throughput Is Expected When Deploying New APs and/or STAs on the Network?

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 (that is, APs, STAs, and so on) 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 menu bar, click 

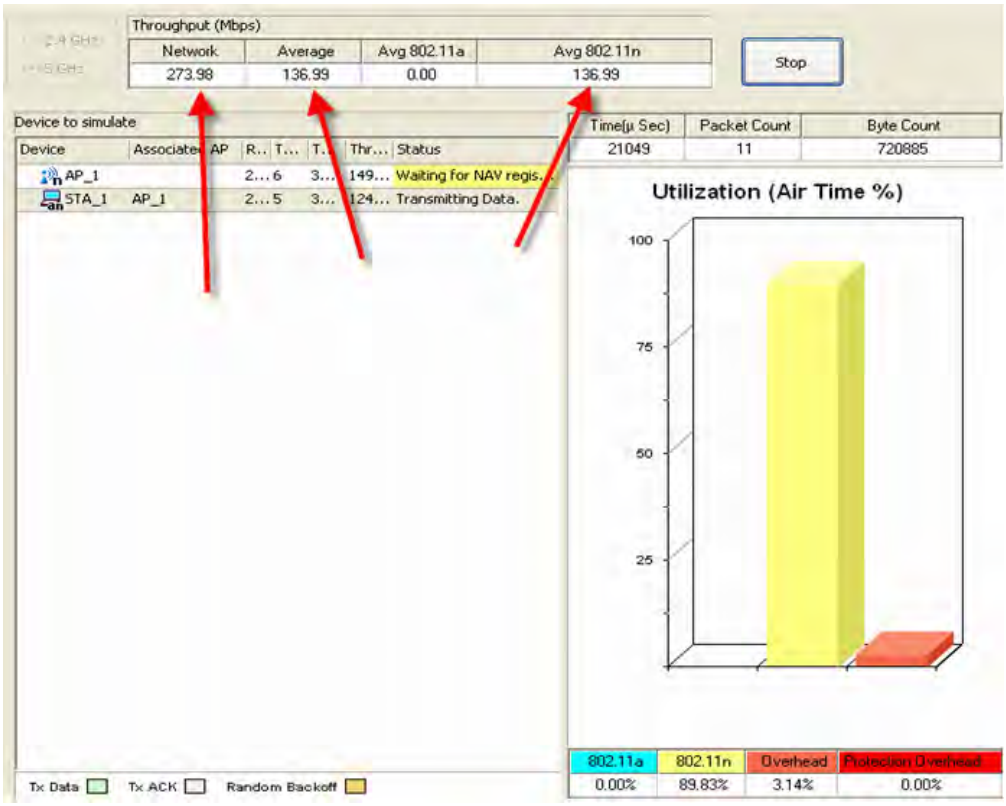
and select an option from the drop-down menu.
4. Associate STAs with APs by clicking an STA and then the down arrow next to it to select an AP to associate with, as shown in the following figure.



5. Repeat Step 3 to make sure that all APs and STAs are associated.

> ***Note:*** *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.



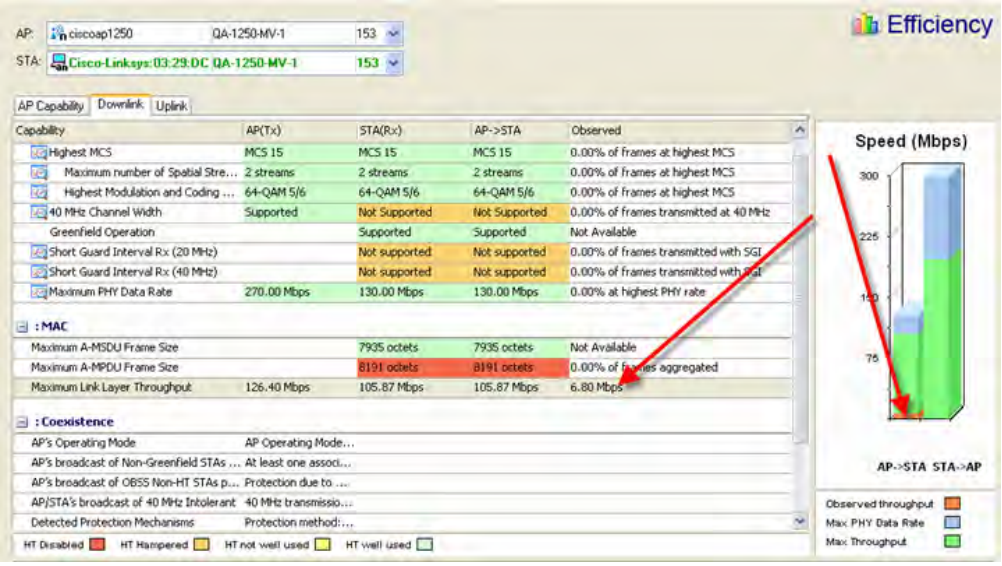
The Network Throughput Simulator allows you to simulate WLAN throughput under various user-defined conditions. You can simulate the impact on the network caused by addition of new APs and/or STAs by associating STAs with simulated APs or real APs that are installed on the network. The Simulator will generate the results and make them available on the screen in no time.

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.



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.

The Observed (Downlink) and Observed (Uplink) columns in the previous figure 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 (that is, 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 (that is, 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 (that is, 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 802.111n specification.

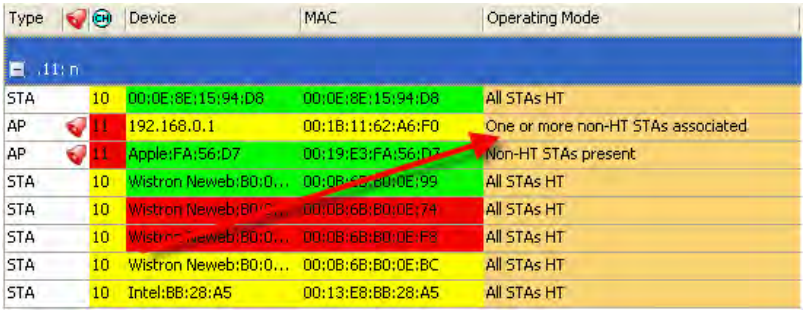
How Can I Know If My 802.11n AP is Associated with Any Legacy Devices?

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 minimized or avoid the potential negative impact that the 802.11n network make 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.

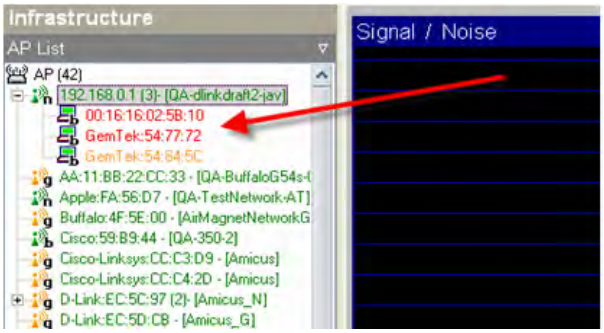
To know if your 802.11n APs are associating with legacy devices?

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.



- Open the Infrastructure screen, click **AP List**, and expand an 802.11n AP that has STAs associated to it.

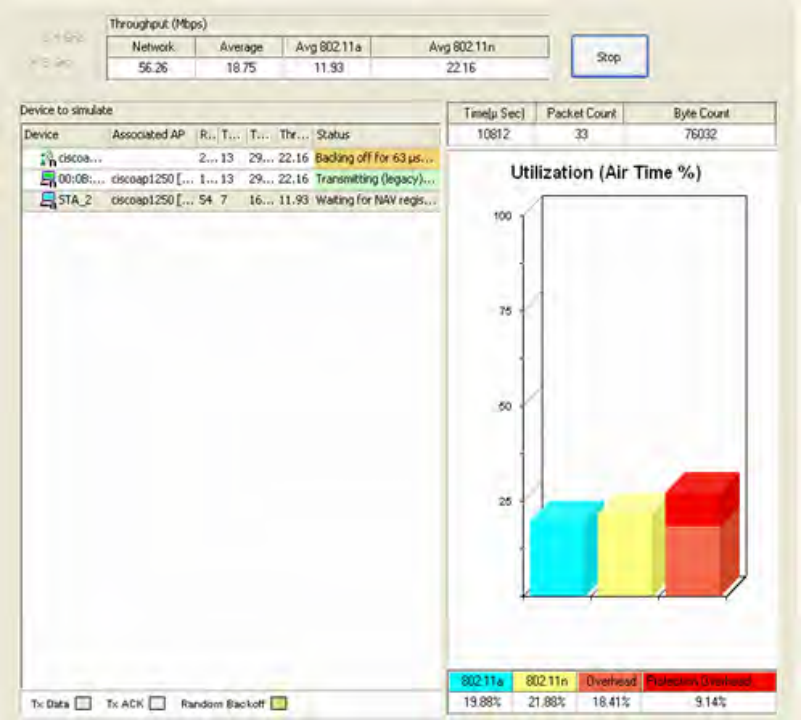


How Much Overhead Does an 802.11n AP Use to Support Legacy Devices?

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 **Network Throughput Simulator,** select 2.4 GHz or 5 GHz, and click Run.



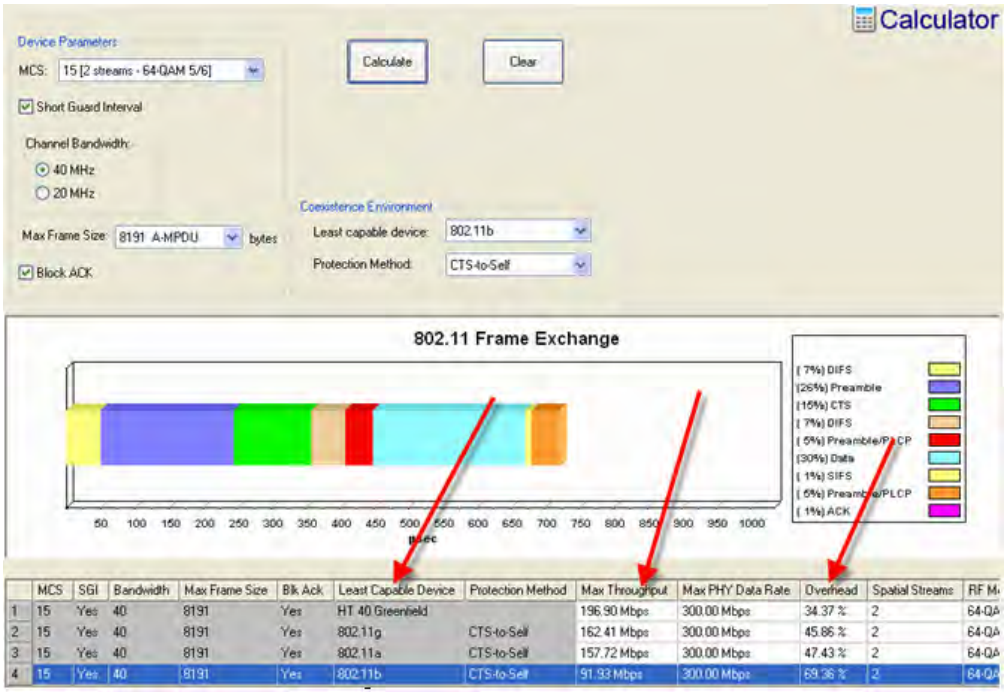
The Simulator allows you to simulate WLAN throughput under user-defined conditions. It allows you to visualize the overhead used by 802.11n APs in support of legacy devices as well as overhead used to protect 802.11n transmission from legacy devices.

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:

1. Open the Device Throughput **Calculator** screen.
2. For (Coexistence Environment) Least Capable Device, select 802.11b and select a Protection Method.
3. Click **Calculate**.
4. Repeat Steps 2-3 to calculate the impact in various conditions.



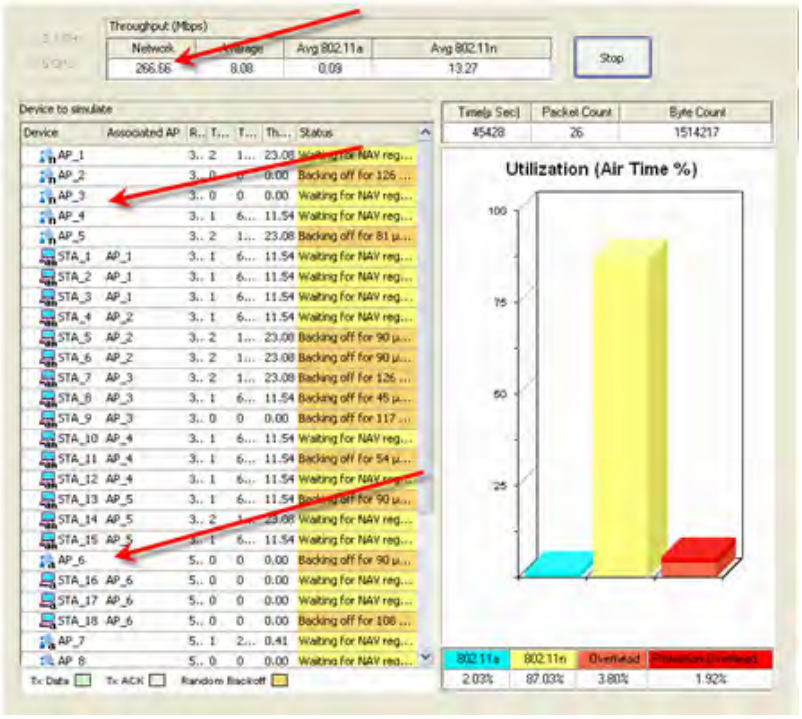
The Device Throughput Calculator tool screen allows you to calculate 802.11n device throughput, taking into consideration of those least capable devices on the network. It also shows the increase in overhead to accommodate for legacy devices.

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.



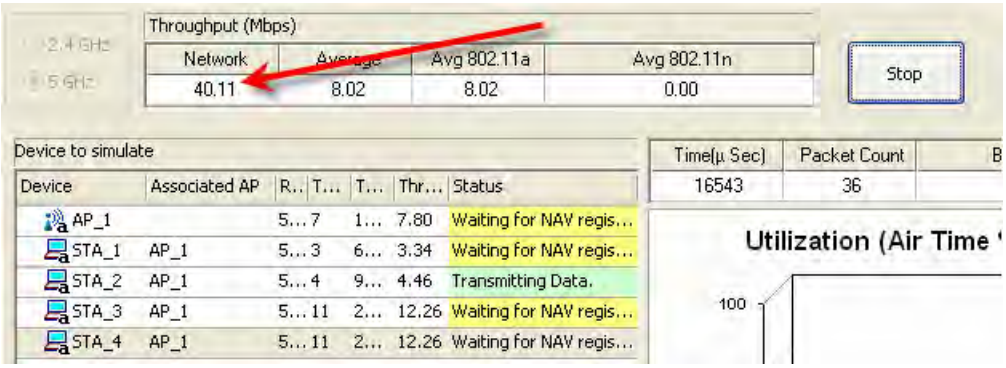
The Network Throughput Simulator tool calculates the throughput values at both the node and network levels, taking into full consideration of least capable devices in the network. It also simulates the impact on the 802.11n network caused by the addition of legacy APs, which can be easily visualized as more and more legacy devices are being added.

How Will 802.11n STAs Affect an Existing 802.11a Network?

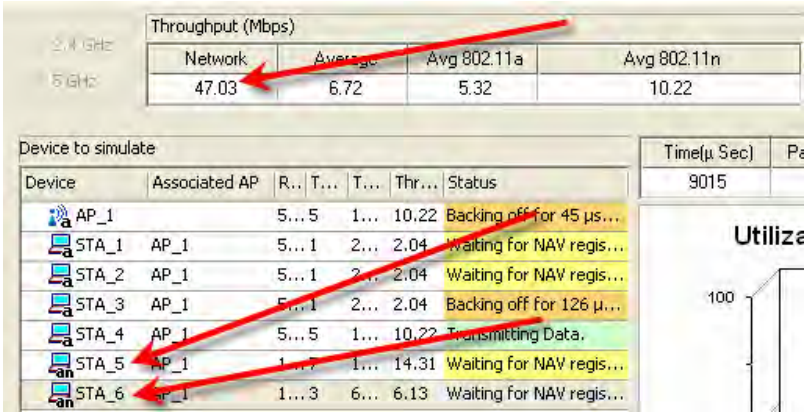
When 802.11n STAs are added to an 802.11a network, the overall throughput of the 802.11a network will increase, since they both support some of the latest 802.11 network technologies. This can be seen easily using the Network Throughput Simulator tool.

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.



3. Run a few simulations by associating 802.11a/n stations with the same 802.11g network and notice the network throughput.



As shown in the figures above, 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%.

Reference

Abbreviations and Acronyms

This section lists the abbreviations and acronyms used in this document. The definitions for many of these terms is provided in the Glossary.

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
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. Refer to 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
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
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired-Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

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.

802.11ac

IEEE 802.11ac is a wireless computer networking standard of 802.11, providing high-throughput wireless local area networks on the 5 GHz band.

Theoretically, this specification will enable multi-station WLAN throughput of at least 1 gigabit per second and a maximum single link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to 8), multi-user MIMO, and high-density modulation (up to 256 QAM).

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 (for example, 802.11x, EAP, and RADIUS) and strong security with the AES-CCMP encryption protocol. Also known as WPA2.

802.11n

IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard that provides a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz.[1][2] 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements, among other features.

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 (for example, 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, and so on.

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 (that is, Channels 1-14) in the 2.4 GHz band (that is, 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, for example, ISDN routers, modem routers, and so on 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, that is, 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 (for example, 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 (for example, 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, Wi-Fi 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 (that is, 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, for example, a laptop, PDA, and so on

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.

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.

Wi-Fi 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 though 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.

License and Copyright

GENERAL TERMS AND CONDITIONS

(v01-Oct-19)

These General Terms and Conditions ("General T&Cs") are by and between the legal entity set forth in the applicable Order (“Company”), as further defined below, and sets forth the terms, conditions, rights and restrictions for which LinkRunner, LLC d/b/a NetAlly, and any of its subsidiaries and affiliates (collectively or individually referred to as "NetAlly") is willing to sell devices ("Hardware") and license NetAlly’s proprietary software, as well as any firmware residing on such Hardware, ("Software") (The Hardware and Software may be collectively referred to as the "Product(s)"), and provide maintenance and technical support services ("Maintenance"), to Company. Unless otherwise governed by a signed contract between Company and NetAlly, only these General T&Cs will apply to any Orders made for NetAlly’s Products. NetAlly’s provisioning of Products, Maintenance or any other services to Company is expressly contingent upon Company’s acceptance of these General T&Cs, “AS IS”.

Receipt without return of any Products from NetAlly by Company shall be deemed as acceptance of this Order and shall also constitutes Company's confirmation that the Products descriptions, quantities, term, and prices set forth in the Order accurately represent Company's intended purchase. All additional and conflicting terms and conditions presented with or in any communication, including but not limited to those set forth in any P.O., except with respect to price, quantity, and location are hereby rejected, and shall be deemed null and void.

1. Definitions.

“API(s)” means the software application interfaces and workflow methods made generally available by NetAlly in certain Products to enable integration, implementation, and interoperability with third party hardware and software.

“Company” means a valid legal entity, in good standing, which has entered into a commercial agreement with NetAlly, allowing for the licensing or re-licensing of Software or distribution, sale, or resale of Products and Service.

“Company Data” means information that Company uploads or uses in conjunction with Company’s use of the Products.

“Data Protection Act” means the Health Information Portability and Accountability Act (HIPAA) (29 U.S. Code § 1181, et seq.), Gramm Leach Bliley Act (GLBA) (15 U.S Code § 1681), General Data Protection Regulation (GDPR) (EU 2016/679), and other applicable regulations which seek to protect the processing and storage of personal information.

“Documentation” means any installation guides, reference guides, operation manuals and release notes provided with the Product in printed, electronic, or online form.

“Evaluation Product” means software that contains a license key, which disables the Software after 30 days, or other term as agreed to by the parties, and which will render the Product unusable.

“Order" means the combination of Company’s P.O., a Quote issued by NetAlly or a NetAlly Company, and these General T&Cs.

“Personal Data” means any information relating to an identified or identifiable natural person (hereafter a “Data Subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

“P.O.” means a purchaser order or document, in tangible or intangible form (e.g. .rtf, .pdf, formats, etc.), issued by Company indicating Company’s acceptance of the Quote and these General T&Cs, without regards to any conflicting terms and conditions presented therein, except with respect to price, quantity, and location of Products or Services.

“Quote” means the document under which NetAlly offers for sale and licenses its Products, Maintenance, and other services.

“Services” means Maintenance as well as any other services offered by NetAlly to Company from time to time.

2. Shipment & Delivery Terms. NetAlly ships all Products hereunder FOB Origin. Unless otherwise agreed to by the parties, all shipments will be made using the carrier designated by Company. If Company does not designate a carrier, NetAlly reserves the right to choose a carrier at Company's expense. For Software available for electronic download, delivery will be deemed to have occurred once NetAlly has made the Software available for download by Company or Company’s designate agent or representative. Unless otherwise stated conspicuously on the face of the applicable Order, NetAlly reserves the right to fulfill Orders via multiple shipments. For all Products shipped internationally, Company will be the importer of record. Company agrees that it will not remove any NetAlly General T&Cs or other agreement from the NetAlly Product(s), and/or associated packaging.

3. License Grant and Restrictions. Subject to payment of the applicable license fee and the terms set forth in an applicable Order, NetAlly grants Company a limited, non-exclusive, non-transferable, revocable license to use the Software and the Documentation for Company’s own internal business purposes.

(a) Evaluation License: NetAlly hereby grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Evaluation Product set forth in the applicable NetAlly Evaluation Request Form solely for internal testing, evaluation, or demonstration purposes. If Company chooses not to purchase a license for the Evaluation Product, the Evaluation Product must be removed from Company’s system(s) and all permitted copies of such Evaluation Product immediately destroyed. A Return Materials Authorization number (“RMA #”) for any Hardware Evaluation Product must be obtained prior to return of such Product.

(b) Pre-Released Products. If the Product Company has received with this license is not yet commercially available ("Pre-Released Product"), then NetAlly grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Pre-Released Product and the

associated Documentation, if any, as provided to Company by NetAlly solely for internal evaluation purposes. NetAlly may terminate Company's right to use the Pre-Released Product at any time at NetAlly's discretion. Company's use of the Pre-Released Product is limited to thirty (30) days unless otherwise agreed to in writing by NetAlly. Company acknowledges and agrees that (i) NetAlly has not promised or guaranteed to Company that the Pre-Released Product will be announced or made available to anyone in the future; (ii) NetAlly has no express or implied obligation to Company to announce or introduce the Pre-Released Product; (iii) NetAlly may not introduce a product similar to or compatible with the Pre-Released Product; and (iv) any use of the Pre-Released Product or any product associated with the Pre-Released Product is entirely at Company's own risk. During the term of these General T&Cs, if requested by NetAlly, Company will provide feedback to NetAlly regarding use of the Pre-Released Product. Company will not disclose any features or functions of any Pre-Released Product until NetAlly makes the Pre-Released Product publicly available.

(c) API License. NetAlly grants Company a limited, non-exclusive, non-transferable revocable license to use the API, together with applicable documentation, any sample code, and any sample applications provided with the API, solely in connection with the Products for Company's internal business purposes; provided that Company may not use the API in connection with developing a product or service that competes with Products.

(d) License Restrictions. Except as required by law, Company will not, and will not cause or permit others to, derive the source code of the Software, or reverse engineer, disassemble, or de-compile the Products. Company may not (i) create derivative works of the Software, (ii) lend, rent, lease, assign, sublicense, and/or make available through timesharing or service bureau the Software, or (iii) transfer the Software or provide third party access to the Software.

(e) Third-party Technology. The Products may contain embedded third-party technology ("Third-party Materials"). Such Third-party Materials are licensed for use solely with the Product. Third-party Materials are provided subject to the applicable third-party terms of use ("TOU"). Company agrees to abide by the TOU and/or to obtain any additional licenses that may be required to use the Third-party Materials.

(f) Ownership. NetAlly and its third-party licensors retain all right, title, and interest in and to the Products, Third party Technology and/or APIs. Company retain all right, title and interest in and to the Company Data.

4. Acceptable Use. Company specifically agrees to limit the use of the Products and/or Services to those specifically granted in these General T&Cs. Without limiting the foregoing, Company specifically agrees not to (i) attempt to reverse engineer, decompile, disassemble, or attempt to derive the source code of the Software or any portion thereof; (ii) modify, port, translate, localize or create derivative works of the Software; (iii) remove any of NetAlly's, or its vendors, copyright notices and proprietary legends; (iv) use the Products to (a) infringe on the intellectual property rights of any third party or any rights of publicity or privacy; (b) violate any law, statute, ordinance, or regulation (including but not limited to the laws and regulations governing export/import control, unfair competition, anti-discrimination and/or false advertising); or (c) propagate any virus, worms, Trojan horses or other programming routine intended to damage any system or data; and/or (v) file copyright or patent applications that include the Product or any portion thereof.

5. Company & Personal Data. During the Term, Company may provide to NetAlly Company Data. NetAlly may use Company Data in connection with the performance of its obligations under these General T&Cs. Company hereby agrees to strictly comply with any and all applicable Data Protection Acts with regards to the transfer, handling storage and processing of Personal Data. Company acknowledges and agrees that should Company transfer such Personal Data to NetAlly, or other third-parties, Company will serve as such Personal Data's "Controller", as set forth in the applicable Data Protection Acts. Further, in the event of a breach of Personal Data, attributed to Company's actions or inactions in furtherance of these General T&Cs, in violation of the Data Protection Acts, Company shall promptly (i) take all necessary steps to curtail such breach; (ii) undertake all necessary actions to mitigate damages; (iii) provide the necessary notification and remediation, as set forth in the applicable Data Protection Act; and (iv) aid and assist in NetAlly's efforts to do the same, at Company's sole cost and expense.

6. Term and Termination. These General T&Cs shall continue unless terminated pursuant to this Section; provided, that the applicable subscription term for any licenses purchased hereunder shall continue for the period of time specified in the applicable Quotation. Either party may terminate these General T&Cs immediately upon providing written notice of breach to the other party, if such other party materially breaches any of its obligations hereunder but fails to cure such breach within a period of thirty (30) days following receipt of such written notice. Upon any termination of these General T&Cs (i) all licenses granted hereunder shall immediately terminate, (ii) Company will either return the Software, Documentation, and Copies or, with NetAlly's prior consent, destroy the Software, Documentation, and Copies.

7. Confidentiality. "Confidential Information" shall mean any and all non-public technical, financial, commercial or other confidential or proprietary information, Services, Product roadmaps, pricing, software code, Documentation, techniques and systems, and any and all results of benchmark testing run on the Products. Neither party will disclose Confidential Information to any third party except to the extent such disclosure is necessary for performance of these General T&Cs, or it can be documented that any such Confidential Information is in the public domain and generally available to the general public without any restriction. Each party will use the same degree of care to protect Confidential Information as Company uses to protect Company's own confidential information but in no event less than reasonable care.

8. Warranties. NetAlly warrants, for Company's benefit alone, (i) that the Hardware will be free from material defects for a period of twelve (12) months following the date of shipment of the Hardware ("Hardware Warranty Period"); and (ii) the Software, will conform materially and substantially to the Documentation for a period of ninety (90) days

following the date when first made available to Company for download ("Software Warranty Period"). The warranties set forth herein do not apply to any failure of the Software or Hardware caused by (a) Company's failure to follow NetAlly's installation, operation, or maintenance instructions, procedures, or Documentation; (b) Company's mishandling, misuse, negligence, or improper installation, de-installation, storage, servicing, or operation of the Product; (c) modifications or repairs not authorized by NetAlly; (d) use of the Products in combination with equipment or software not supplied by NetAlly or authorized in the Documentation; and/or (e) power failures or surges, fire, flood, accident, actions of third parties, or other events outside NetAlly's reasonable control. NetAlly cannot and does not warrant the performance or results that may be obtained by using the Products, nor does NetAlly warrant that the Products are appropriate for Company's purposes or error-

free. If during the Software Warranty Period or Hardware Warranty Period, a nonconformity is reported to NetAlly, NetAlly, at its option, will use commercially reasonable efforts to repair or replace the non-conforming Software or Hardware. THIS REMEDY IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY, AND NETALLY'S SOLE LIABILITY FOR A BREACH OF WARRANTY. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS SECTION 8, "WARRANTIES" NETALLY DISCLAIMS ALL WARRANTIES ON MERCHANDISE SUPPLIED UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

9. LIMITATION OF LIABILITY. NETALLY SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE UNLESS SUCH LOSS OR DAMAGE IS DUE TO NETALLY'S GROSS NEGLIGENCE AND/OR WILLFUL MISCONDUCT. IF NETALLY IS FOUND LIABLE, THE AMOUNT OF NETALLY'S MAXIMUM LIABILITY FOR ANY AND ALL LOSSES AND/OR DAMAGES (IN CONTRACT, TORT, OR OTHERWISE) SHALL NOT EXCEED THE TOTAL AMOUNT OF ALL LICENSE FEES ACTUALLY PAID TO NETALLY FOR THE RELEVANT NETALLY PRODUCT(S) OR SERVICE(S) WITHIN THE PRIOR SIX (6) MONTHS FROM WHICH SUCH CLAIM ARISES.

10. EXCLUSION OF CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, AND/OR INCIDENTAL DAMAGES, WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOST PROFITS OR LOSS OF DATA, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH POTENTIAL LOSS OR DAMAGE.

11. ESSENTIAL PURPOSE. THE LIMITATION OF LIABILITY AND EXCLUSION OF CERTAIN DAMAGES STATED HEREIN SHALL APPLY REGARDLESS OF THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. BOTH PARTIES HEREUNDER SPECIFICALLY ACKNOWLEDGE THAT THESE LIMITATIONS OF LIABILITY ARE REFLECTED IN THE PRICING.

12. Indemnification. For any claims based on Company's breach of Section 3, "License Grant and Restrictions", 4. "Acceptable Use", 5 "Company & Personal Data", 7 "Confidentiality", 8 "Warranties", 14.4 "Compliance & Export Controls", 14.6 "Anti-Corruption and Anti-Bribery" and/or Company use of Product(s), Company hereby agrees to indemnify, defend, and hold NetAlly harmless against such claim(s) at Company's expense and pay all damages that a court of competent jurisdiction finally awards, provided that NetAlly (i) promptly notifies Company in writing of the claim(s); (ii) allows Company to control the defense or any related settlement negotiations; and (iii) cooperates with Company in the defense of any such claim(s); provided, that, Company will not affect any settlement unless such settlement provides NetAlly with a full release.

13. Relationship with Third parties. The relationship between the parties established by these General T&Cs is that of independent contractors, and nothing contained in these General T&Cs shall be construed to: (i) give either party the power to direct or control the day-to-day activities of the other; (ii) constitute the parties as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking or franchise; (iii) allow Company to create or assume any obligation on behalf of NetAlly for any purpose whatsoever; or (iv) allow any customer, End-User, or other person or entity not a party to these General T&Cs to be considered a third-party beneficiary of these General T&Cs.

14. General Provisions.

14.1 Entire Agreement T&Cs & Integration. These General T&Cs and all Exhibits referencing these General T&Cs represent the entire agreement between the parties on the subject

matter hereof and supersede all prior discussions, agreements and understandings of every kind and nature between the parties. Neither party shall be deemed the drafter of these General T&Cs. No modification of these General T&Cs shall be effective unless in writing and signed by both parties. All additional and conflicting terms and conditions presented with or in any communication, including but not limited to Company's P.O., except with respect to price, quantity, and location specified in a P.O., are hereby rejected, and shall be deemed null and void.

14.2 Severability & Survival. The illegality or unenforceability of any provision of these General T&Cs shall not affect the validity and enforceability of any legal and enforceable provisions hereof. Should any provision of these General T&Cs be deemed unenforceable by a court of competent jurisdiction then such clause shall be re-construed to provide the maximum protection afforded by law in accordance with the intent of the applicable provision. Any provision contained herein, which by its nature should survive the termination of these General T&Cs shall survive, including, but not limited to, Section 7 "Confidentiality", 9 "Limitation of Liability & Exclusion of Consequential Damages", 12 "Indemnification", and 14 "General Provisions".

14.3 Assignment. Neither party may assign any rights or delegate any obligations hereunder, whether by operation of law or otherwise, except in the case of a sale of either party's business whether by merger, sale of assets, sale of stock or otherwise, or except with the prior written consent of the other party, which consent will not be unreasonably withheld. These General T&Cs binds the parties, their respective participating subsidiaries, affiliates, successors, and permitted assigns.

14.4 Compliance & Export Controls. Company shall comply fully with all applicable laws, rules, and regulations including those of the United States, and any and all other jurisdictions globally, which apply to Company's business activities in connection with these General T&Cs. Company acknowledges that the NetAlly Products and/or NetAlly Services are subject to United States Government export control laws. Company shall comply with all applicable export control laws, obtain all applicable export licenses, and will not export or re-export any part of the Products and/or Services to any country in violation of such restrictions or any country that may be subject to an embargo by the United States Government or to End-Users owned by, or with affiliation to, such countries embargoed by the United States Government.

14.5. U.S. Government Use Notice. The NetAlly Software is a "Commercial Item", as that term is defined at 48 C.F.R. § 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202, as applicable. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202-1 through 227.7202-4, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government End-Users (a) only as Commercial Items and (b) with only those rights as are granted to all other End-Users pursuant to the terms and conditions herein. For some components of the Software as specified in the Exhibit, Attachment, and/or Schedule, this Software and Documentation are provided on a RESTRICTED basis. Use, duplication, or disclosure by the United States Government is subject to restrictions set forth in Subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.

14.6 Anti-Corruption and Anti-Bribery. Company will not make or permit to be made any improper payments and will comply with the U.S. Foreign Corrupt Practices Act, the UK

Bribery Act, the Organization for Economic Co-operation and Development (“OECD”) Convention on Anti-Bribery, and other applicable local anti-bribery laws and international anti- bribery standards. Company represents and warrants that it will not pay any commission, finder's fee, or referral fee, or make any political contribution, to any person in connection with activities on behalf of NetAlly.

14.7 Applicable Law & Disputes. The parties specifically agree that the U.N. Convention on the International Sale of Goods, the Uniform Computer Information Transactions Act (“UCITA”), and the International Commercial Terms issued by the International Chamber of Commerce (“Incoterms”) shall not apply to any and all actions performed by either party hereunder in furtherance of these General T&Cs. These General T&Cs and all resulting claims and/or counterclaims shall be governed, construed, enforced and performed in accordance with the laws of the State of Colorado, United States of America, without reference and/or regard to its conflicts of laws principles. The parties hereto specifically agree that the exclusive jurisdiction for any and all resulting claims and/or counterclaims arising out of these General T&Cs shall be the federal and local courts of Denver, Colorado.

14.8 Force Majeure. Neither party shall be liable for any failure or delay in performing Services or any other obligation under these General T&Cs, nor for any damages suffered by the other or an End-User by reason of such failure or delay, which is, indirectly or directly, caused by an event beyond such party’s foreseeable control including but not limited to strikes, riots, natural catastrophes, terrorist acts, governmental intervention, or other acts of God, or any other causes beyond such party’s reasonable control.

14.9 Waiver. Each party agrees that the failure of the other party at any time to require performance by such party of any of the provisions herein shall not operate as a waiver of the rights of such party to request strict performance of the same or like provisions, or any other provisions hereof, at a later time.

15. Notices. All notices under these General T&Cs shall be in English and shall be in writing and given to the address indicated upon the cover page and may be sent either by (i) registered airmail; (ii) overnight delivery through a reputable third-party courier; or (iii) via electronic mail (email) sent “read receipt” and “delivery receipt”. With respect to NetAlly’s receipt of electronic notice set forth in (iii) above such notice shall only been deemed received once Company receives a confirmation of “read receipt” and “delivery receipt” and such notice shall only be valid if sent to legal@netally.com.

See also https://www.netally.com/web-legal/.

Upper-layer Decode Support Feature 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!

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

CONTIBUTORS 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

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

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, ROCUREMENT 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

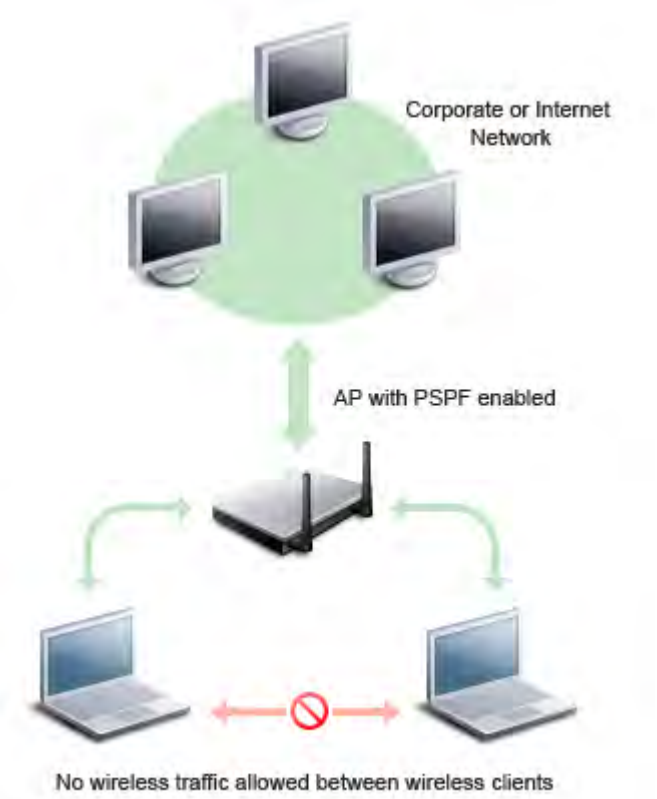
Policy

AP With Encryption Disabled

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the administrator on any AP operating without any WLAN layer 2 data encryption mechanisms such as **WEP**, **TKIP**, or **AES**. **VPN** technologies at layer three and above are the most commonly used alternatives to the WLAN layer 2 data encryption mechanisms. If neither encryption mechanism is used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. Typically, for an AP that is operating without any sort of encryption mechanism, there can be unauthorized clients without encryption keys that can associate with the AP and obtain access to the enterprise wired network. This not only risks the user's data privacy but also exposes the corporate wired network access.

This alarm may be turned off for the enterprise guest WLAN network or for hotspot deployments where encryption is generally not required. However, you may consider turning on the PSPF (Publicly Secure Packet Forwarding) alarm to protect your unencrypted wireless network. **PSPF** is a feature implemented on the WLAN Access Points to block wireless clients from communicating with other wireless clients.



AirMagnet Solution

AirMagnet WiFi Analyzer detects devices that are not using any encryption and recommends that the user use higher encryption mechanisms. For most WLAN environment, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF, it protects wireless clients from being hacked by an intruder's wireless devices. PSPF is effective in protecting wireless clients at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, and etc, where authentication is null and any one can associate with the APs. PSPF prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Client With Encryption Disabled

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the administrator on any client station operating without any WLAN layer 2 data encryption mechanisms such as **WEP**, **TKIP**, or **AES**. **VPN** technologies at layer three and above are the most commonly used alternatives to the WLAN layer 2 data encryption mechanisms. If neither encryption mechanism is used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. Clients with WEP disabled risk their file system, which may contain confidential corporate information from wireless intruders. These clients can then act as an entry point into the corporate network for intruders.

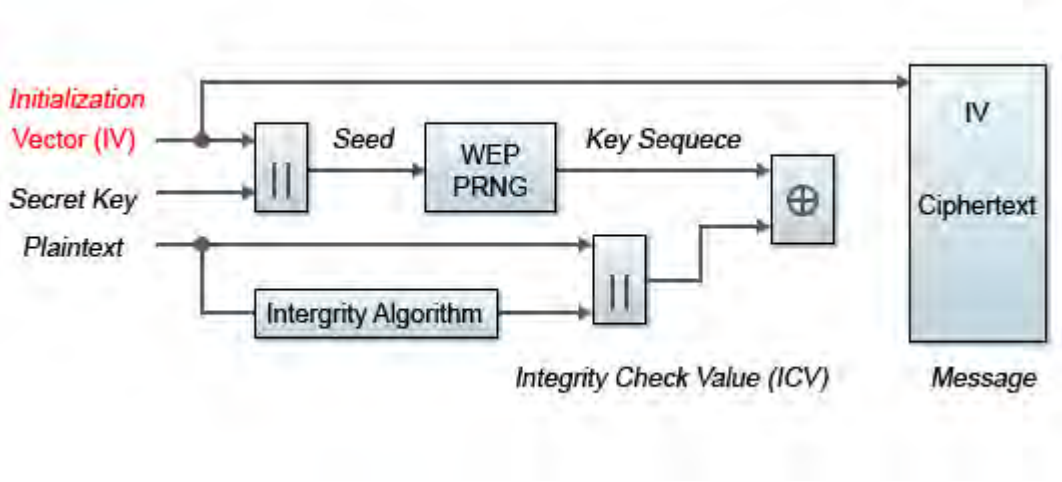
AirMagnet Solution

AirMagnet WiFi Analyzer detects devices that are not using any encryption and recommends that the user use higher encryption mechanisms.

WEP IV Key Reused

Alarm Description & Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir*).



WEP Encipher process Block Diagram

Cracked WEP secret key results in no encryption protection thus compromised data privacy. The key that is input to the 64 bit or 128 bit WEP encryption algorithm consists of the secret key configured by the user concatenated with the 24 bit IV (Initialization Vector). The IV is determined by the transmitting station. When IV key is reused frequently or in consecutive frames, it increases the possibility for the secret key to be recovered by wireless hackers.

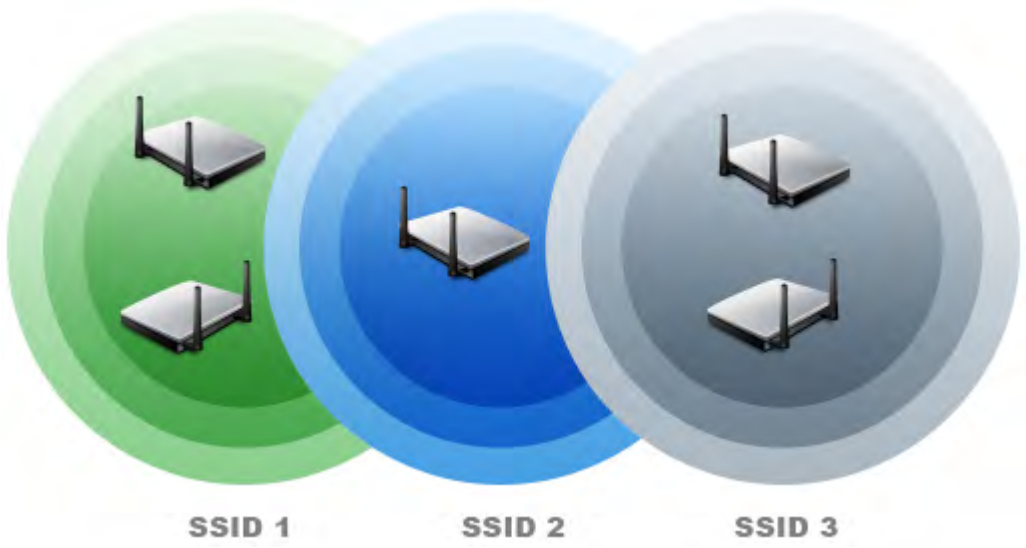
AirMagnet Solution

AirMagnet WiFi Analyzer alerts on weak WEP implementation and recommends device firmware upgrade from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN network can protect against WEP vulnerability by using TKIP (Temporal Key Integrity Protocol) encryption, which is supported by most enterprise grade wireless equipment. TKIP enabled devices are not subject to WEP key attack.

Insufficient RF Coverage

Alarm Description & Possible Causes

A WLAN installation site survey ensures sufficient RF coverage (maintaining a user-specified minimum RF signal strength) with at least one AP to serve the intended coverage area. Because of the dynamic nature of the RF environment, the actual coverage area may change from time to time. For example, if walls or partitions (which could cause interference) are rearranged, or if new devices that also operate on the 2.4 GHz spectrum (cordless phones, microwaves, and so on) are introduced, the RF coverage produced by APs could be compromised. If such a change becomes dramatic, wireless clients could not only experience degraded performance levels but could face connectivity issues.



AirMagnet Enterprise tracks RF coverage from multiple WLANs by their SSIDs

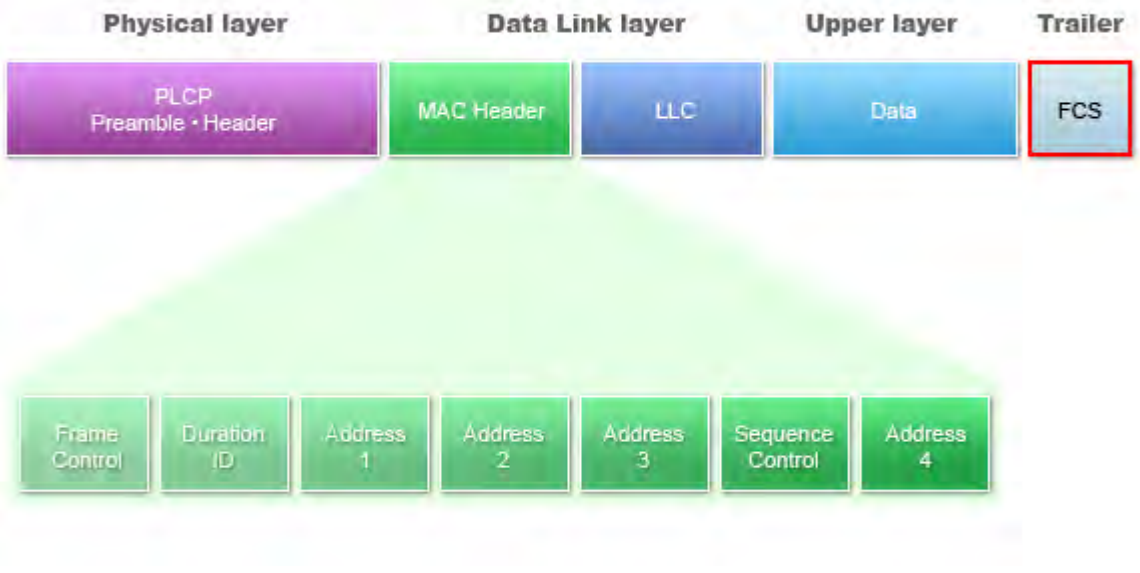
AirMagnet Solution

AirMagnet WiFi Analyzer tracks multiple WLANs by their SSIDs to make sure each SSID is covered sufficiently by at least one AP at the location. When AirMagnet WiFi Analyzer discovers any SSID not meeting the user-specified minimum AP signal strength, it generates an Insufficient RF Coverage alarm. This may be remedied by adding more APs to the SSID area or remedying the sources of interference.

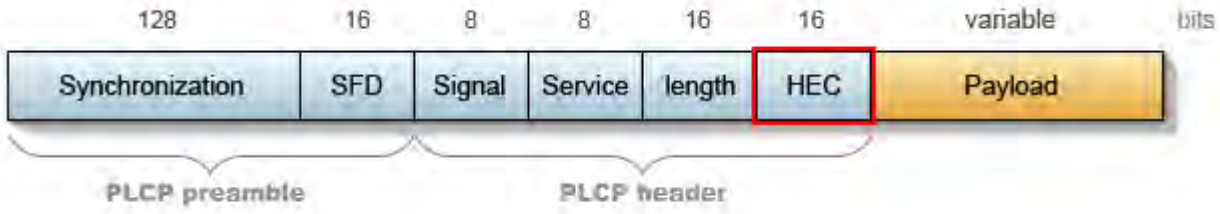
Excessive Packet Errors

Alarm Description & Possible Causes

The WLAN RF spectrum is open, dynamic, shared, and is subject to noise, interference, packet collisions, multipath, hidden node syndrome, and so on. IEEE 802.11 has a built in error checking mechanism to detect transmit and receive errors caused by any of the above mentioned issues. For example, the IEEE 802.11b **DSSS** (Direct Sequence Spread Spectrum) physical layer specification defines the PLCP (Physical Layer Convergence Protocol) header to include a HEC (Header Error Check) field for error detection (See illustration below). The receiver performs calculations on the synchronization, service and the length fields and compares it to the transmitted value. If the results do not match, the receiver has to make the decision of terminating the frame.



IEEE 802.11 Frame Includes Checksum in PLCP and FCS for Frame Header and Frame Body Respectively



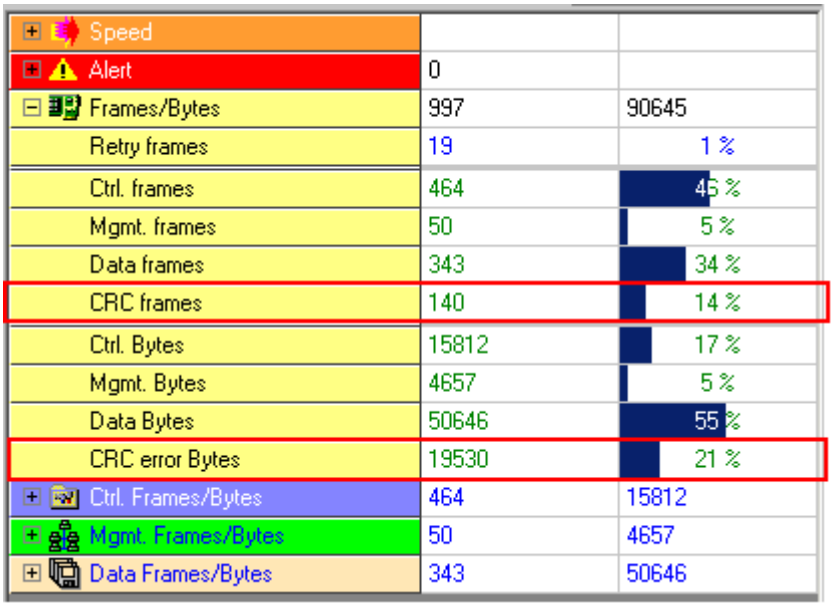
HEC (Header Error Checksum) defined in PLCP Header

802.11 MAC layer protocol also defines the FCS (Frame Checksum) field at the end of a packet for error detection. Refer to the illustration

Frame Control	Duration ID	Address 1 (source)	Address 2 (destination)	Address 3 (rx node)	Sequence Control	Address 4 (tx node)	Data	FCS
2	*2*	*6*	*6*	*6*	*2*	*6*	*0-2,312*	*4*

FCS (Frame Checksum) defined in 802.11 MAC Protocol format

AirMagnet WiFi Analyzer detects these error frames and tracks them based on per device and per channel orientation. See illustration below:



Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	46 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

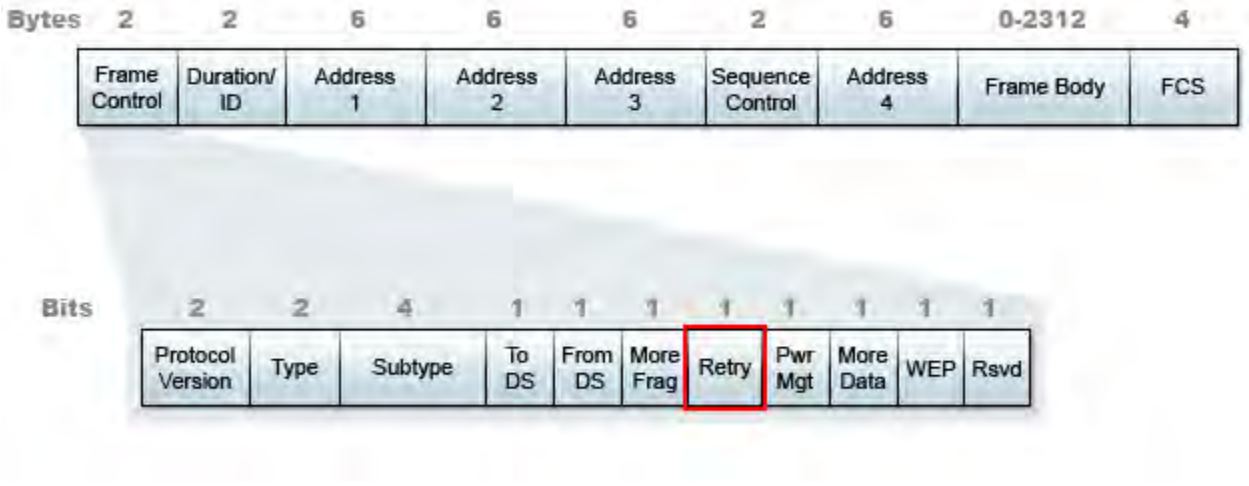
AirMagnet WiFi Analyzer CRC frame error tracking display for a channel or a device

When the CRC error frame to total frame ratio exceeds a user-definable threshold, AirMagnet WiFi Analyzer alerts the administrator to indicate a possible WLAN performance problem.

Excessive Frame Retries

Alarm Description & Possible Causes

The WLAN RF spectrum is open, dynamic, shared, and is subject to noise, interference, packet collisions, multipath, hidden node syndrome, and so on. When there are errors caused by any of the above issues, the transmitter of the error frame would not receive an 802.11 control frame called an **acknowledgement** frame. When there is no acknowledgement observed, the transmitter, assuming that the receiver did not receive the frame successfully, would re-transmit the unacknowledged frame with the **Retry** bit in the frame set to one. This indicates a re-transmission. The figure below illustrates the **Retry** field in the 802.11 frame header.



802.11 Frame Header including the Retry field to indicate frame re-transmission

AirMagnet Solution

AirMagnet WiFi Analyzer detects these retry frames and tracks them on a per device and per channel orientation. Refer to the illustration below:

Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	45 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

AirMagnet WiFi Analyzer Retry frame error tracking display for a channel or a device

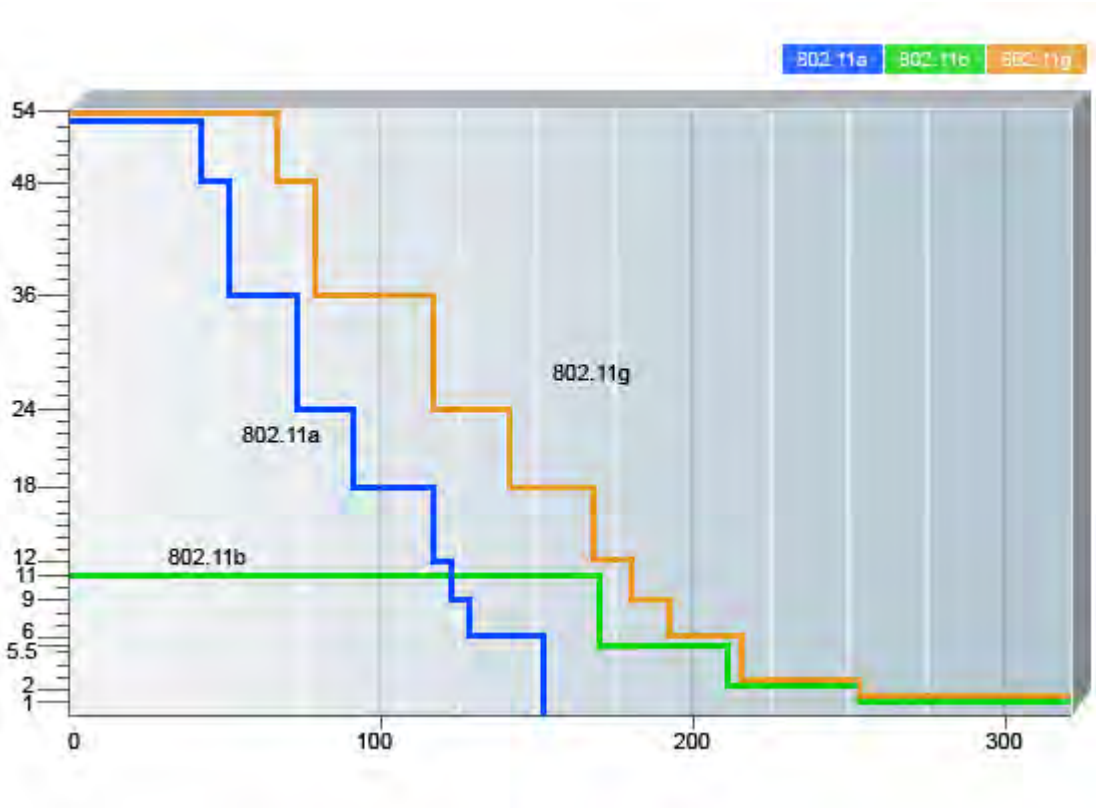
When the ratio of retry frames to total frames exceeds a user-definable threshold, AirMagnet WiFi Analyzer alerts the administrator of a possible WLAN performance problem due to noise, interference, packet collisions, multipath, hidden node syndrome, and so on. The administrator can then take appropriate steps to avoid such problems. For example, if

the problem stems from noise or interference, AirMagnet WiFi Analyzer's Find tool can be used to help track down and remedy the root cause.

Excessive Low Speed Transmission

Alarm Description & Possible Causes

802.11a, 11b or 11g devices use several different transmit speeds from frame to frame. Higher speed transmission consumes less bandwidth and allows higher throughput. Transmit speed optimization is a key factor during the WLAN site survey and deployment process. It is typically impacted by signal quality and distance.



802.11 a/b/g Speed and Range Correlation

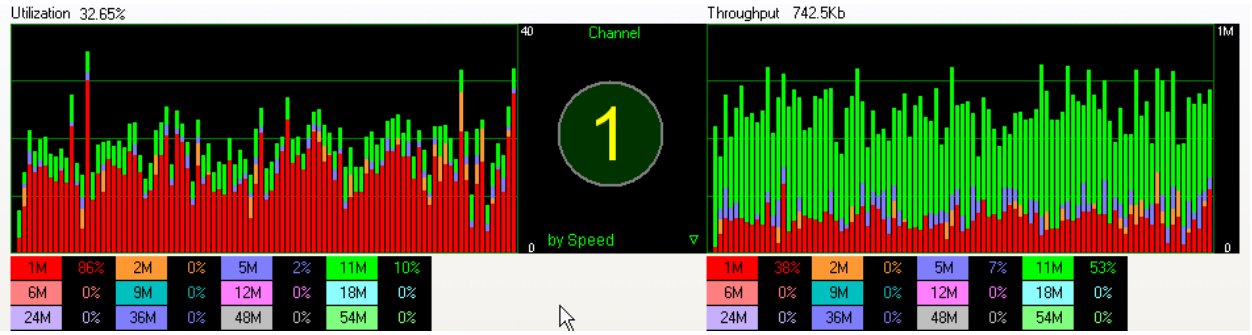
802.11b Speed and Coverage correlation

Refer to the table below for all the supported speeds and what AirMagnet WiFi Analyzer considers to be a low speed for the selected standard.

Speed	*802.11b (mbps)*	*802.11g (mbps)*	*802.11a (mbps)*
Support Speed	*1, 2, 5.5, 11*	*1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54*	*6, 9, 12, 24, 36, 48, 54*
AirMagnet Enterprise Considered Low Speed	*1, 2*	*1, 2, 5.5, 6, 9, 11, 12, 24, 36*	*6, 9, 12, 24, 36*

Supported transmission Speeds and AirMagnet Wi-Fi Analyzer considered 'Low' Speed

However, high speed transmission requires better signal quality to achieve the same low error rate as compared to the low speed transmissions. The transmit speed selection is a decision made by the transmitter that will also detect reception problems from the lack of acknowledgements. The transmitter may vary the transmit speed to increase reliability. When this scenario occurs too often, the WLAN slows down and the throughput degrades. Refer to the problem illustrated in the AirMagnet WiFi Analyzer screen shot below. It shows excessive low speed transmission (1mbps), high utilization (32%), and low throughput (931kbps).



AirMagnet WiFi Analyzer Channel screen shot on Bandwidth Utilization, Throughput, and Transmit Speed Relationship

AirMagnet Solution

AirMagnet WiFi Analyzer will alert the administrator if it sees a high amount traffic at lower speeds that may lead to excessive bandwidth usage and lower throughput. The administrator must take appropriate steps to ensure better signal quality to get higher speeds. Also, it is important to note that the distance from the stations to the AP should be appropriate to avoid lower speed transmissions.

Device Using Open Authentication

Alarm Description & Possible Causes

802.11 Open Authentication (as opposed to **Shared-key** authentication) is widely used today in conjunction with a higher-level authentication protocol such as **802.1x** to secure a WLAN. In some deployments, **Shared-key** Authentication where a static WEP key is used to challenge client stations attempting to associate with the AP is used instead of **Open** Authentication. Open Authentication, on the other hand, accepts associations from any client and there is no verification of the client's identity. Shared-key authentication appears to be more secure but actually has been proven to be vulnerable to WEP key cracking by wireless intruders because the challenge text and response are both clear and unencrypted. This means that the information is easily intercepted and interpreted by anyone with the appropriate software.

AirMagnet Solution

The recommended practice is to use 802.11 Open Authentication with some higher-level authentication mechanisms, such as the 802.1x/EAP framework or VPN. In case your deployment chooses to use Shared-key Authentication or something other than Open Authentication, you can enable this alarm to have AirMagnet Mobile alert you whenever it detects any device that violates your deployment policy of not using Open Authentication.

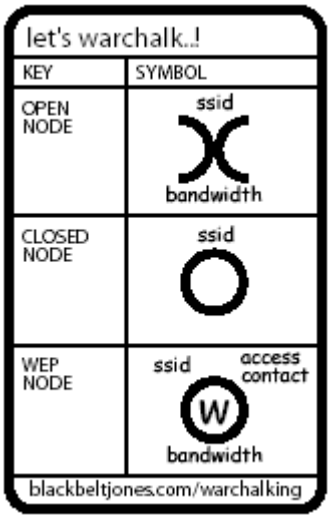
Device Probing for APs

Commonly used scan Tools: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo™ Scans, WiNc™, AP Hopper, NetChaser.

Alarm Description & Possible Causes

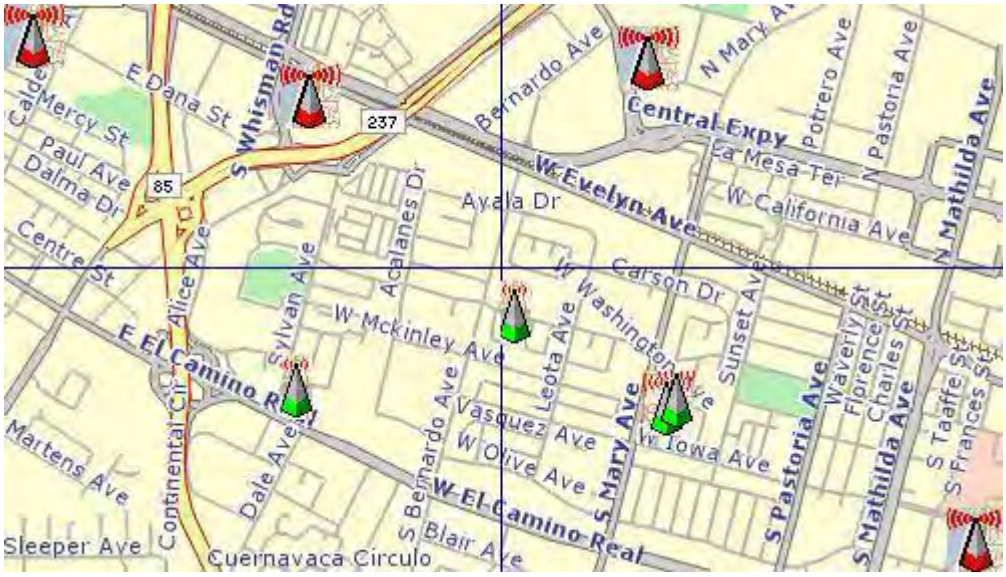
AirMagnet WiFi Analyzer detects wireless devices probing the WLAN and attempting association (that is, association request for an AP with any SSID). Such devices could pose potential security threats in one of the following two ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing and war-flying.
- Legitimate wireless client attempting risky promiscuous association.



War-chalker publishes a discovered WLAN and its configuration at the WLAN location with these universal symbols

The first potential security threat as indicated by this AirMagnet WiFi Analyzer alarm is the presence of WLAN war-driving, war-chalking, war-walking, and war-flying activities with tools mentioned above. A wireless hacker uses war-driving tools to discover APs and publish their information (MAC address, SSID, security implemented, and so on) on the Internet with the APs' geographical location information. War-chalkers discover WLAN APs and mark the WLAN configuration at public locations with universal symbols as illustrated above. You can think of war-walking as war-driving, but the hacker is on foot instead of a car. War-flying is just as the name implies, sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.



802.11 APs location posted on the Internet by war-driving groups

The second potential security threat for this alarm may be even more damaging. Some of these alarms could be from legitimate and authorized wireless clients on your WLAN that are attempting to associate with any AP that they can talk to including your neighbor's AP or the more damage causing rogue AP. This can be from a Microsoft Windows laptop with a built-in Wi-Fi card or laptops using wireless connectivity tools such as the Boingo™ client utility and the WiNc™ client utility. Once associated, this client station can be accessed by an intruder leading to a major security breach. To make matters worse, the client station may even unknowingly bridge the unintended AP with your company's wired LAN. A typical scenario, for example, is that modern laptops today are equipped with built-in Wi-Fi cards and are also at the same time physically attached to your company wired LAN for network connectivity. If the Windows bridging service is enabled on that Windows laptop, your wired network is then open wirelessly. To be secure, all client stations should be configured with specific SSID(s) to avoid associating with an unintended AP. Mutual authentication such as 802.1x and various EAP methods should also be considered to tackle such an issue.

AirMagnet WiFi Analyzer also detects a wireless client station probing the WLAN for an anonymous association (that is, association request for an AP with any SSID) using the NetStumbler tool. The **Device probing for AP** alarm is generated when hackers use latest versions of the NetStumbler tool. For older versions, AirMagnet WiFi generates the **NetStumbler detected** alarm.

NetStumbler is the most widely used tool for war-driving and war-chalking. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores.

AirMagnet Solution

To prevent your APs from being discovered by these hacking tools, you can configure your APs to not broadcast its SSID. You can use the information generated by the AirWISE alarm

to determine which of your APs is broadcasting (announcing) their SSID in the beacons. You may then adjust the AP properties to turn off the SSID broadcast feature.

AP Association Capacity Full

Alarm Description & Possible Causes

All WLAN Access Points have a resource limit for the number of client stations that can associate to it to receive wireless services. Usually, this limit is a user-configurable number on the AP. After an AP reaches this limit, it will not accept any more new client association requests.

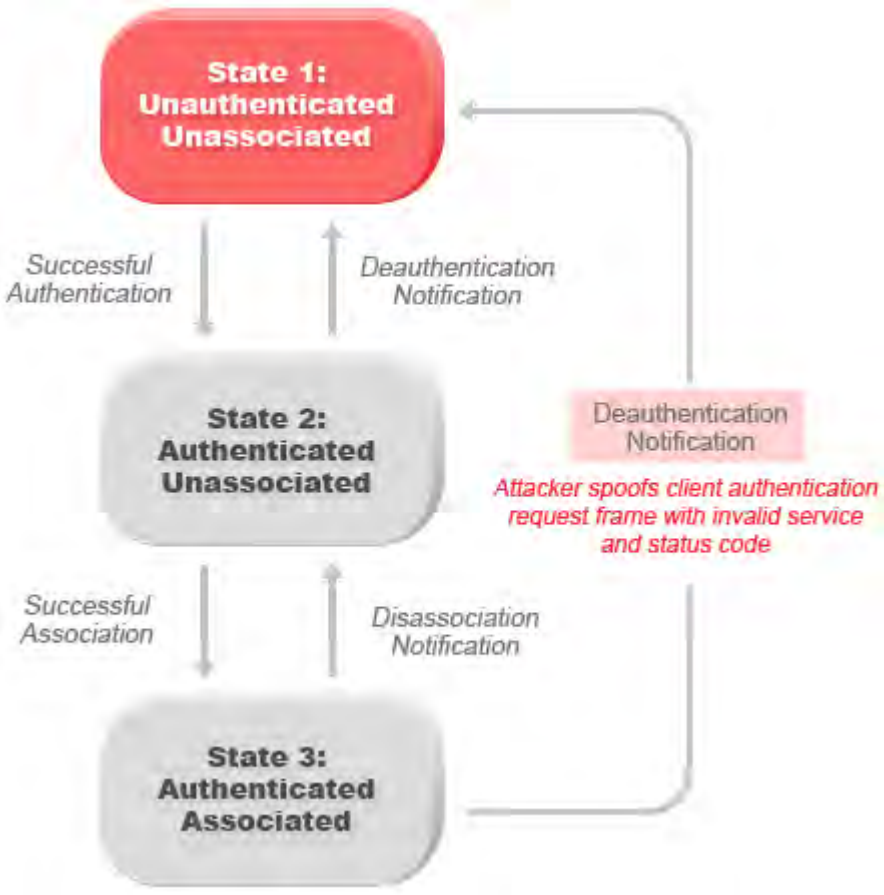
AirMagnet Solution

AirMagnet WiFi Analyzer monitors rejected association requests and responses to determine the cause of failed associations. When AirMagnet WiFi Analyzer concludes that they are due to an AP association capacity overflow problem, this alarm is generated. This alarm indicates under-provisioning or failed load balancing for the WLAN deployment. To remedy the problem, you can add additional APs to your existing infrastructure or try to remove unnecessary devices that are currently using up association positions on your current APs.

Denial-of-Service Attack: Authentication-Failure Attack

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and APs implement such a state computer (refer to the illustration below) based on the IEEE standard. A successfully associated client station must remain in **State 3** in order to continue wireless communication. A client station in **State 1** or **State 2** cannot participate in the WLAN data communication process until it is authenticated and associated to reach **State 3**. IEEE 802.11 also defines two authentication services: **Open System Authentication** and **Shared Key Authentication**. Wireless clients go through one of the two authentication processes to associate with an AP.



Attacker spoofs invalid authentication requests from associated client station to trick the AP into disassociating the associated client

A form of denial-of-service attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in **State 3** to an AP. Upon receiving the invalid authentication requests, the AP updates the client to **State 1**, which disconnects its wireless service.

AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of a denial-of-service attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an AP, AirMagnet WiFi Analyzer raises this alarm to indicate a potential intruder's attempt to breach security by brute force of computer power.

Note: *This alarm focuses on 802.11 authentication methods (Open System, Shared Key, etc). 802.1x and EAP-based authentications are monitored by other AirMagnet WiFi Analyzer alarms.*

AP Configuration Changed (Channel)

Alarm Description & Possible Causes

Most of the current day wireless 802.11b LAN equipment use Direct Sequence Spread Spectrum (DSSS) technology to send and receive data. In DSSS, the data signal is combined with the chipping code, which will divide the signal depending on the spreading ratio. 802.11a/g devices use the Orthogonal Frequency Division Multiplexing (OFDM) modulation technology to help achieve higher data rates. In this technology the high speed signal is divided into separate sub-carrier signals.

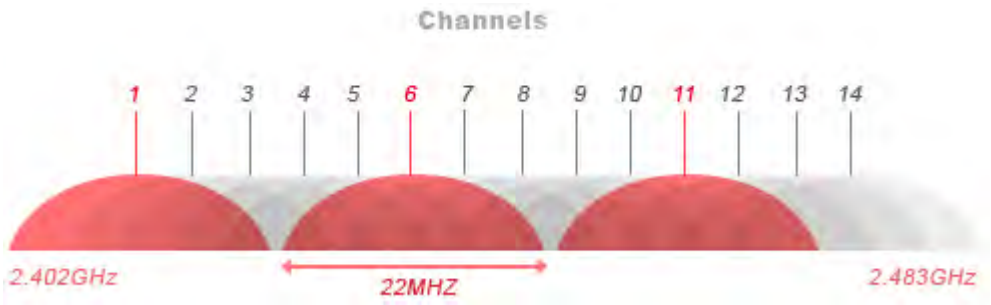
According to the 802.11 standard, the user sets the channel for the Access point and the wireless client adjusts its frequency to the same channel and then begins the association phase.

The IEEE 802.11 standard mandates the use of 802.11b/g devices in the 2.4 GHz ISM (Industrial, Scientific and Medical) band only while the 802.11a devices operate in the 5Ghz UNII (Unlicensed National Information Infrastructure) band. 802.11a devices cannot interoperate with 802.11b/g devices as they operate in different frequency bands.

Channel Identifer	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170	---	X	---	---
36	5180	X	---	X	---
38	5190	---	X	---	---
40	5200	X	---	X	---
42	5210	---	X	---	---
44	5220	X	---	X	---
46	5230	---	X	---	---
48	5240	X	---	X	---
52	5260	X	---	---	X
56	5280	X	---	---	X
60	5300	X	---	---	X
64	5320	X	---	---	X
149	5745	---	---	---	---
153	5765	---	---	---	---
157	5785	---	---	---	---
161	5805	---	---	---	---

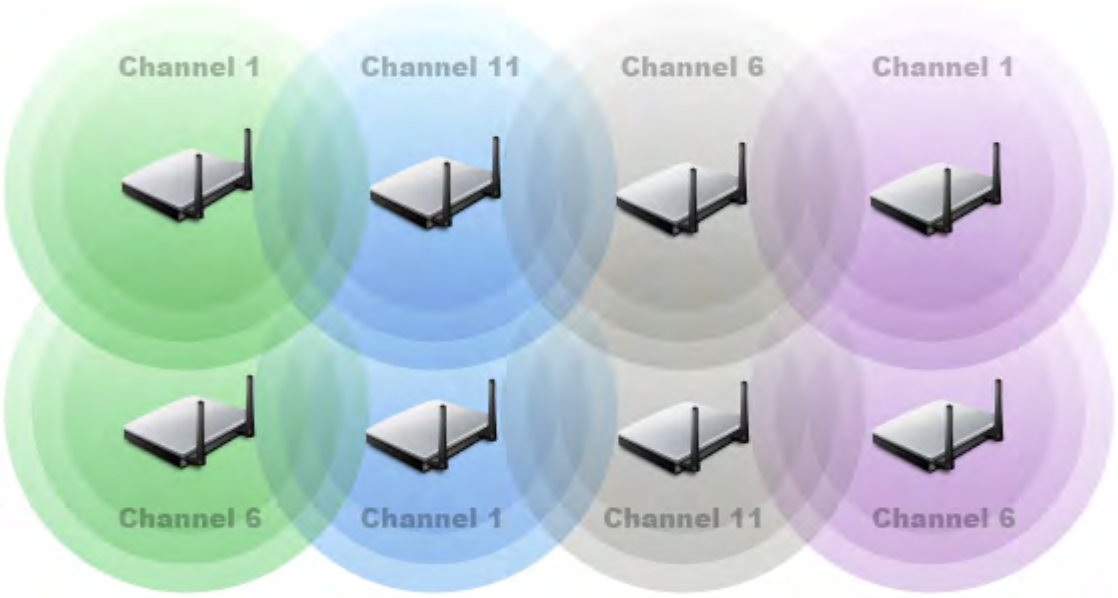
Channel assignment for 802.11b devices. Mexico is included in the Americas domain but channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. France is included in the EMEA regulatory domain, but only channels 10 through 13 can be used in France.

For 802.11b/g, a total of 14 channels are defined by the IEEE standard in the ISM band with each channel occupying 22 MHz. Adjacent channels overlaps with each other in RF frequency usage (refer to the illustration below).



802.11b and 11g Channel Allocation and Frequency Overlaps

Wireless devices operating in adjacent channels (channel numbers less than 5 apart) have their RF frequencies overlapped and will interfere with one another. Ideally, APs should be 5 channels apart to avoid such problem. This means that channel 1, 6 and 11 are the three non-overlapping channels in the frequency spectrum. Refer to the sample channel allocation and AP deployment below.



Site Survey Allocate Non-overlapping Channels to Physically Adjacent APs

After the initial site survey, in which channels for different APs were considered, it becomes very important that no changes be made in channel allocation. Any changes could lead to potential interference between APs and increased noise level in the frequency spectrum. Such a change could render the pre and post site survey useless. Sudden changes in the channel allocation for the APs could also indicate that an unauthorized person has gained access to the APs and has made those changes.

AirMagnet Solution

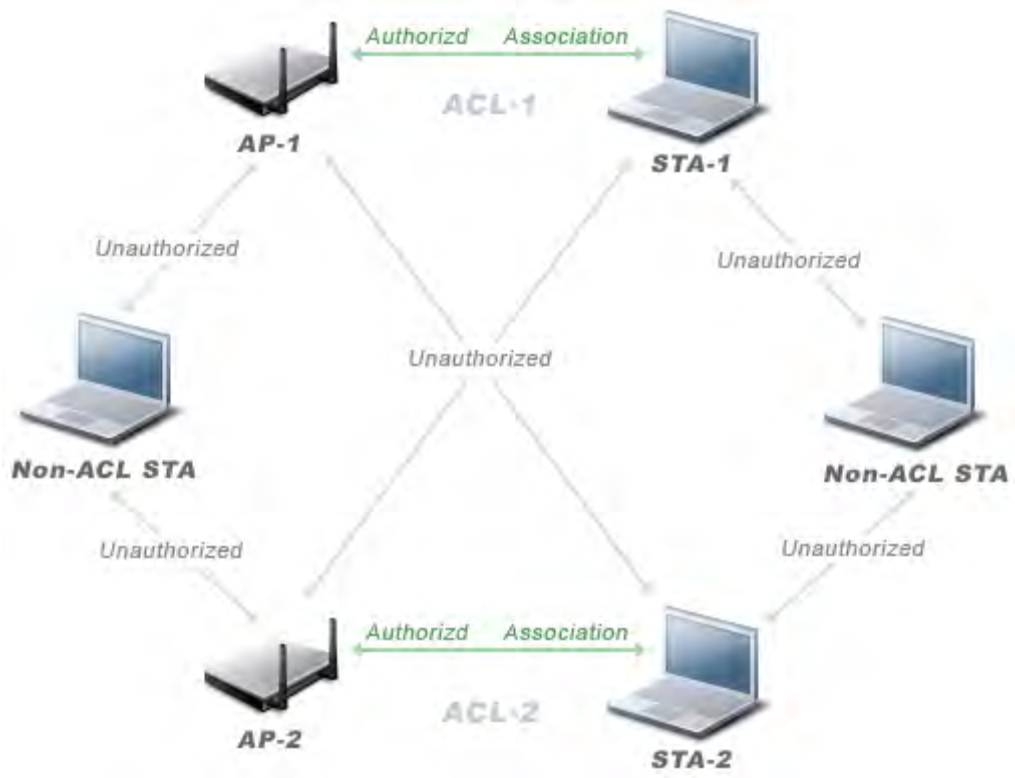
AirMagnet WiFi Analyzer also alerts you to any sudden changes in the SSID of the access point. This may indicate that an intruder has control over the access point and has modified the SSID configuration. This can cause all valid clients to get disconnected from the AP as they now are not talking on the same network. Connect to the AP whose configuration has changed and assign a stronger password for the access point login and change the SSID back to the original one to continue providing service to the clients.

Unauthorized Association Detected

Alarm Description & Possible Causes

AP-station association on an enterprise WLAN can be controlled through a network access control list (ACL) which consists of the MAC addresses of all the APs and stations that are officially deployed on the network. The ACL dictates that the APs can only associate with stations in the (same) ACL, and vice versa. Any AP-station association beyond the boundary of the ACL is unauthorized and, therefore, is prohibited. Once an ACL is configured on AirMagnet Wi-Fi Analyzer, it can be used as an effective tool to detect and alert WLAN administrators on any unauthorized association that is happening on the WLAN. The following are the typical situations of unauthorized associations, which are also illustrated in the diagram below:

- An AP in one ACL is associating with a station in another ACL, or vice versa.
- A station in an ACL is associating with a non-ACL AP.
- An AP in an ACL is associating with a non-ACL station.



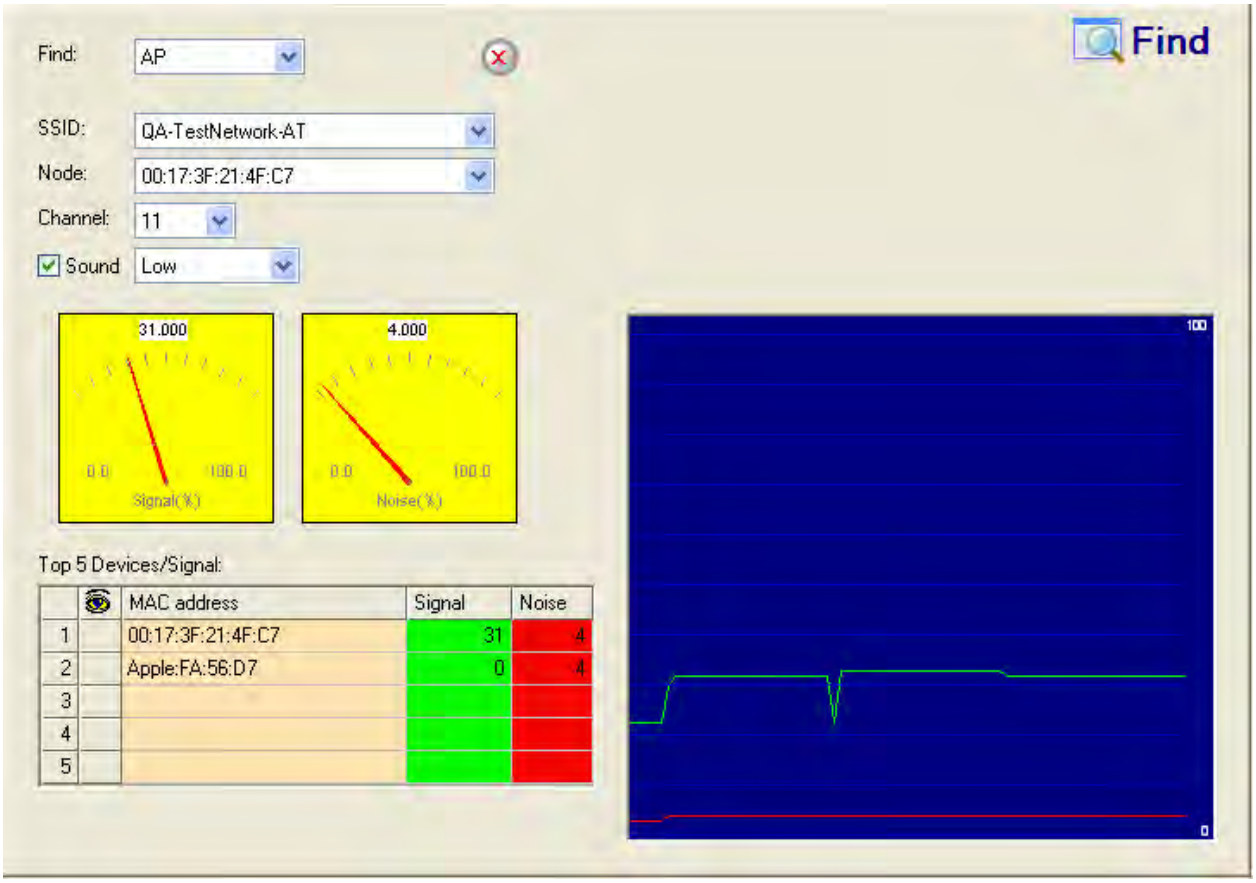
The diagram above illustrates the three scenarios of unauthorized AP-station associations, as indicated by the red arrows. Note that non-ACL AP/STA encompasses all APs or stations that are not in the ACL, which include rogue APs and stations, neighboring APs and stations, guest APs and stations, and so on. Also, authorized AP-station association can only occur between APs and stations within the same ACL.

In an enterprise network environment, rogue APs installed by employees usually do not follow the network's standard deployment practice and therefore compromise the integrity of the network. They are the loopholes in network security and make it easy for intruders to hack into the enterprise wired network. Nowadays, one of the major concerns that most wireless network administrators face is unauthorized associations between stations in an ACL and a rogue AP. Since data to and from the stations flows through the rogue AP, it leaves the door wide open for hackers to get all sorts of sensitive information. Rogue stations, on the other hand, not only cause security concerns, but also undermine network performance. They take up air space and compete for bandwidths on the network. Since an AP can only serve a certain number of stations, it will start rejecting association requests from stations once its capacity is reached. An AP laden with rogue stations will deny legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

Users can use AirMagnet WiFi Analyzer's Start screen to mark all legitimate devices on their network as valid devices by right-clicking in the screen and selecting a Valid Device category from the right-click menu. In so doing the application will treat all unknown devices as rogue and consequently trigger this alarm should an unknown device is detected on the network.

AirMagnet Solution

AirMagnet WiFi Analyzer can automatically alert network administrators to any unauthorized AP-station association it has detected on the network through this alarm. Once the alarm has been triggered, the rogue or unauthorized device must be identified and actions must be taken to resolve the reported issue. You can use AirMagnet WiFi Analyzer's Find tool to physically locate the AP and the station engaged in an unauthorized association and take them out of service to prevent them from further compromising network security.



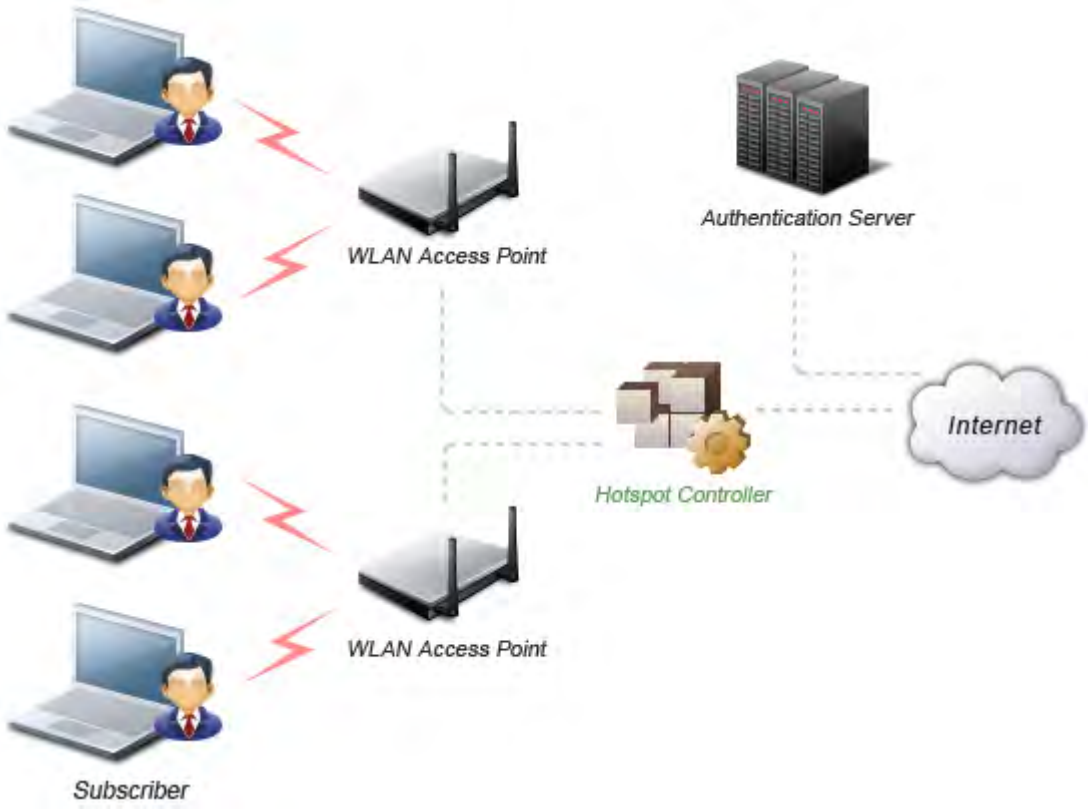
AirMagnet WiFi Analyzer's Find tool locates a device by tracking its signal and noise level

Airsnarf Attack Detected

Alarm Description & Possible Causes

A hotspot is any location where WiFi network access is made available for the general public. One often finds hotspots in airports, hotels, coffee shops, and other places where business people tend to congregate. It is probably one of the most important network access service for business travelers these days. All the customer requires is a wireless-enabled laptop or handheld device. Then the user can connect to the legitimate access point and get the service. Most Hotspots do not require the user to have any advanced authentications mechanism to connect to the access point, other than popping up a

webpage for the user to login. So, the criterion for entry is dependent only on whether the subscriber has paid the subscription fees or not. In a wireless hotspot environment, one can say that one should not trust anyone else. These days due to the concern of security, some WLAN Hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.



Basic components of a WLAN Hotspot network

The 4 components of a basic Hotspot network are:

- **Hotspot Subscribers:** These are valid users with a wireless-enabled laptop or handheld device and valid login for accessing the Hotspot network.
- **WLAN Access Points:** These can be SOHO gateways or enterprise level access points depending upon the Hotspot implementation.
- **Hotspot Controllers:** This box deals with user authentication, gathering billing information, tracking usage time, filtering functions, and so on. This can be an independent computer, or can be incorporated in the access point itself.
- **Authentication Server:** This server contains the login credentials for the subscribers. Hotspot controller in most cases after receiving the credential for the subscribers, verifies it with thee authentication server.

Airsnarf is a wireless access point setup utility to show how a hacker can steal username and password credentials from public wireless hotspots.

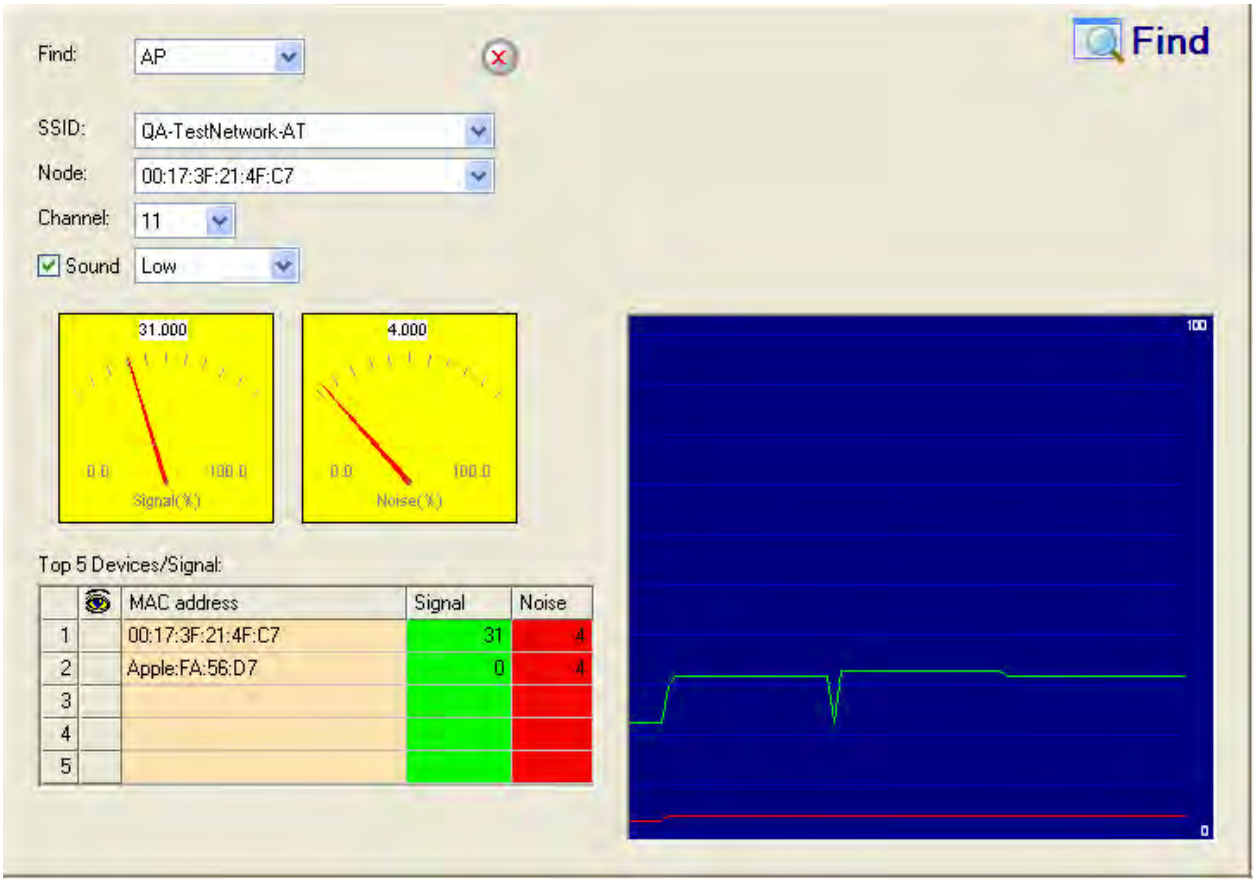
Airsnarf, a shell script based tool creates a hotspot complete with a captive portal where the users enter their login information. Important values such as local network information, gateway IP address, and SSID can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal, that will disassociate the hotspot wireless clients from the authorized AP connected to the Internet. The wireless clients assuming that they were temporarily disconnected from the Internet due to some unknown issue, will try to login again to resume their activities. Innocent wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf Access Point instead of the legitimate AP installed by the hotspot operator. The users will be shown a webpage that requests a username and password as now the DNS queries are resolved by the rogue Airsnarf AP. The username and password entered will be collected by the hacker.

The user name and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it could have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme.

The Airsnarf tool can also penetrate the laptop clients that are unknowingly connected to the Airsnarf AP. The AirSnarf tool can be downloaded by hackers from http://airsnarf.shmoo.com/

AirMagnet Solution

AirMagnet WiFi Analyzer will detect the wireless device running the AirSnarf tool. Appropriate action must be taken by the administrator to locate remove the AirSnarf tool from the WLAN environment. The Find tool can be used for this purpose.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Potential ASLEAP Attack Detected

Alarm Description & Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (Refer to the paper Weaknesses in the Key Scheduling Algorithm of RC4-I by Scott Fluhrer, Itsik Mantin and Adi Shamir).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out. The LEAP solution was considered to be not only a stable security solution but also considered to be easy to configure.

Joshua Wright, a network engineer at Johnson & Wales University in Providence, Rhode Island has written a hacking tool that compromises wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords The tool after detecting WLAN networks that use LEAP, de-authenticates the users forcing them to reconnect and provide their user name and password credentials. The hacker can capture packets of legitimate

users trying to re-access the network. After that the attacker can analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel, or perform channel hopping to look for target networks running LEAP.
- Actively deauthenticate users on LEAP networks, forcing them to reauthenticate. This makes the capture of LEAP passwords very fast.
- Only de-authenticating users who have not already been seen, doesn't waste time on users who are not running LEAP.
- Reading from stored libpcap files.
- Using a dynamic database table and index to make lookups on large files very fast. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing just the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq), and then process the LEAP credentials stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at *http://asleap.sourceforge.net*.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which will stop these dictionary attacks. EAP-FAST helps prevent Man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some of the major advantages of EAP-FAST are that it is not proprietary, is compliant with the IEEE 802.11i standard, supports TKIP and WPA, does not use certificates thus avoiding complex PKI infrastructures and supports multiple Operating Systems on the PCs and the Pocket PCs.

AirMagnet Solution

AirMagnet WiFi Analyzer detects the presence of a potential ASLEAP attack tool. Once detected, AirMagnet WiFi Analyzer alerts the wireless administrator and the user of the attacked station is advised to reset his/her password. The best solution to counter potential ASLEAP attacks is to replace LEAP with EAP-FAST in the corporate WLAN environment.

RF Regulatory Rule Violation

Alarm Description & Possible Causes

Most of the present-day wireless 802.11b LAN equipment uses Direct Sequence Spread Spectrum (DSSS) technology to send and receive data. In DSSS, the data signal is combined with the chipping code, which will divide the signal depending on the spreading ratio. 802.11a/g devices use the Orthogonal Frequency Division Multiplexing (OFDM) modulation technology to help achieve higher data rates. In this technology, the high-speed signal is divided into separate sub-carrier signals.

The IEEE 802.11 standard mandates the use of 802.11b/g devices only in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band, while the 802.11a devices operate in the 5Ghz UNII (Unlicensed National Information Infrastructure) band. 802.11a devices cannot interoperate with 802.11b/g devices as they operate in different frequency bands. According to the 802.11 standard, the user sets the channel for the Access point and the wireless client adjusts its frequency to the same channel and then begins the association phase.

Every region has its own local regulating body to police the operations of the 802.11 devices to ensure they are operating in the correct channel. In the USA, this regulating body is the Federal Communications Commission (FCC). The FCC assigns the non-licensed use of only 11 channels in the United States for 802.11b/g devices. Any device that is operating in other frequencies is violating the regulation and could invite strict action from the government agency.

Channel Identifer	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170	---	X	---	---
36	5180	X	---	X	---
38	5190	---	X	---	---
40	5200	X	---	X	---
42	5210	---	X	---	---
44	5220	X	---	X	---
46	5230	---	X	---	---
48	5240	X	---	X	---
52	5260	X	---	---	X
56	5280	X	---	---	X
60	5300	X	---	---	X
64	5320	X	---	---	X
149	5745	---	---	---	---
153	5765	---	---	---	---
157	5785	---	---	---	---
161	5805	---	---	---	---

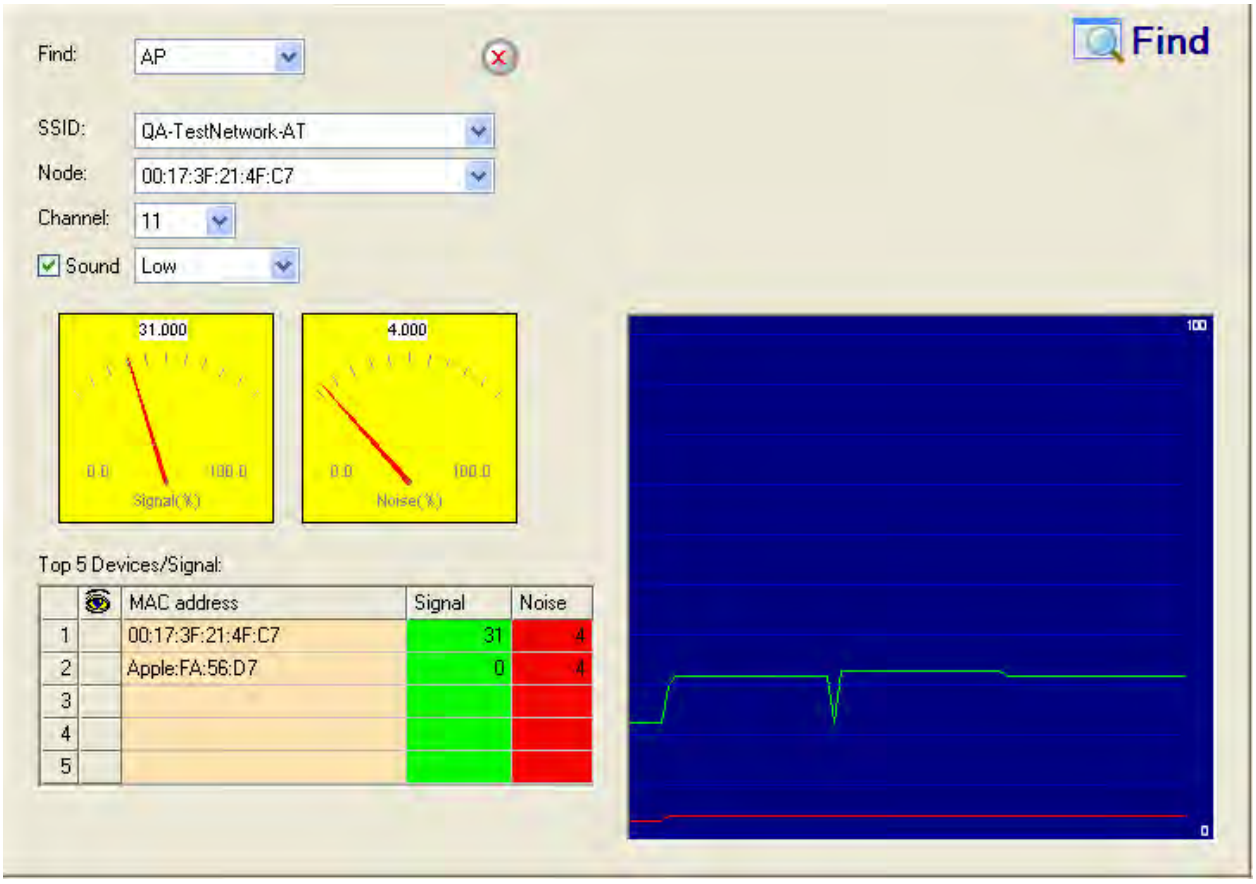
Channel assignment for 802.11a devices. All the channels are for indoor usage except channels 52 to 64 in Americas which can be used for indoor and outdoor usage.

Channel Identifer	Frequency in MHz	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japan (-J)
1	2412	X	X	---	X	X
2	2417	X	X	---	X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	---	X	X
11	2462	X	X	---	X	X
12	2467	---	X	---	---	X
13	2472	---	X	---	---	X
14	2484	---	---	---	---	X

Channel assignment for 802.11b devices. Mexico is included in the Americas domain but channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. France is included in the EMEA regulatory domain, but only channels 10 through 13 can be used in France.

AirMagnet Solution

AirMagnet WiFi Analyzer detects 802.11 devices operating in channels that are not authorized for use by the local geographic regulating body. For example, AirMagnet WiFi Analyzer can detect an AP operating in channel 14 in the United States, which is a violation as this channel is not authorized for use by the FCC. The administrator must take appropriate steps to locate the device and remove it from the wireless environment. Once the violating AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Device Unprotected by EAP-FAST

Alarm Description & Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See the paper Weaknesses in the Key Scheduling Algorithm of RC4-I by Scott Fluhrer, Itsik Mantin and Adi Shamir).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out. The LEAP solution was considered to be not only a stable security solution but also considered to be easy to configure.

Joshua Wright, a network engineer at Johnson & Wales University in Providence, Rhode Island has written a hacking tool that compromises wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords The tool after detecting WLAN networks that use LEAP, de-authenticates the users forcing them to reconnect and provide

their user name and password credentials. The hacker can capture packets of legitimate users trying to re-access the network. After that the attacker can analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel, or perform channel hopping to look for target networks running LEAP.
- Actively deauthenticate users on LEAP networks, forcing them to reauthenticate. This makes the capture of LEAP passwords very fast.
- Only de-authenticating users who have not already been seen, doesn't waste time on users who are not running LEAP.
- Reading from stored libpcap files.
- Using a dynamic database table and index to make lookups on large files very fast. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing just the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq), and then process the LEAP credentials stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which will stop these dictionary attacks. EAP-FAST helps prevent Man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some of the major advantages of EAP-FAST are that it is not proprietary, is compliant with the IEEE 802.11i standard, supports TKIP and WPA, does not use certificates thus avoiding complex PKI infrastructures and supports multiple Operating Systems on the PCs and the Pocket PCs.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts the wireless administrator on devices that are using the 802.1x authentication mechanism but are not using the EAP-FAST protocol. It is recommended that EAP-FAST be implemented in the wireless environment.

LEAP Vulnerability Detected

Alarm Description & Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See the paper Weaknesses in the Key Scheduling Algorithm of RC4-I by Scott Fluhrer, Itsik Mantin and Adi Shamir).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out. The LEAP solution was considered to be not only a stable security solution but also considered to be easy to configure.

Joshua Wright, a network engineer at Johnson & Wales University in Providence, Rhode Island has written a hacking tool that compromises wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords. The tool after detecting WLAN networks that use LEAP, de-authenticates the users forcing them to reconnect and provide their user name and password credentials. The hacker can then capture packets of legitimate users trying to re-access the network. After that the attacker can analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel, or perform channel hopping to look for target networks running LEAP.
- Actively deauthenticate users on LEAP networks, forcing them to reauthenticate. This makes the capture of LEAP passwords very fast.
- Only de-authenticating users who have not already been seen, doesn't waste time on users who are not running LEAP.
- Reading from stored libpcap files.
- Using a dynamic database table and index to make lookups on large files very fast. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing just the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq), and then process the LEAP credentials stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which will stop these dictionary attacks. EAP-FAST helps prevent Man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some of the major advantages of EAP-FAST are that it is not proprietary, is compliant with the IEEE 802.11i standard, supports TKIP and WPA, does not use certificates thus avoiding complex PKI infrastructures and supports multiple Operating Systems on the PCs and the Pocket PCs.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts the wireless administrator on devices that are using LEAP and are vulnerable to the ASLEAP attack and are under the risk of exposing their user-name and password information. It is recommended that EAP-FAST be implemented in the wireless environment.

Malformed 802.11 Packets Detected

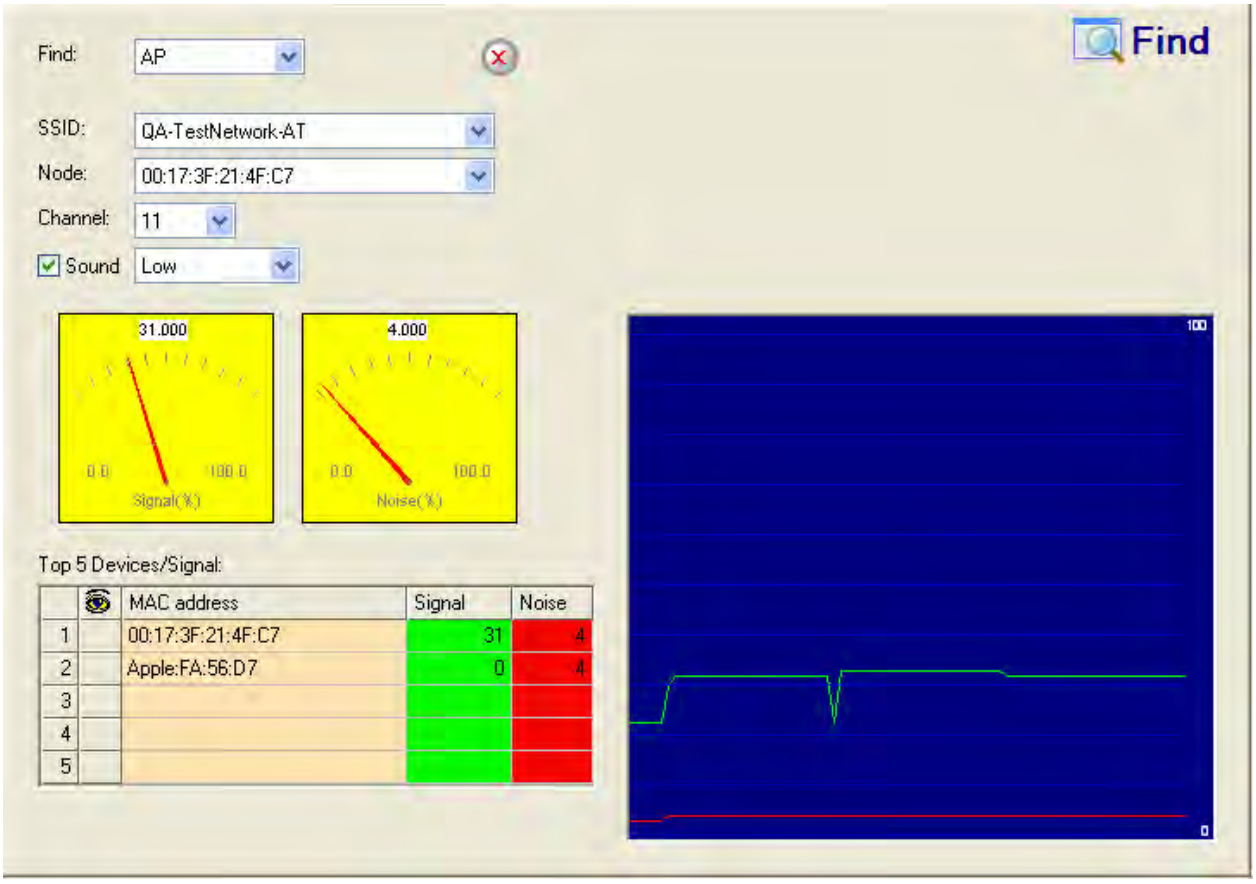
Alarm Description & Possible Causes

Hackers using illegal packets (malformed non-standard 802.11 frames) can force wireless devices to behave in strange manners. It is a well-known fact that illegal packets can cause the firmware of a few vendors' wireless network cards to crash. Examples of such vulnerability include NULL probe response frame (null SSID in the probe response frame) and oversized information elements in the management frames. These ill-formed frames can be broadcasted to cause multiple wireless clients to crash.

AirMagnet Solution

AirMagnet WiFi Analyzer can detect these illegal packets and raise an alarm when they appear. Wireless clients experiencing blue screen or lock-up problems during the attack period should consider upgrading the WLAN NIC driver or the firmware.

Once the client is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate it.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal and noise

Denial-of-Service Attack: PS Poll Flood Attack

Alarm Description & Possible Causes

Power Management is probably one of the most critical features of wireless LAN devices. This helps conserve the power used by the stations by keeping them in their power saving state for longer periods of time and receiving data from the AP only at specified intervals.

The wireless client device has to inform the AP of the duration of time that it will be in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks if it has any data frames waiting for it. After it completes a handshake with the AP it can receive the data frames. The beacons from the AP include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

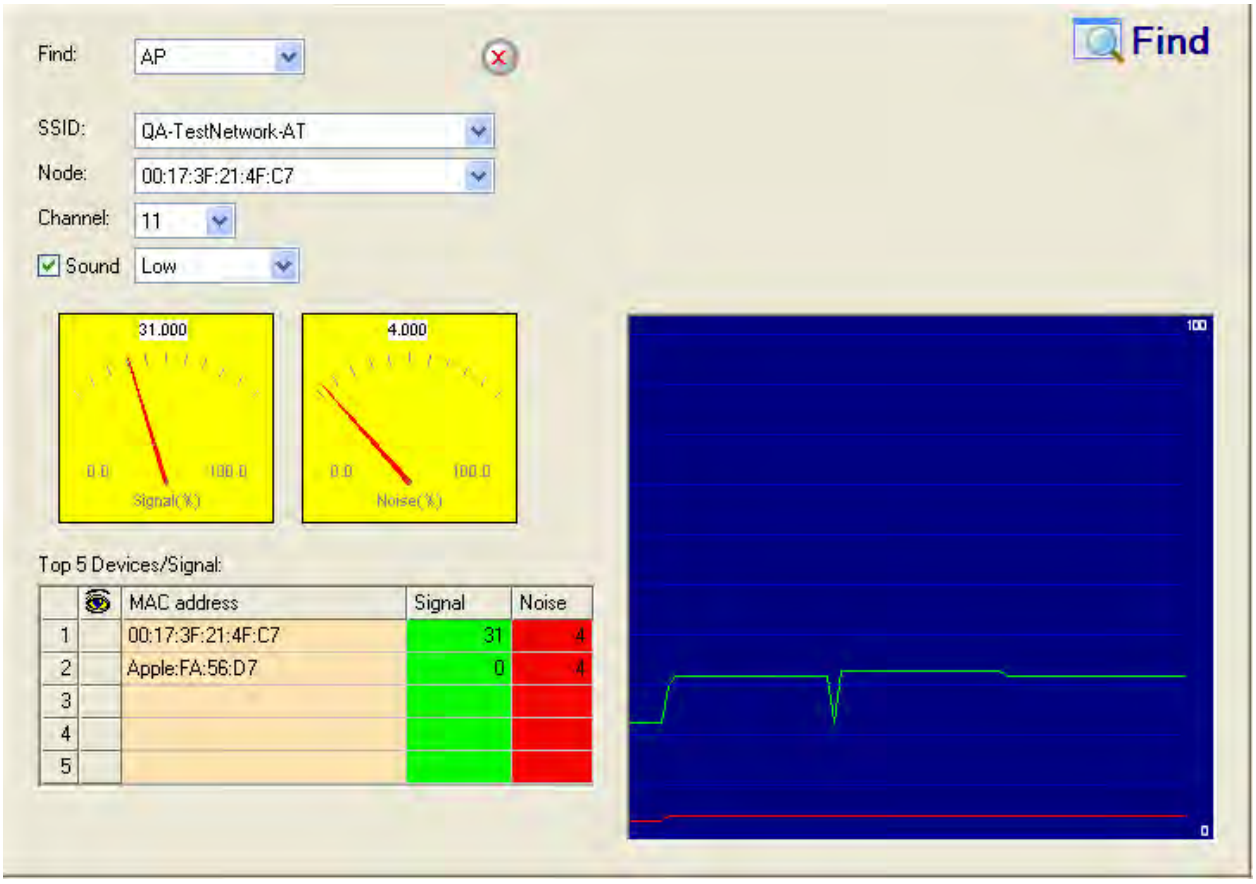
The AP will then continue to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the AP will notify the wireless client that it has data buffered for it. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the AP. For every PS-Poll frame, the AP responds with a data frame. If there are more frames buffered for the wireless client, the AP sets the more data bit in the frame response. The client will then send another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. In return, the AP will send out the buffered data frames to the wireless client. In reality, the client could still be in the Power Safe mode and will miss those data frames.

AirMagnet Solution

AirMagnet WiFi Analyzer can detect this Denial of Service attack that can cause the wireless client to lose legitimate data. You can use the Find tool to locate the source device and take appropriate steps to remove it from the wireless environment.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue AP Traced on Enterprise Wired Network

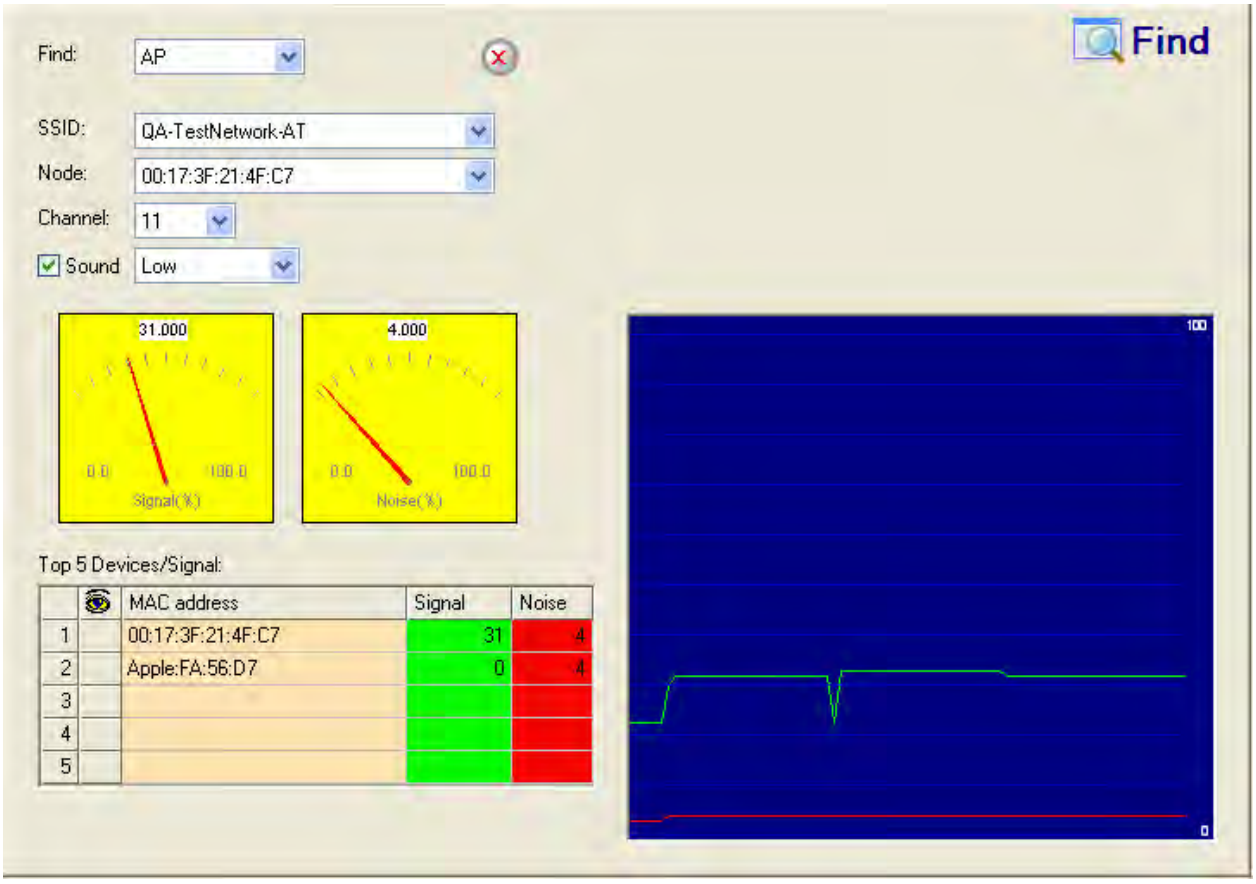
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer can detect rogue APs that are connected to the corporate wired network. Rogue APs installed by unauthorized employees may not follow enterprise standard deployment procedures thus compromising security on the wireless and wired network. Presence of rogue APs may also indicate malicious intruders attempting to hack into enterprise wired network. AirMagnet WiFi Analyzer discovered rogue devices should be thoroughly investigated. To use this feature, ensure that the laptop running the AirMagnet software is connected to the wired network and check the “Enable Trace” option present in the configuration settings and select the appropriate wired side adapter of the laptop running the AirMagnet software.

AirMagnet Solution

Once a rogue AP is identified, it can be successfully traced to the enterprise network using the AirMagnet WiFi Analyzer wired trace feature provided.

Note: *A rogue AP successfully traced by AirMagnet WiFi Analyzer to an enterprise port is a "TRUE" rogue and should be dealt with immediately. The user can use the FIND tool to physically locate this rogue and carry out the necessary steps to remove it.*



AirMagnet WiFi Analyzer's Find tool locates a rogue AP by tracking down its signal level

Excessive Fragmentation Degrading Performance

Alarm Description & Possible Causes

The 802.11 MAC layer supports the processes of fragmentation and defragmentation. The process of partitioning an 802.11 frame into smaller frames for transmission is called fragmentation; it helps to increase reliability and reduce errors. In cases where channel characteristics limit reception availability, transmitting in smaller (fragmented) frames increases the probability of successful transmission. Fragmentation is accomplished at each immediate transmitter before the actual start of transmission. The process of recombining fragmented frames into the original unfragmented longer frame is defined as defragmentation. The IEEE 802.11 standard defines the packet format to identify fragmented frames for defragmentation (illustrated below).

IEEE 802.11 Frame fields for frame fragmentation and defragmentation

The increased reliability of the smaller fragmented frames comes at the cost of frame transmission overhead. The frame is divided into different segments depending upon the fragmentation threshold. The placement of the fragments in the fragmentation process is decided by the "sequence control field" as shown in the figure above. The "more" field indicates if the fragment is the last fragment. If too many frames are requiring fragmentation and defragmentation, network overhead will be reduced and there may be a larger problem causing the fragmentation.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks the fragmentation statistics on the network and alerts on abused fragmentation usage that could lead to degraded WLAN performance. The fragmentation threshold needs to be carefully set to balance the benefit and overhead. Typically, equipment vendors set the default fragmentation threshold to 1536. Consult your equipment documentation and ensure that the manufacturer's recommendations are met.

AP Configuration Changed (SSID)

Alarm Description & Possible Causes

WLAN SSIDs are typically announced in the broadcast beacon frames sent by Access Points. It is meant for client stations to easily identify available WLANs and the APs providing the service.

Sudden changes in the SSID for the APs could indicate that an unauthorized person has gained access to the APs and has made those changes. Any changes in the SSID may cause network interruption for your clients as they no longer see the original SSID that is configured within their client utility or Windows zero-config.

Also, war-drivers equipped with tools such as Netstumbler sometimes scan for the SSIDs sent by Access Points to discover potential targets. In cases where your network is broadcasting its SSID, your network may be susceptible to two specific threats:

- Intruders can set the SSID on their client to attempt to join that WLAN. According to most war-driving web sites, many Access Points implemented these days are operating without any security. Even though knowing the SSID name does not necessarily mean that rogue clients will be able to join the network, it is necessary to carry out other forms of security attacks (such as Denial-of-service).
- Your WLAN and APs with GPS information on your geographical location may be collected in a global database and published on the Internet.

Sudden changes in the “broadcasting SSID” configuration on your AP may indicate that

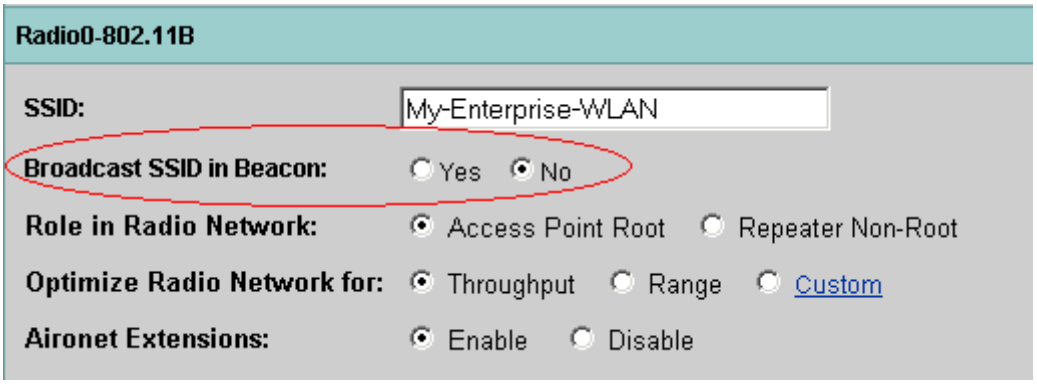
1. an unauthorized person has gained access to the APs and has made those changes (from “Not broadcasting SSID” to “broadcasting SSID”).
2. changes could be made to enhance the security of the network (from “broadcasting SSID” to “Not broadcasting SSID”) by the Access Point administrator.

AirMagnet Solution

AirMagnet WiFi Analyzer also alerts the user for any sudden changes in the SSID of the access point. This may indicate that an intruder has control over the access point and has modified the SSID configuration. This can cause all valid clients to get disconnected from the AP as they now are not talking on the same network or compromise the security of the network. Connect to the AP whose configuration has changed and assign a stronger password for the access point login and change the SSID back to the original one or restore the “broadcasting SSID” property to the original one to continue providing service to the clients.

Type	CH	Device	MAC	S	N		Security		SSID
AP	7	QA_VoFi_1	00:14:F1:AF:1B:94	58	0	2	?	N	
AP	2	QA_VoFi_3	00:0F:34:A7:78:10	46	0	4	WEP	N	QACiscoVoice
AP	5	QA_VoFi_2	00:12:44:B8:9C:32	26	0	2	WEP	N	QAVOFI
AP	6	192.168.12.1	00:0D:0B:4F:5E:00	79	0	0	Open	N	BuffaloWing_AME
AP	7	QA_VoFi_1	00:14:F1:AF:1B:93	56	0	2	WEP	N	QAVocera
AP	5	QA_VoFi_2	00:12:44:B8:9C:31	27	0	2	802.1x	N	QASpectralink
AP	11	ciscoap1250	00:17:DF:A6:5B:D0	90	0	1	WPA-P	N	EA-Cisco-Jav
AP	7	QA_VoFi_1	00:14:F1:AF:1B:92	55	0	2	WEP	N	QAVOFI
AP	5	QA_VoFi_2	00:12:44:B8:9C:30	25	0	2	WEP	N	QACiscoVoice
AP	7	QA_VoFi_1	00:14:F1:AF:1B:91	57	0	1	802.1x	N	QASpectralink

AirMagnet WiFi Analyzer's START screen shows non-broadcast SSID in red



Turning off SSID broadcast for Cisco Aironet Access Point through the browser interface

Denial-of-Service Attack: Virtual Carrier Attack

Alarm Description & Possible Causes

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to the legitimate users.

Under normal circumstances the only time a ACK frame should carry a large duration value is when the ACK is part of a fragmented packet sequence. The only legitimate occasion a data frame can carry a large duration value is if it is a subframe in a fragmented packet exchange.

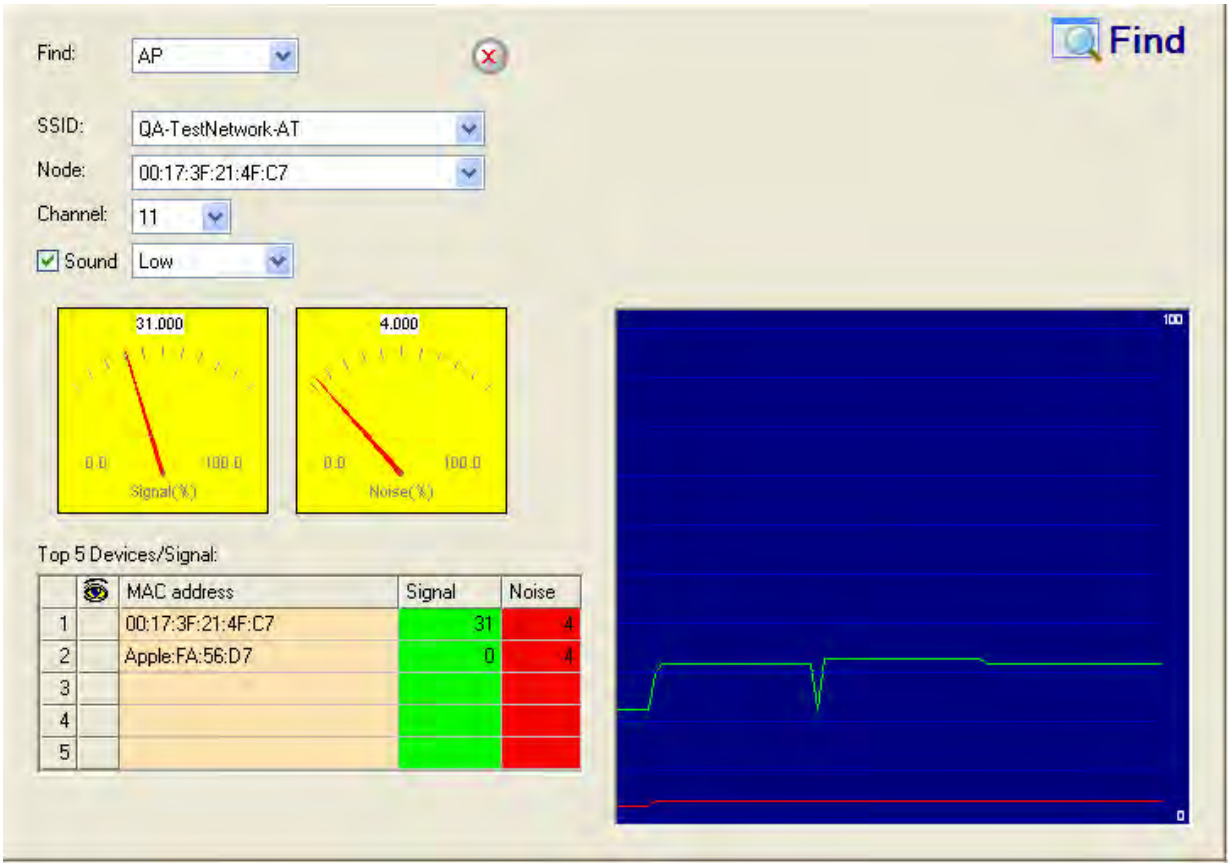
One approach to deal with this attack is by placing a limit on the duration values accepted by nodes. Any packet containing a larger duration value is simply truncated to the maximum allowed value. One can use low cap and high cap values. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is usable when the only packet that can follow the observed packet

is an ACK or CTS. This includes RTS and all management (association, etc) frames. The high cap, on the other hand, is used when it is valid for a data packet to follow the observed frame. The limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame will also receive the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. So the duration value of RTS is respected till the following data frame is received/not receive. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out of range station, one method of defense is to introduce authenticated CTS frames, containing cryptographically signed copy of the preceding RTS. But then there is possibility of overhead and feasibility issues.

AirMagnet Solution

AirMagnet WiFi Analyzer detects this Denial of Service attack. Locate the device and take appropriate steps to remove it from the wireless environment.



AirMagnet WiFi Analyzer'S FIND tool locates devices by tracking down their signal level

Fake DHCP Server Detected (Potential Wireless Phishing)

Alarm Description & Possible Causes

Dynamic Host Configuration Protocol (DHCP) is used for assigning dynamic IP addresses to devices on a network.

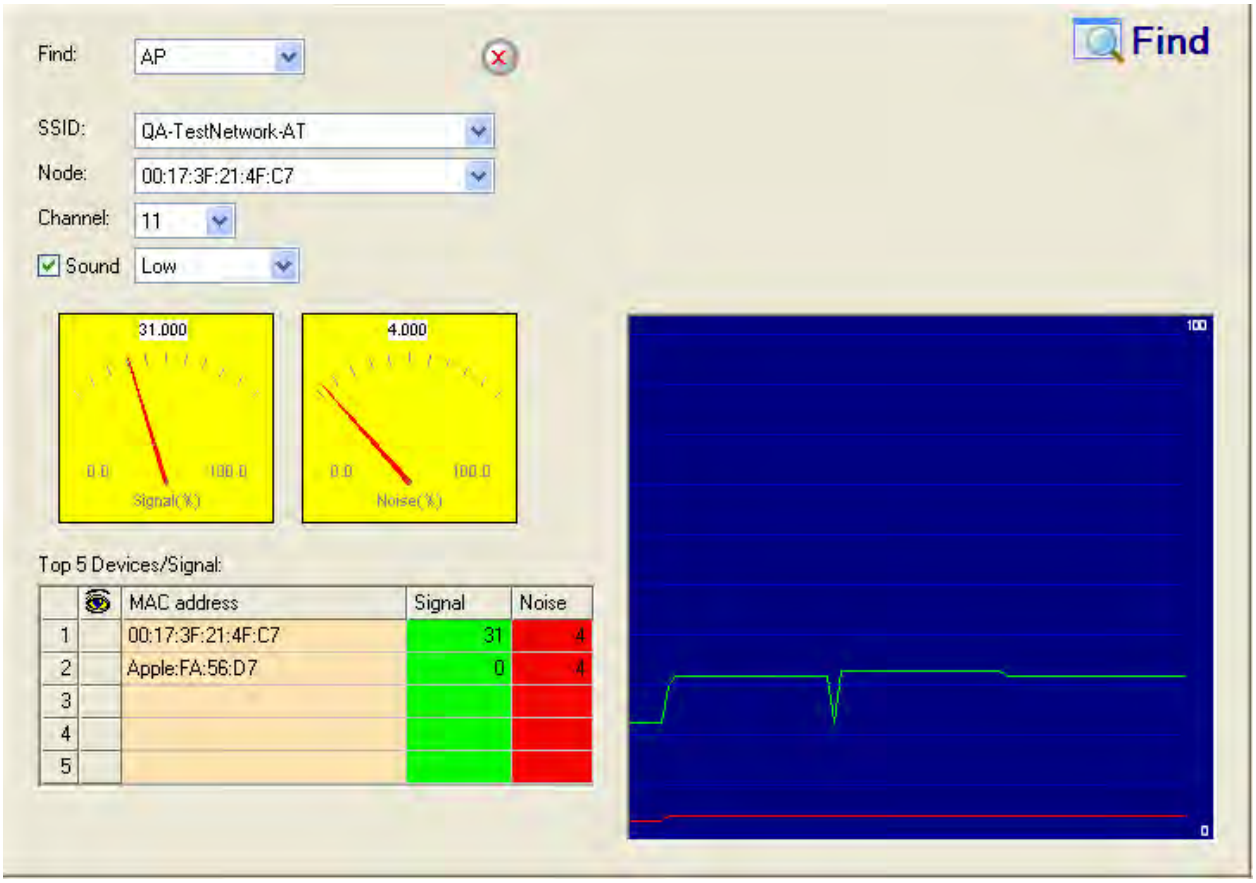
DHCP address assignment takes place as follows:

1. The client NIC sends out a DHCP discover packet, indicating that it requires an IP address from a DHCP server.
2. The server sends a DHCP offer packet with the IP address it has on offer.
3. The client NIC then sends a DHCP request, informing the DHCP server that it wants to be assigned the IP address offered.
4. The server returns a DHCP ACK, acknowledging that the NIC has sent a request for a specific IP address. At this point the client's interface assigns/binds the initially offered IP address from the DHCP server.

The DHCP server should be a dedicated machine that is part of the enterprise wired network or it could be wireless/wired gateway. However, other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then inadvertently connect to these Fake DHCP servers to get their IP addresses, as the clients do not have any means to authenticate the server in any way. These Fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. This would then give the hackers a chance to eavesdrop on every packet sent by the client. The hacker, with the aid of rogue DNS servers, could also send the users to fake web pages that require them to login, which provides the attacker with username and password credentials. It could also simply give out non-functional and non-routable IP addresses to achieve a Denial of Service attack. This sort of attack is generally against a WLAN without encryption, such as hotspots or trade show networks.

AirMagnet Solution

AirMagnet WiFi Analyzer detects such wireless STAs running the DHCP service and providing IP addresses to unaware users. Once the client is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Device Unprotected by Other Encryption

Alarm Description & Possible Causes

If your WLAN security deployment mandates the use of encryption technologies provided by Cranite Systems, Inc., you may enable this AirMagnet WiFi Analyzer alarm to alert you on devices that are participating in WLAN communication without Cranite encryption.

Cranite's WirelessWall software provides robust wireless security, seamless mobility and increased network visibility, while meeting the government's stringent FIPS 140-2 security standard. It encrypts full Ethernet frames, rather than just IP payloads, hiding vital information such as IP addresses, applications and ports from unauthorized listeners.

Frame-level encryption also protects non-data network traffic, including DHCP requests or ARP messages, from being compromised and used to attack the network. Unlike IPSec-based solutions, frame-level encryption allows the easy native use of other protocols such as IPX and AppleTalk.

AirMagnet WiFi Analyzer allows enterprise network administrators to monitor, administer and secure an organization's WLANs across any number of campuses and office locations and drill down into individual network elements from a remote management interface. AirMagnet WiFi Analyzer identifies more than 100 different kinds of wireless problems, providing a comprehensive security, reliability and performance management system that monitors every WLAN band and channel in use worldwide (802.11a, 802.11b, or 802.11g), no matter how large or dispersed.

AirMagnet Solution

Take appropriate steps to enable the use of Cranite encryption for various devices in the wireless environment. This new security alert identifies users who fail to run Cranite's WirelessWall technology. This will allow security-conscious customers who have chosen WirelessWall to verify that their authentication/encryption policies are being followed in every installation worldwide. In addition, shared notifications among both systems will allow Cranite administrators to see external wireless threats. The integration of the AirMagnet alerts into WirelessWall will enable Cranite users to have a better view of the overall performance of their network, and be able to identify external threats, such as denial-of-service attacks. The combined product offering brings together Cranite's government-certified WirelessWall software, which secures wireless local area networks (LANs), and AirMagnet WiFi Analyzer's security and performance management system, which manages and monitors wireless security. With this solution, organizations benefit from government-certified Layer 2 security, seamless roaming and mutual authentication, combined with the most complete monitoring of rogues, wireless exploits and network intrusions.

Denial-of-Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

Alarm Description & possible causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism as well as the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to Denial of Service RF Jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points (AP), to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b and low-speed (below 20Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20Mbps using OFDM) 802.11g wireless devices are not affected by this specific attack. Also not affected are devices that use FHSS.

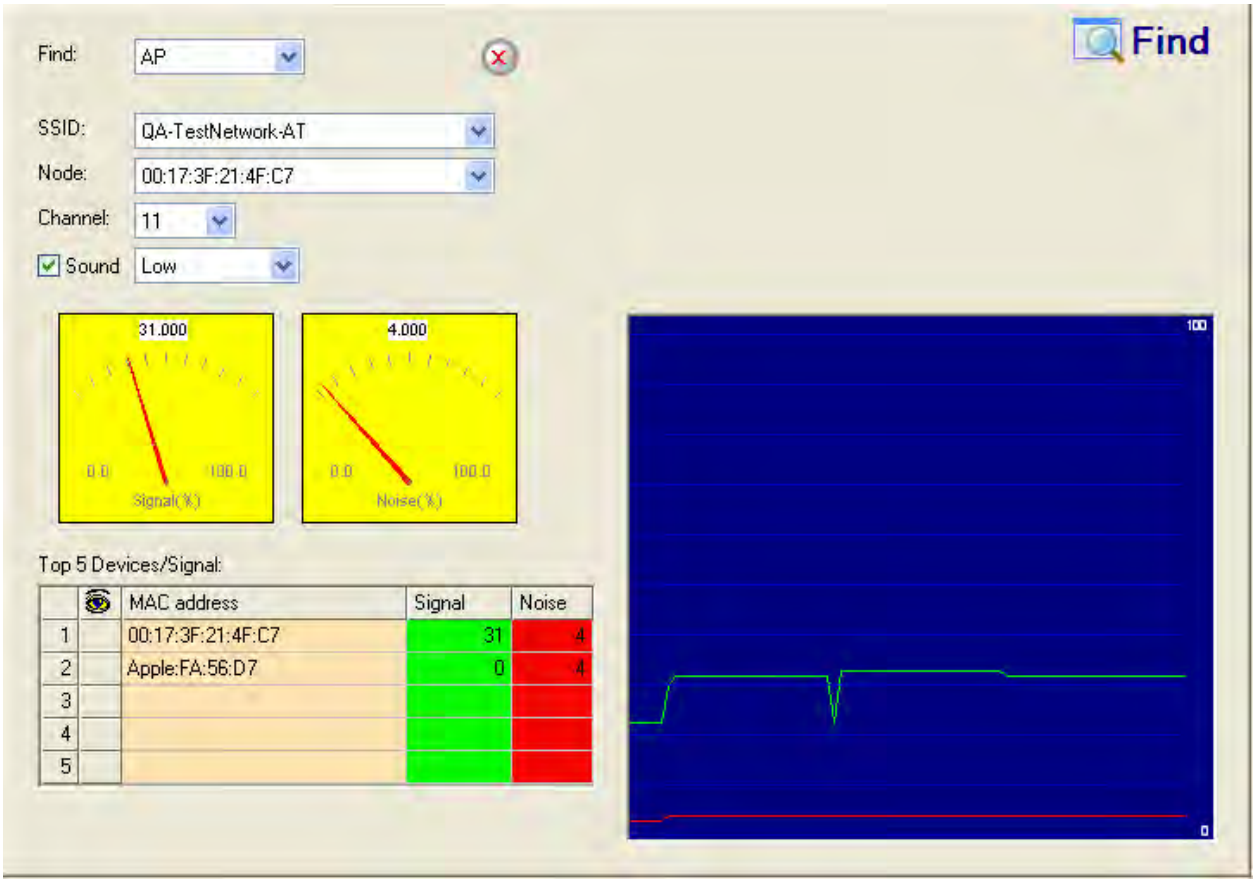
Any attacker using a PDA or a laptop equipped with a WLAN card can launch such an attack on SOHO and enterprise WLANs. The only solution or known protection against such an attack is switching to the 802.11a protocol.

For more information on this DoS attack please refer to:

- www.isi.qut.edu.au/
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

AirMagnet Solution

AirMagnet WiFi Analyzer detects this specific DoS attack and sets off the alarm. Use the Find tool to locate the responsible device and take appropriate steps to remove it from the wireless environment.



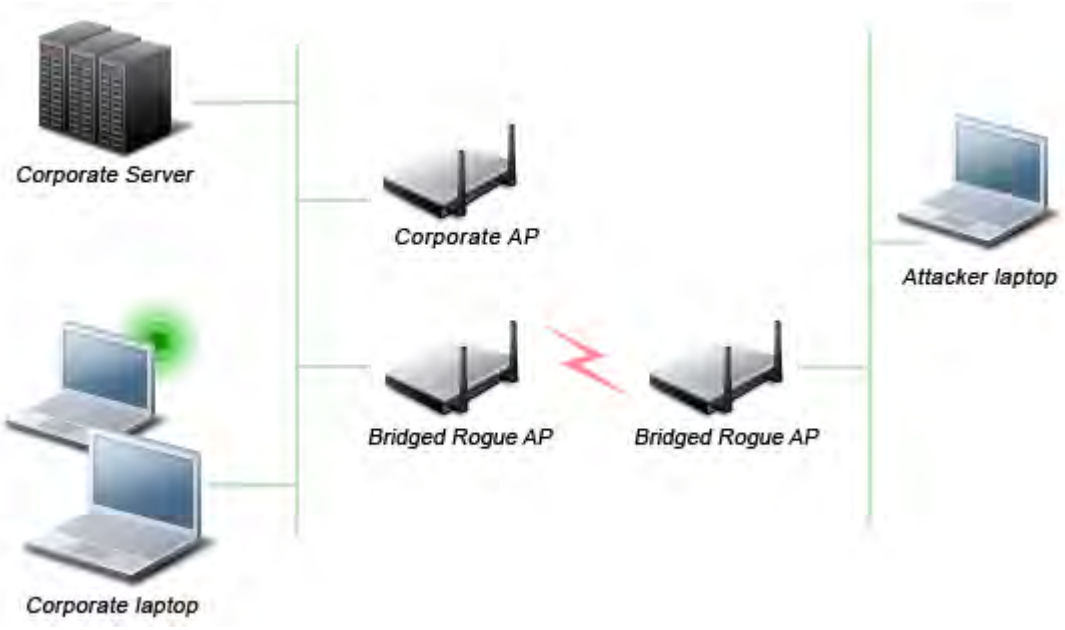
AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

AP Operating in Bridged Mode Detected

Alarm Description & Possible Causes

Access Points are the most commonly used infrastructure products for WLAN networks. An AP will act as a centralized hub through which different wireless devices can connect to the wired distribution network. There are access points that are available that can operate in both the access point mode as well as the bridged mode. Most of them can operate in either mode at a time, though there are a few vendor devices that support both modes simultaneously. In bridged mode, the wireless bridge can be used to connect two wired LAN segments together. This can be in the point-to-point or point-to-multipoint configuration.

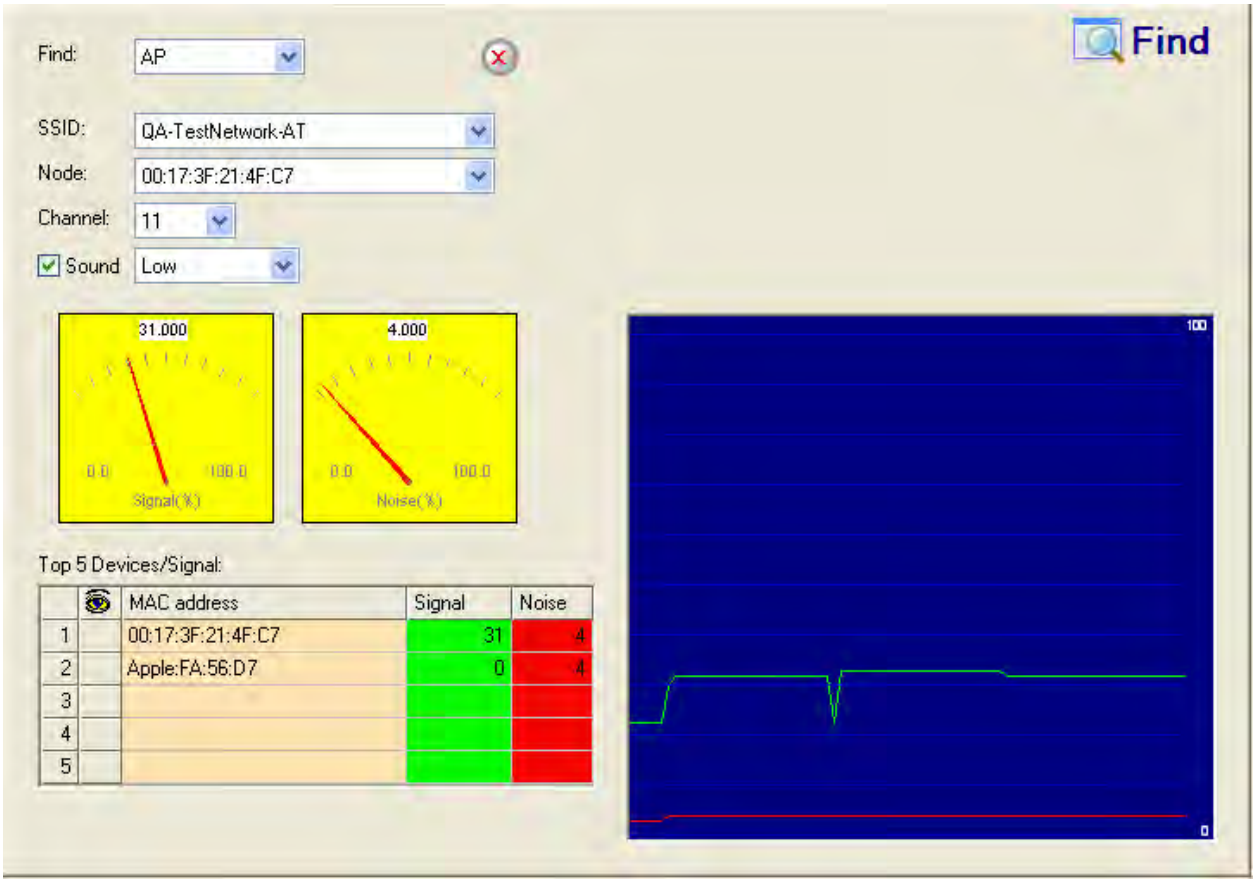
An attacker or a rogue insider could install such a wireless bridge inside the corporate network that would invariably extend the corporate network to any location outside the corporate premises. Detection of such wireless bridge devices indicates that something is wrong and the security of the corporate network could be compromised.



Attacker connects a Rogue Bridged AP / Wireless Bridge to the corporate network and compromises security

AirMagnet Solution

AirMagnet WiFi Analyzer will alert the administrator when it detects a wireless bridge. Once a Rogue AP running in the bridged mode is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

EAP Attack Against 802.1x Authentication Type

Alarm Description & Possible Causes

IEEE 802.1x provides an EAP (Extensible Authentication Protocol) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Wireless vendors supporting 802.1x or WPA implement authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, TTLS, EAP-FAST and so on. Some of these authentication protocols are based upon the user name and password mechanism, where the user name is transmitted clear without encryption and the password is used to answer authentication challenges.

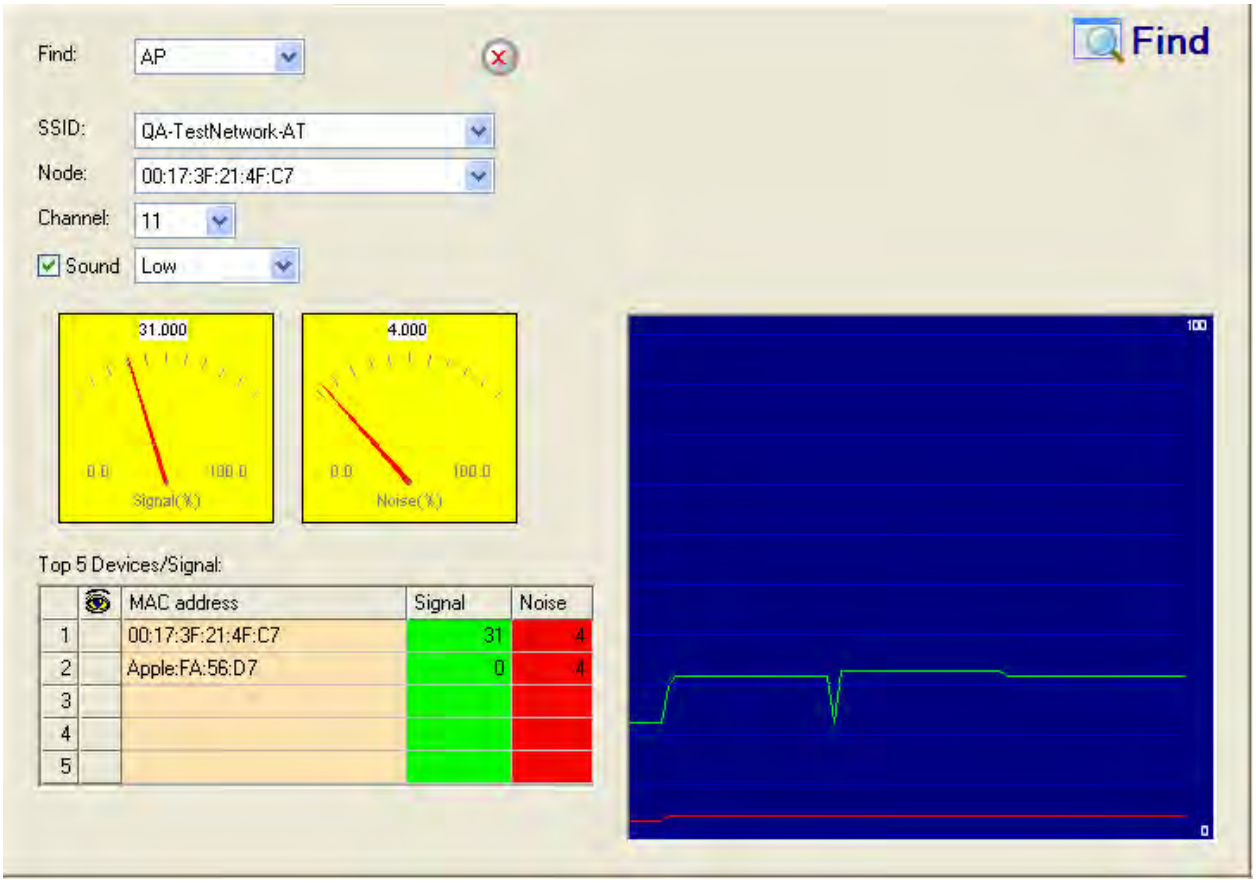
Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker would gain the user name from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user's password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a

common word, name, or concatenation of words or names with a minor modification such as a trailing digit or two.

Intruders with the legitimate 802.1x user identity and password combination (or valid certificate) can penetrate the 802.1x authentication process without the proper knowledge of the exact EAP-type. The intruder will try different EAP-types such as TLS, TTLS, LEAP, EAP-FAST, PEAP, and so on to successfully logon to the network. This is on a trial and error basis, as there are only a handful EAP-types for the intruder to try and somehow manage to get authenticated to the network.

AirMagnet Solution

AirMagnet WiFi Analyzer detects such an attempt by an intruder to gain access to the network using different 802.1x authentication types. Take appropriate steps to locate the device and remove it from the wireless environment. Use the FIND tool for this purpose.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Potential Honey Pot AP Detected

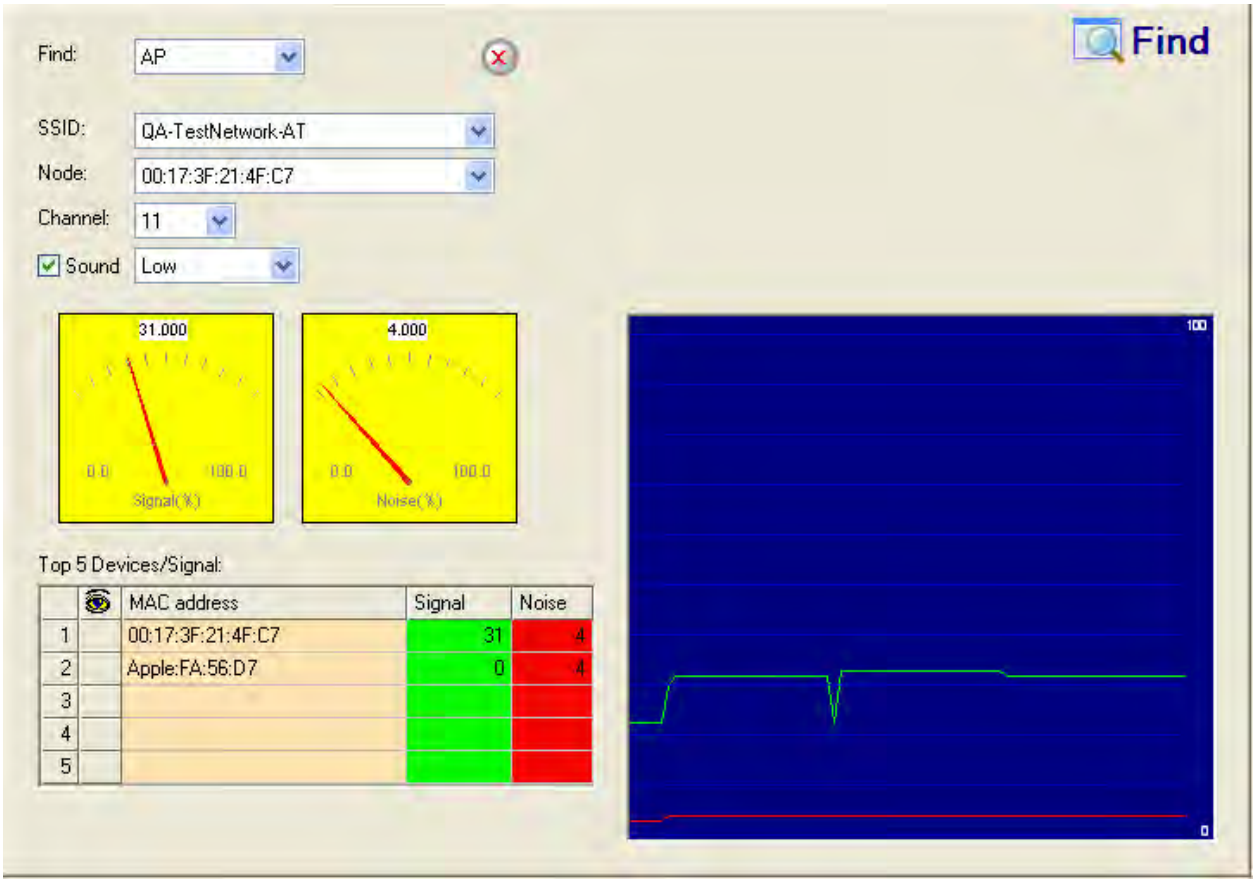
Alarm Description & Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. The Rogue AP can put the entire corporate network at risk of outside penetration and attack. Not to understate the threat of the rogue AP, there are many other wireless security risks and intrusions such as mis-configured AP, unconfigured AP, and Denial-of-Service attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a "Honey pot" AP. An intruder can using different tools such as NetStumbler, Wellenreiter, MiniStumbler, and so on. discover the SSID of the corporate AP. Then the intruder can set up an AP outside the building premises or if possible within the premises and will broadcast the corporate SSID previously discovered. Any unsuspecting client could then connect to this Honey pot AP with a higher signal strength. Once associated, the intruder can perform various attacks against the client station as the traffic will now be diverted through the Honey pot AP.

AirMagnet Solution

Once a Honeypot AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator can use the FIND tool to locate the rogue device.

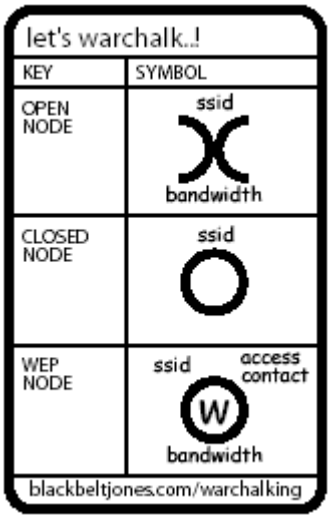


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

NetStumbler Detected

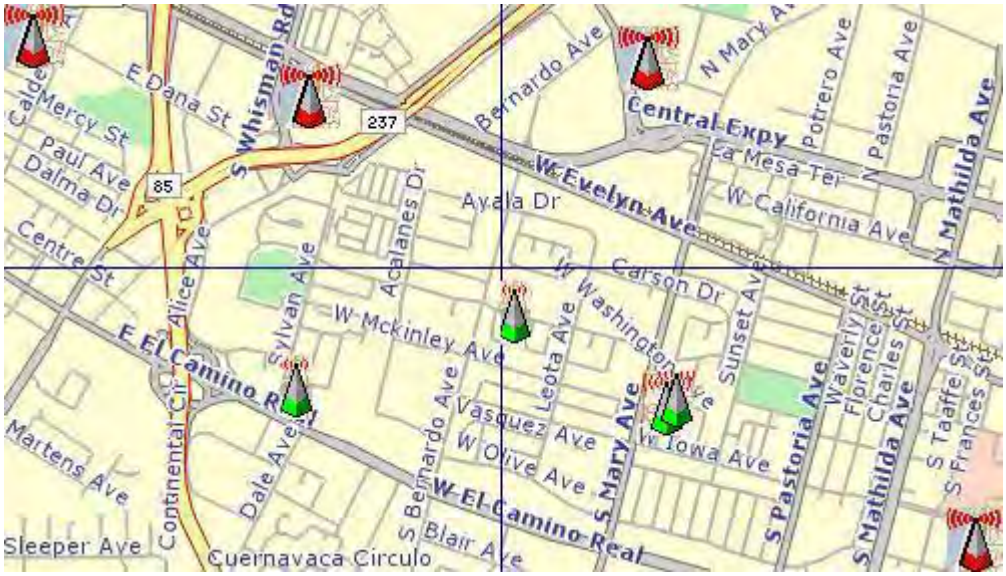
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer detects a wireless client station probing the WLAN for an anonymous association (that is, association request for an AP with any SSID) using the NetStumbler tool. The **Device probing for AP** alarm is generated when hackers use latest versions of the NetStumbler tool. For older versions, AirMagnet Enterprise generates the **NetStumbler detected** alarm.



War-chalker publishes a discovered WLAN and its configuration at the WLAN location with these universal symbols

NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover APs and publish their information (MAC address, SSID, security implemented, and so on) on the Internet with the APs' geographical location information. War-chalkers discover WLAN APs and mark the WLAN configuration at public locations with universal symbols as illustrated above. You can think of war-walking as war-driving, but the hacker is on foot instead of a car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is just as the name implies, sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.



802.11 APs location posted on the Internet by war-driving groups

AirMagnet Solution

To prevent your APs from being discovered by these hacking tools, you can configure your APs to not broadcast their SSIDs. You can use AirMagnet WiFi Analyzer to see which of your APs are broadcasting (announcing) their SSIDs in the beacons.

AP Using Default Configuration

Alarm Description & Possible Causes

Access Points shipped by wireless equipment vendors usually come with a set of default configuration parameters. Until these configuration parameters are set based on your corporate security policy, new Access Points should not be connected to the corporate wired network. Depending on the manufacturer, unconfigured APs have a default administrator password, SSIDs, channels, authentication/encryption settings, SNMP read/write community strings, and so on. Such default values are public knowledge available in user manuals and installation guides on the vendor web site and may be used by wireless hackers to compromise WLAN security.

Default SSID	Vendor / Products
tsunami	Cisco Aironet

Compaq	Compaq WL-100/200/300/400
WLAN	D-Link DL-713
WLAN	SMC SMC2652W/SMC2526W
comcomcom	3Com AirConnect
Intel	Intel Pro/Wireless 2011
Symbol	Symbol Technologies AP
AirPort Network	Apple Airport
Mello	ZCOMMax XWL 450
Roamabout Default Network Name	Lucent, Cabletron, or Enterasys AP
Bridge	SMC SMC2682
MAC address	SOHOware NetBlaster

Sample default SSIDs for APs from different wireless equipment vendors

AirMagnet Solution

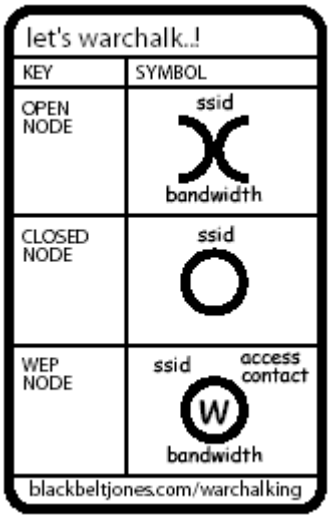
AirMagnet WiFi Analyzer scans the WLAN for unconfigured APs by matching factory default settings against an internal database of well known default configurations such as SSID. When a match is found, AirMagnet WiFi Analyzer alerts the WLAN administrator of the

unconfigured AP. The administrator should change the default settings of the AP to avoid easy hacking of the AP.

Wellenreiter Detected

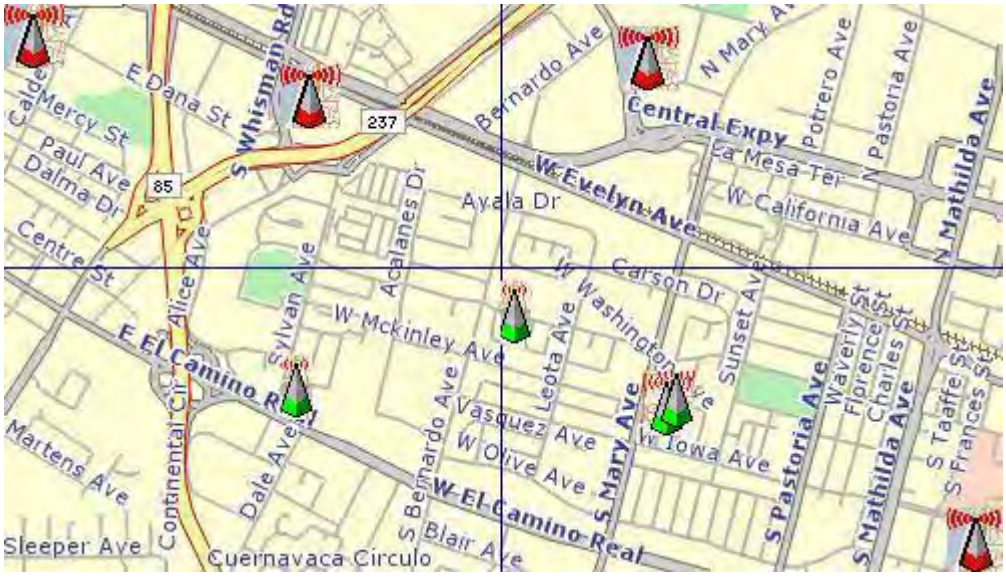
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer detects a wireless client station probing the WLAN for an anonymous association (that is, association request for an AP with any SSID) using the Wellenreiter tool.



War-chalker publishes a discovered WLAN and its configuration at the WLAN location with these universal symbols

Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover APs and publish their information (MAC address, SSID, security implemented, and so on) on the Internet with the APs geographical location information. War-chalkers discover WLAN APs and mark the WLAN configuration at public locations with universal symbols as illustrated above. You can think of war-walking as war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is just as the name implies, sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.



802.11 APs location posted on the Internet by war-driving groups

The tool supports Prism2, Lucent, and Cisco based cards. The tool can discover infrastructure and ad-hoc networks, if those networks are broadcasting their SSID, their WEP capabilities and provides vendor information automatically. It also creates an ethereal/tcpdump-compatible dumpfile and an Application savefile. It also has GPS support. Users can download the tool from http://sourceforge.net/projects/wellenreiter/

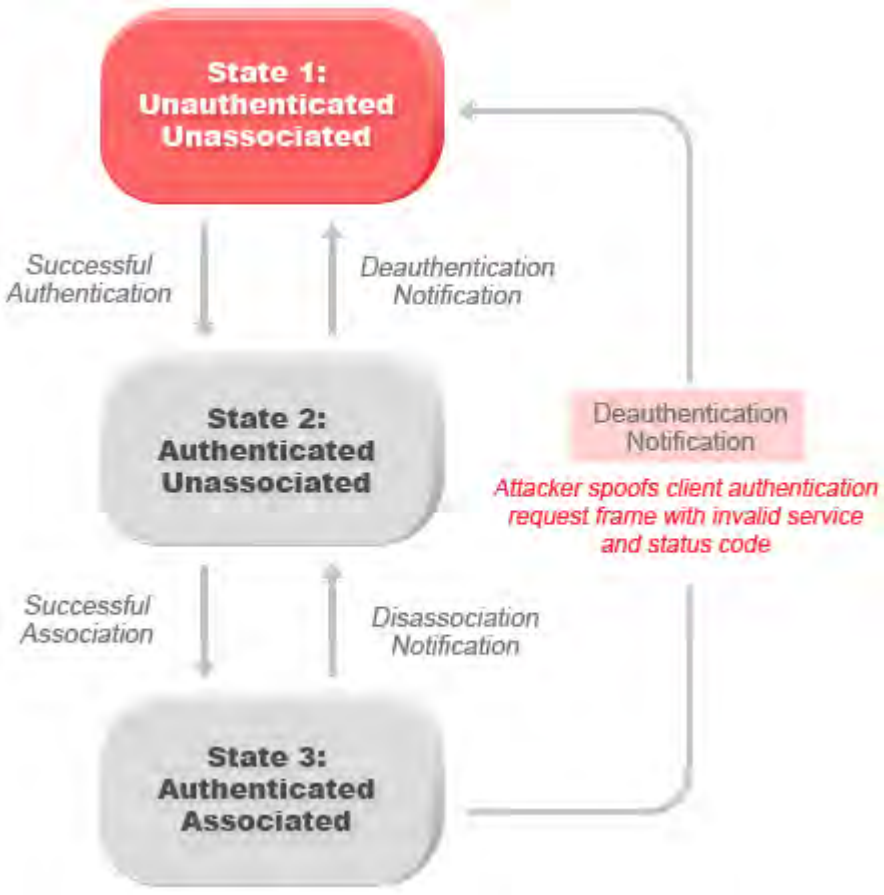
AirMagnet Solution

To prevent your APs from being discovered by these hacking tools, you can configure your APs to not broadcast their SSIDs. You can use AirMagnet WiFi Analyzer to see which of your APs are broadcasting (announcing) their SSIDs in the beacons.

Denial-of-Service Attack: FATA-Jack Tool Detected

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and APs implement such a state machine (illustration below) based on the IEEE standard. A successfully associated client station stays in **State 3** in order to continue wireless communication. A client station in **State 1** and **State 2** cannot participate in the WLAN data communication process until it is authenticated and associated to **State 3**. IEEE 802.11 also defines two authentication services: **Open System Authentication** and **Shared Key Authentication**. Wireless clients go through one of the two authentication process to associate with an AP.



Attacker spoofs invalid authentication requests from associated client station to trick the AP into disassociating the associated client

A form a denial-of-service attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in **State 3** to an AP. Upon reception of the invalid authentication requests, the AP would update the client to **State 1**, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. It does this after it spoofs the MAC address of the Access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

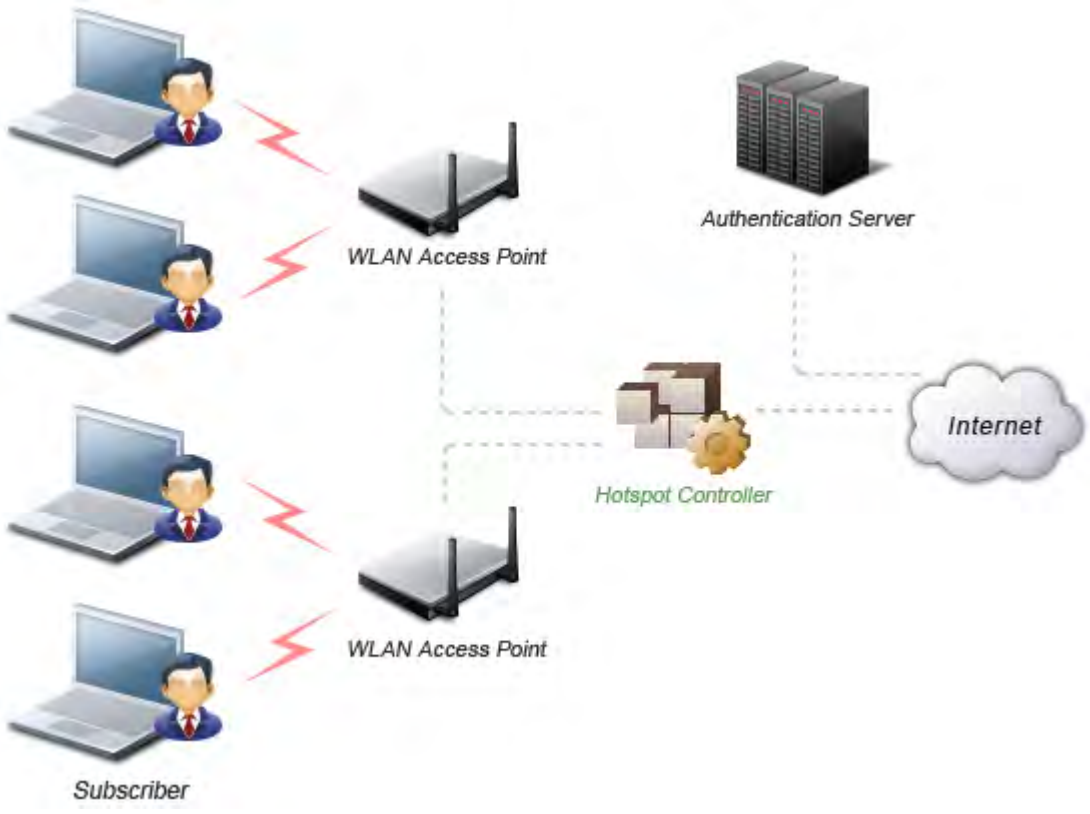
AirMagnet Solution

AirMagnet WiFi Analyzer detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an AP, AirMagnet WiFi Analyzer raises this alarm to indicate a potential intruder's attempt to breach security by brute force computer power. Please note that this alarm focuses on 802.11 authentication methods (Open System, Shared Key, and so on). 802.1x and EAP based authentications are monitored by other AirMagnet WiFi Analyzer alarms.

Device Vulnerable to Hotspot Attack Tools

Alarm Description & possible causes

A hotspot is any location where Wi-Fi network access is made available for the general public. One often finds hotspots in airports, hotels, coffee shops, and other places where business people tend to congregate. It is probably one of the most important network access services for business travelers these days. All the customer requires is a wireless-enabled laptop or handheld. Then the user can connect to the legitimate access point and get the service. Most Hotspots do not require the user to have any advanced authentication mechanisms to connect to the access point, instead simply popping up a web page for the user to login. So, the criterion for entry is dependent only on whether the subscriber has paid the subscription fees or not. In a wireless hotspot environment, one can say that one should not trust anyone else. Due to the concern of security these days, some WLAN Hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.



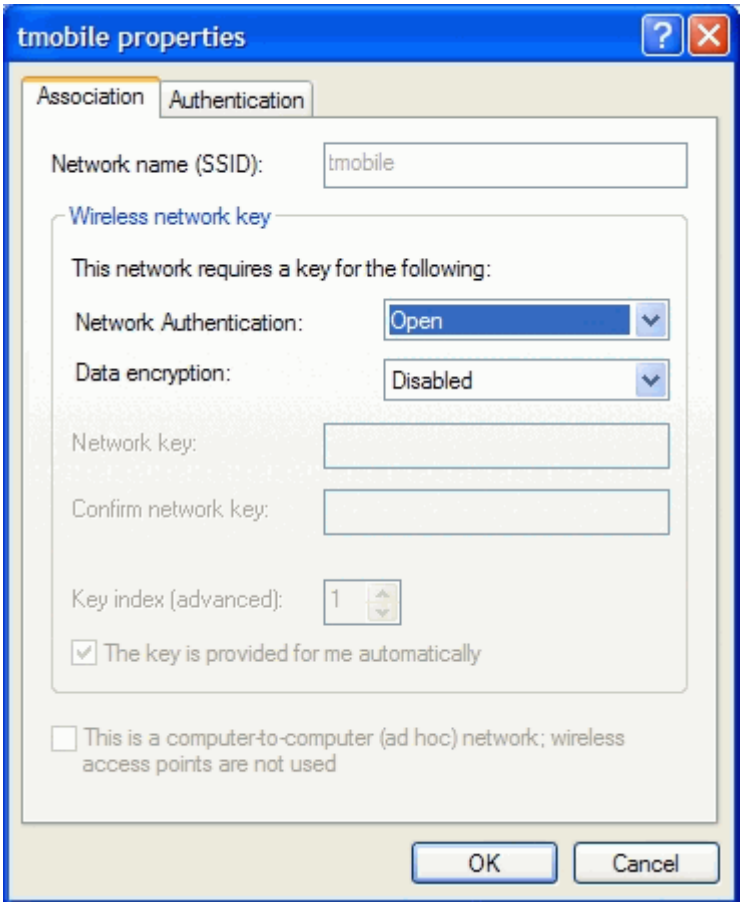
Basic components of a WLAN Hotspot network

The 4 components of a basic Hotspot network are:

- **Hotspot Subscribers:** These are valid users with a wireless enabled Wi-Fi Analyzer or handheld and valid login for accessing the Hotspot network.

- **WLAN Access Points:** These can be SOHO gateways or enterprise level access points depending upon the Hotspot implementation.
- **Hotspot Controller:** This box deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine or can be incorporated in the access point itself.
- **Authentication Server:** This server contains the login credentials for the subscribers. The Hotspot controller will, in most cases, verify the credential for the subscriber with the authentication server after it is received.

The Hotspot users will have SSID configured in their Windows wireless settings or in the WLAN card profile. The wireless card will be sending out probe requests with the Hotspot SSID. This will make the client stations vulnerable to attacks by tools like Airsnarf and Hotspotter.



Network Settings for the client adapter

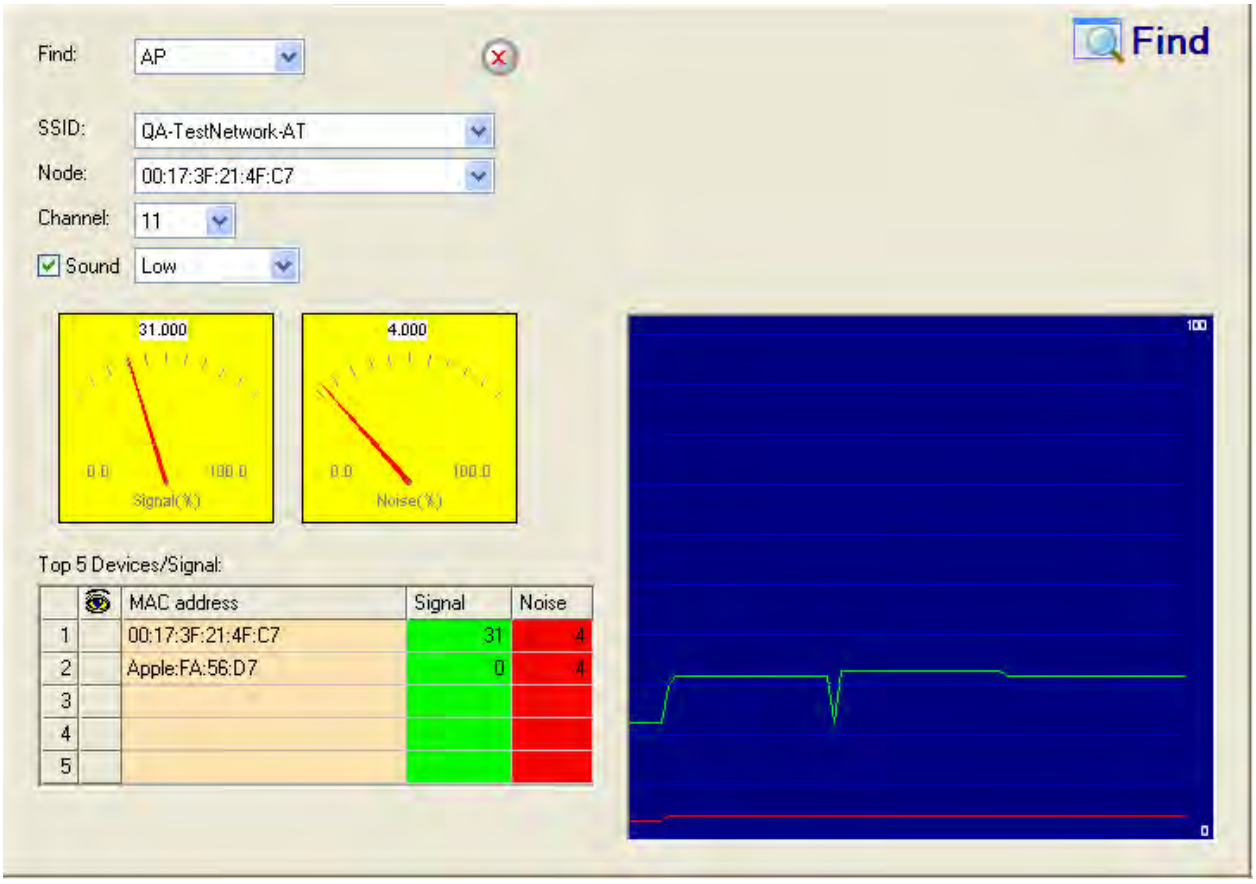
Commonly used attack tools automate a method of penetration against wireless clients, independent of the encryption mechanism used. Using the attack tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows clients. After it gets the preferred network information, the intruder can then compare the network name (SSID) to a supplied list of commonly used hotspot network names. Once a match is found, the attack client will now act as an access

point. The clients can then authenticate and associate unknowingly to this Fake AP. Once the client gets associated, the attack tool can be configured to run a command, possibly a script to kick off a DHCP daemon and other scanning against the new victim. **Hotspotter** is one such tool.

Airsnarf is a wireless access point setup utility to show how a hacker can steal username and password credentials from public wireless hotspots. Airsnarf, a shell script based tool creates a hotspot complete with a captive portal where the users enter their login information. Important values such as local network information, gateway IP address, and SSID to assume can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal, that will disassociate the hotspot wireless clients from the authorized AP connected to the Internet. The wireless clients assuming that they were temporarily disconnected from the Internet due to some unknown issue, will try to login again to resume their activities. Innocent wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf Access Point instead of the legitimate AP installed by the hotspot operator. The users will be shown a webpage that requests a username and password as now the DNS queries are resolved by the rogue Airsnarf AP. The username and password entered will be mailed to *root@localhost*. The user name and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it could have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme. The AirSnarf tool can be downloaded by hackers from http://airsnarf.shmoo.com/

AirMagnet Solution

AirMagnet WiFi Analyzer detects client stations that are using SSIDs configured for use in the Hotspot environment. AirMagnet Wi-Fi Analyzer suggests that the administrator use the AirMagnet Find tool to locate the clients and take appropriate steps to avoid probing using the Hotspot SSID.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Streaming Traffic from Wireless Device

Alarm Description & possible causes

The WLAN spectrum is a shared medium with a limitation on bandwidth. Be it 802.11b at 11 mbps or 802.11a/g at 54 mbps, bandwidth utilization should be closely monitored on a per channel and per device basis to ensure sufficient WLAN provisioning for all client devices. This makes it very important for administrators to ensure that a single client station should not use up the entire bandwidth. For example, enterprise networks could have a problem due to an authorized user who is downloading music or movies from the Internet causing the bandwidth of the corporate network to choke. Music, movie streaming, wireless cameras cause constant traffic to flow on the wireless network.

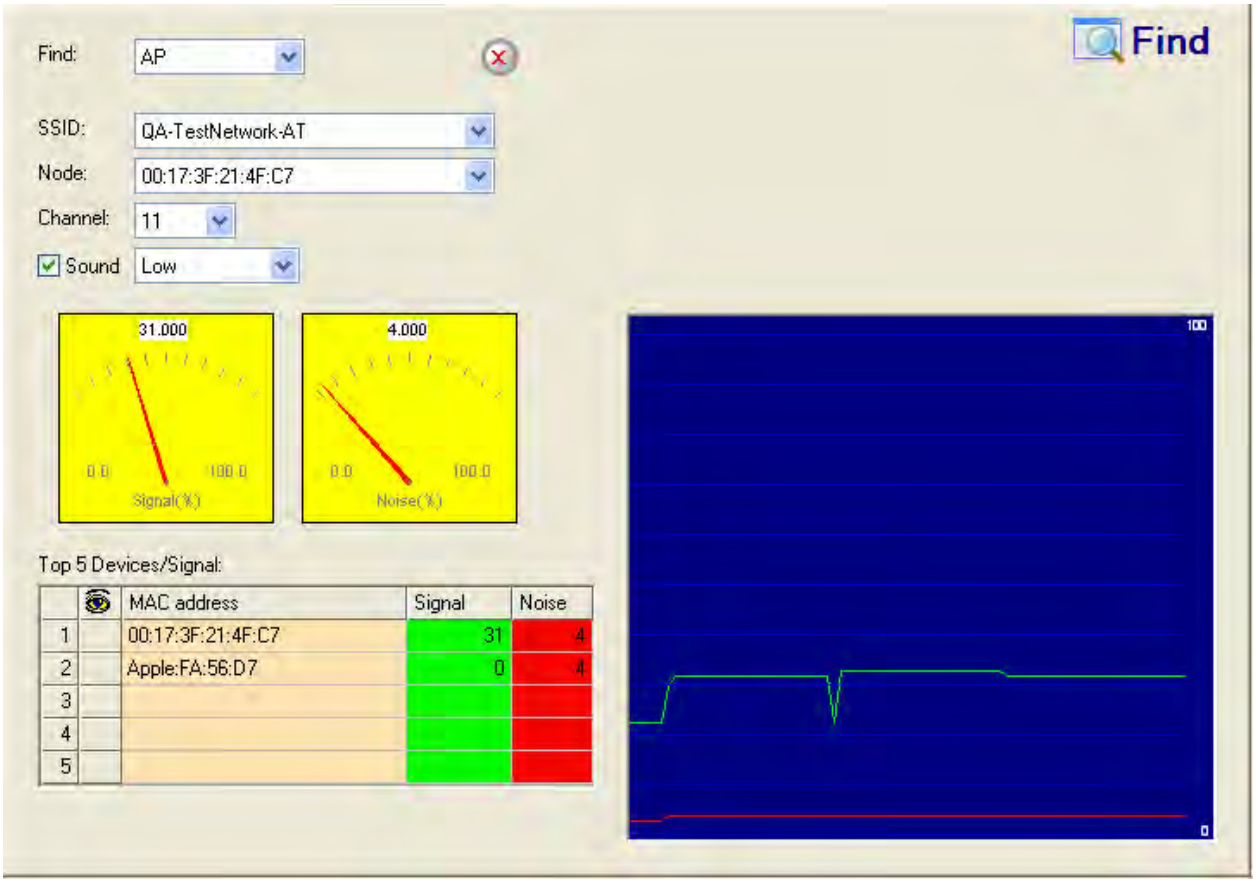
Streaming traffic from wireless PC

Streaming applications though may not be a critical problem for wired networks, but can cause significant impact to the wireless networks especially VoWLAN (Voice over WLAN).

AirMagnet Solution

AirMagnet WiFi Analyzer tracks such wireless client stations that are constantly streaming data over the wireless network over a specified amount of time. AirMagnet advises the user to locate such stations and take appropriate action to disconnect it from the wireless network or instruct the person to avoid using the wireless network for these activities.

Once the streaming client is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the streaming device.

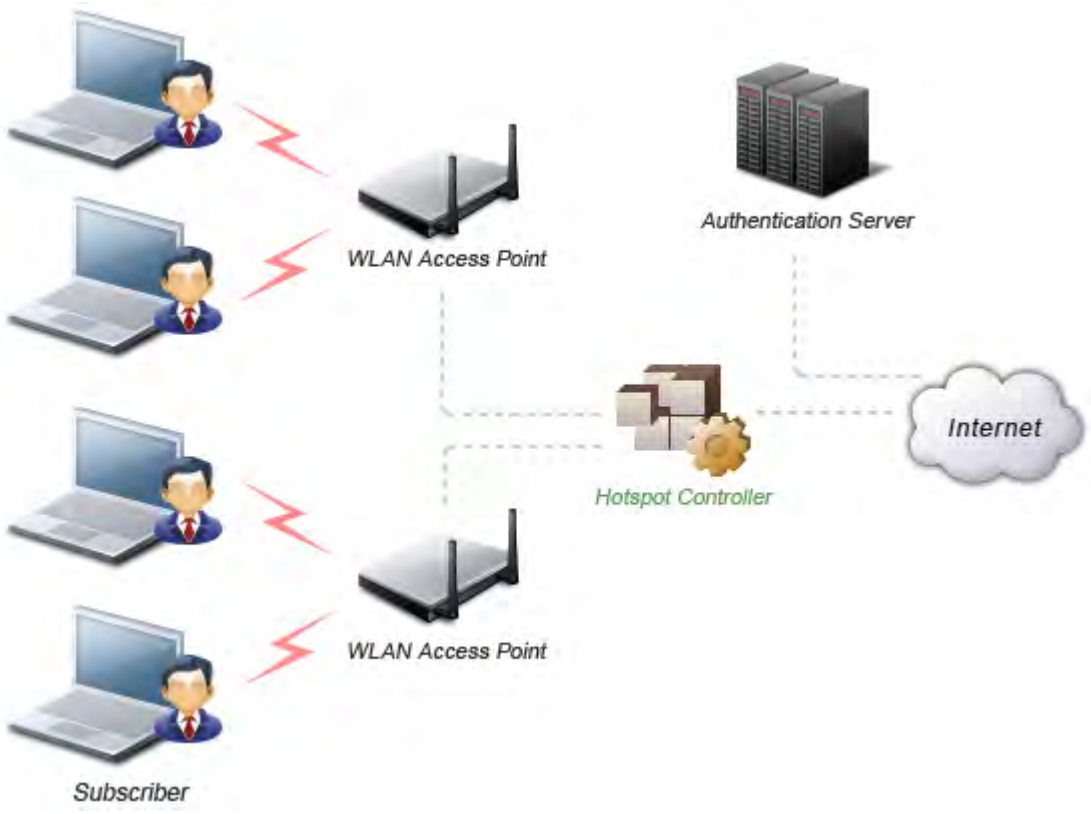


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Hotspotter Tool Detected (Potential Wireless Phishing)

Alarm Description & Possible Causes

A hotspot is any location where Wi-Fi network access is made available for the general public. One often finds hotspots in airports, hotels, coffee shops, and other places where business people tend to congregate. It is probably one of the most important network access service for business travelers these days. All the customer requires is a wireless enabled laptop or handheld. Then the user can connect to the legitimate access point and get the service. Most hotspots do not require the user to have any advanced authentications mechanism to connect to the access point, other than popping up a web page for the user to login. So, the criterion for entry is dependent only on whether the subscriber has paid the subscription fees or not. In a wireless hotspot environment, one can say that one should not trust anyone else. These days due to the concern of security, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.



Basic components of a WLAN Hotspot network

The 4 components of a basic hotspot network are:

- **Hotspot Subscribers:** These are valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.
- **WLAN Access Points:** These can be SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- **Hotspot Controllers:** This box deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine, or can be incorporated in the access point itself.
- **Authentication Server:** This server contains the login credentials for the subscribers. The hotspot controller will, in most cases, verify the credential for the subscriber with the authentication server after it is received.

"Hotspotter" automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitors the wireless network for probe request frames to identify the SSIDs of the networks of the Windows clients.

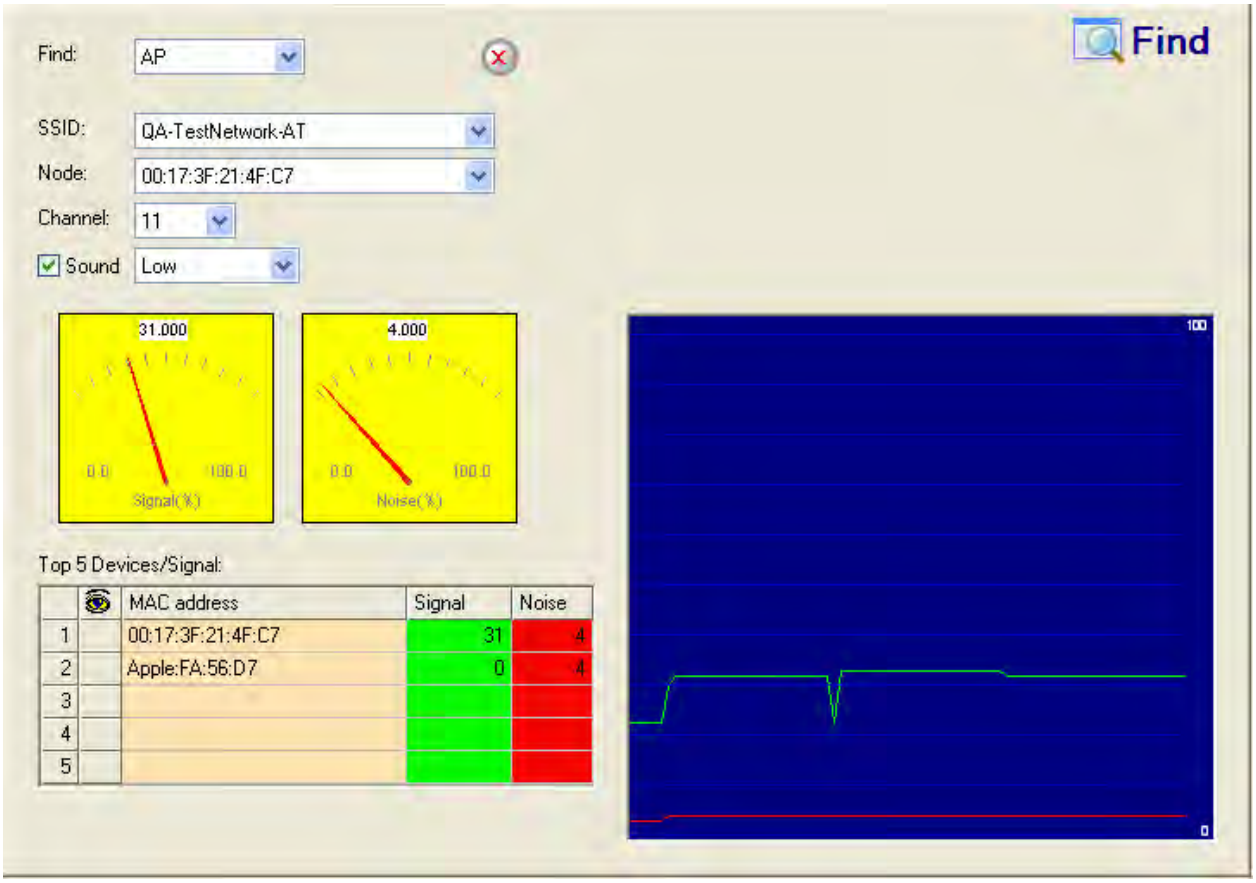
After it gets the preferred network information, the intruder can then compare the network name (SSID) to a supplied list of commonly used hotspot network names. Once a match is found, the Hotspotter client will now act as an access point. The clients can then authenticate and associate unknowingly to this Fake AP.

Once the client gets associated, the Hotspotter tool can be configured to run a command, possibly a script to kick off a DHCP daemon and other scanning against the new victim.

The clients are susceptible to this kind of attack not only in the hotspot environment, but also when they are operating in different environments (home and office) when they are still configured to include the hotspot SSID in the Windows wireless connection settings. The clients will send out probe requests using that SSID and will make themselves vulnerable to the tool.

AirMagnet Solution

Once the Rogue AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

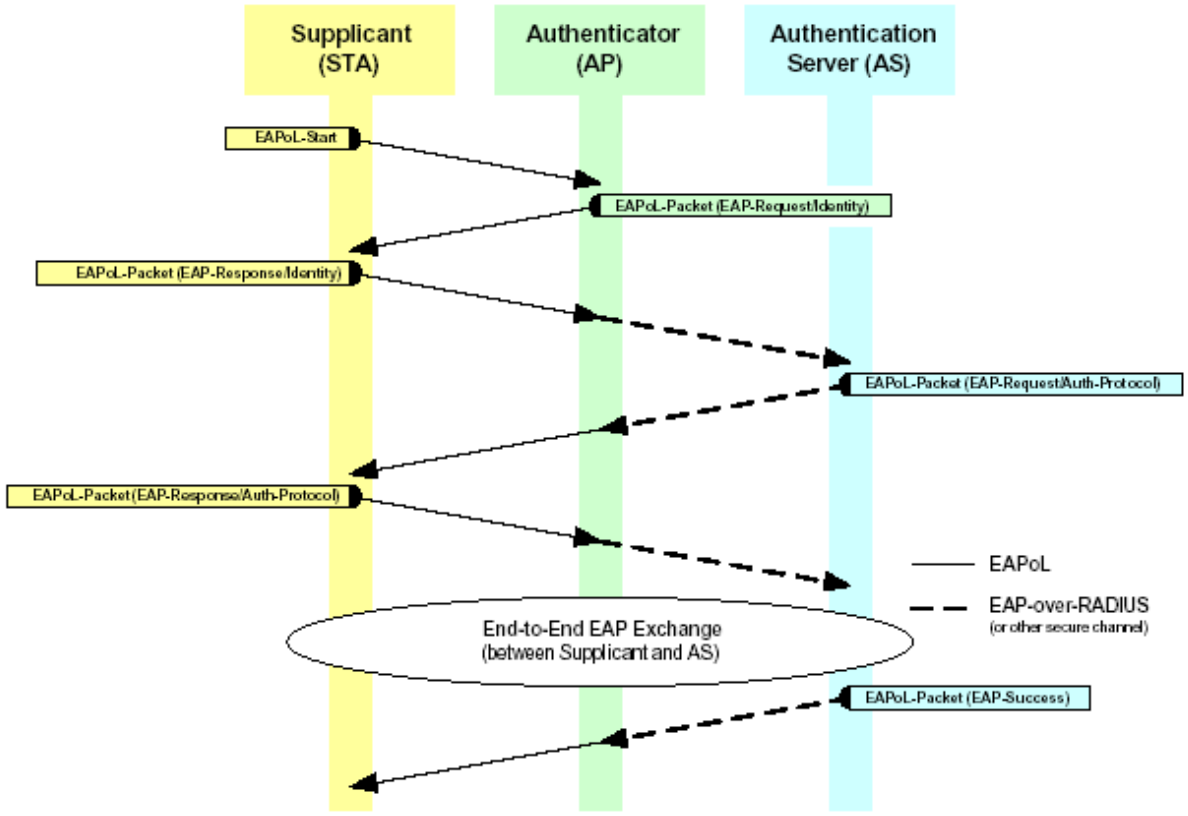
Device Unprotected by IEEE 802.11i/AES

Alarm Description & Possible Causes

The new 802.11i standard provides the much necessary two of the three critical network security capabilities:- authentication and privacy. AirMagnet Enterprise alerts on detecting devices that are not using the IEEE 802.11i standard. Devices that are not using this security standard could be vulnerable to various attacks, compromising the enterprise network's security.

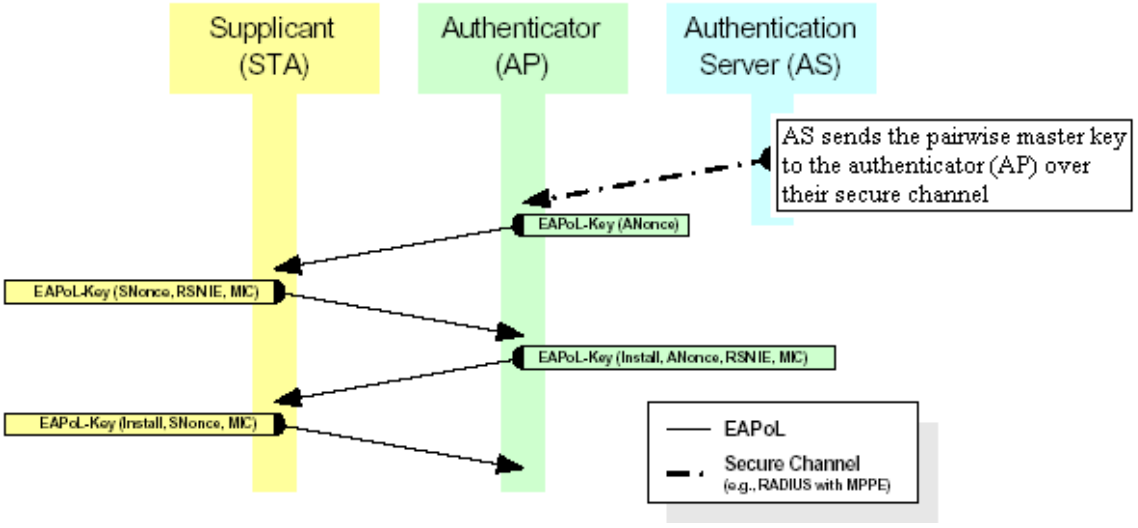
When the IEEE 802.11 standard was ratified it suggested the implementation of the 64-bit WEP key as a security standard. As time passed by, equipment vendors increased this to 128 bit keys as so forth. Some implementations even announced that they were using upto 256 bit WEP keys. Since then, Static WEP has been proved to be flawed with respect to authentication, encryption and integrity checks. Soon the Wi-Fi alliance realized the importance of having an alternative to the WEP standard. The IEEE 802.11i standard was introduced to mitigate all the security issues that have been plaguing the wireless networks in the enterprise environment. This standard creates Robust Secure Networks (RSN).

As the 802.11i standard would not be ratified in time, the Wi-Fi Alliance created a subset of the IEEE 802.11i standard called Wi-Fi Protected Access (WPA).WPA/802.11i implements 802.1x for user authentication and key distribution. 802.1x is used with a variety of **(Extensible Authentication Protocol) types such as LEAP, TLS**, **TTLS**, **EAP-FAST** and **PEAP** to implement an authentication and encryption mechanism. The IEEE 802.11i standard leaves it upto the user to select the authentication scheme.



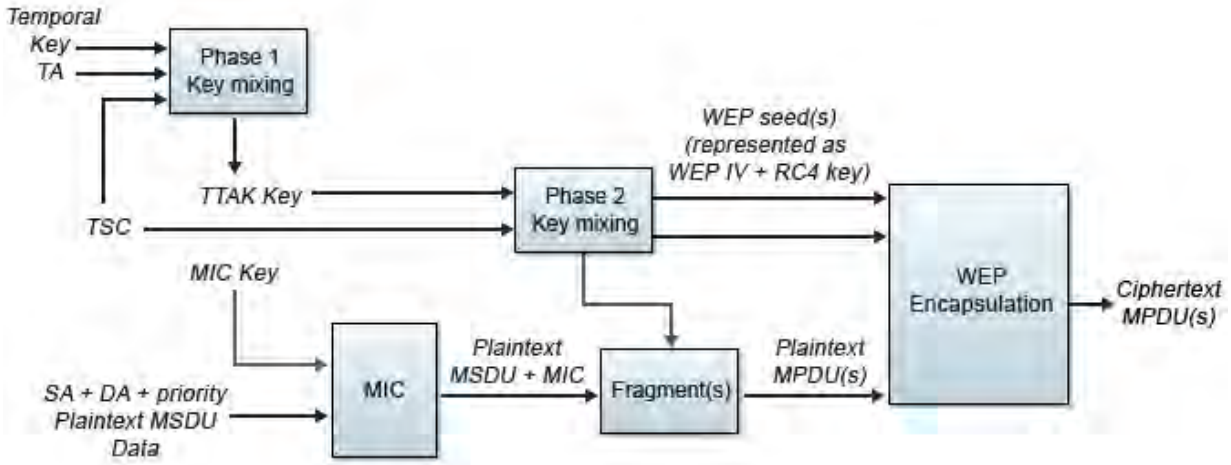
802.1x framework provides centralized user authentication and encryption key management

The IEEE 802.11i standard provide a pre-shared key (PSK) mechanism and the 802.1x-server based key management schemes. The server based mechanism requires an authentication server such as a RADIUS server to securely and dynamically distribute session keys (Pairwise Master Key or PMK). When PSK is used instead of 802.1x, the passphrase PSK is converted via a formula into a 256-bit value needed for the Pairwise Master Key. In the PSK mode, the 802.11i defined 4-way handshake is used for encryption key management, with no EAP exchange. As there is no RADIUS server and no EAP methods (EAP-TLS, LEAP) involved, the PSK mode is less secure.

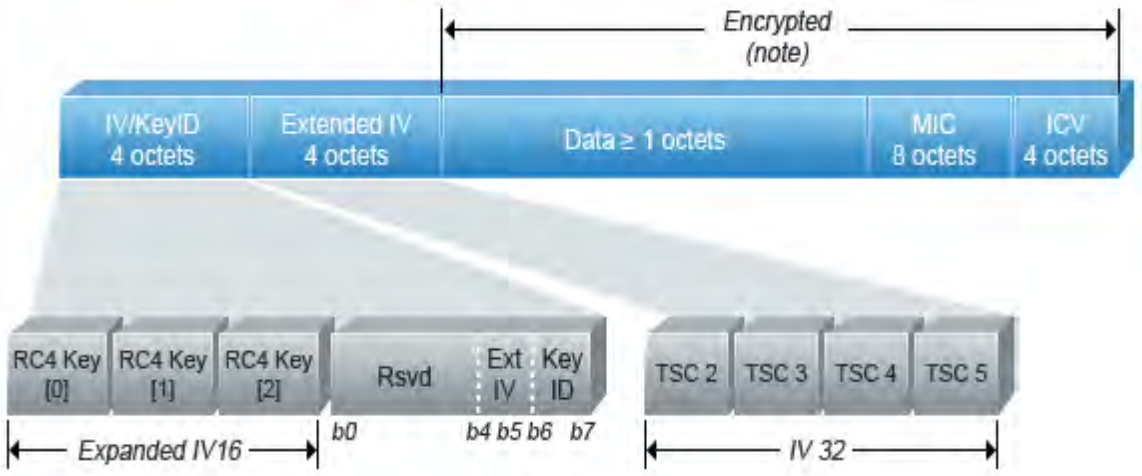


4-way handshake completes the key exchange for the Pre-shared Key mode operation (Authenticator AP and Authentication Server AS are on the AP device)

There are two encryption standards defined in the IEEE 802.11i standard, Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard-Counter Mode-CBC MAC Protocol. WLAN traffic encrypted with TKIP and MIC defeats packet forgery, and replay attack. TKIP is most importantly immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with MIC, TKIP also provides per packet key mixing which helps prevent many keystream attacks.



TKIP and MIC encryption algorithm addresses the weakness of static WEP as well as defeating packet forgery and replay attack

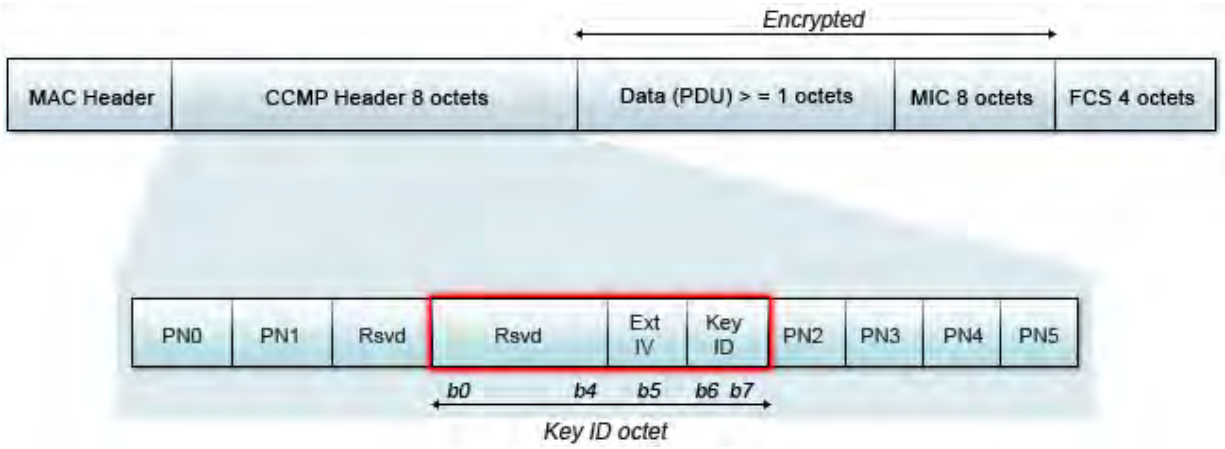


TKIP and MIC encrypted frames expands the original data by 20 bytes for stronger encryption and integrity check

The implementation of AES-CCMP is mandatory for the IEEE 802.11i standard. The IEEE standard supports only the 128-bit AES. As AES is supposed to work on 128-bit blocks, CCMP provides the padding necessary to increase the bit size for the data block. This padding is added before encryption and is discarded after the decryption.

AES-CCMP mode provides authentication and encryption using the AES block cipher. CCMP is a combination of the Counter (CTR) mode encryption for data privacy, and Cipher Block Chaining Message Authentication Code (CBC-MAC) authentication, for an authenticate-and-encrypt security process for each data block processed. CCMP computes the CBC-MAC over the IEEE 802.11 header length, selected parts of the IEEE 802.11 MAC Payload Data Unit (MPDU) header, and the plaintext MPDU data, whereas the old IEEE 802.11 WEP mechanism

provided no protection to the MPDU header. Second, both CCMP encryption and decryption use only the forward AES block cipher function leading to significant savings in code and hardware size.



CCMP MPDU

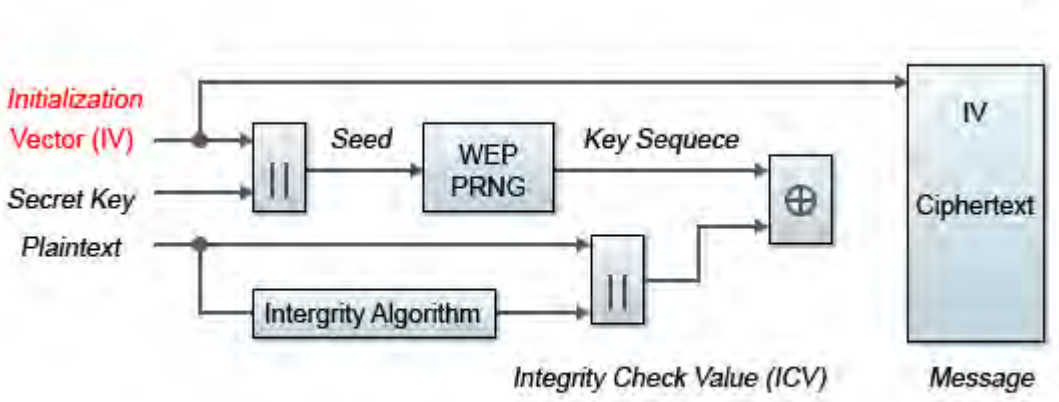
AirMagnet Solution

AirMagnet WiFi Analyzer alerts on detecting devices that are not using the IEEE 802.11i standard and possibly compromising the security of the wireless network. AirMagnet WiFi Analyzer recommends that the user take the appropriate steps to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Fast WEP Crack (ARP Replay) Detected

Alarm Description & Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to ***Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir***).



WEP Encipherment Block Diagram

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user concatenated with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150K unique IVs and for 128-bit WEP keys around 500k to a million unique IVs should be enough. In case there is not sufficient traffic, hackers have come with a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them again and again, the other host will respond with encrypted replies thus providing new and possibly weak IVs.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the **TKIP** (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. **TKIP** enabled devices are not subject to any such WEP key attacks.

AP Overloaded by Voice Traffic

Alarm Description & Possible Causes

A WLAN Access Point has only limited resources and therefore it can service only a limited number of clients. When the limit is reached, additional clients may find their service requests rejected or existing clients may experience degraded performance. This is

unacceptable in an environment implementing VoWLAN phones. When designing the WLAN equipment deployment and the provisioning for service, this limitation should be considered. The most important thing to remember is that typically one AP supporting VoWLAN traffic is used to provide voice services for 6 to 8 phones and that the issues with voice are drastically different than those that arise with normal data transfers on the wireless network. After deployment, as the number of users grows, it may become increasingly difficult for the existing deployment to maintain constant service. This situation requires constant monitoring in case problems arise.

AP overloaded with VoWLAN phones

In certain scenarios, roaming VoWLAN clients may detect an AP with better signal reception and try to roam to that AP. However, if this particular AP is overloaded with other clients or has high bandwidth utilization, the VoWLAN calls may be choppy and experience degraded performance.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors on the AP work load by tracking its active VoWLAN clients. You can configure the system to generate an alarm based on the number of phones supported by each AP on your network. This allows you to ensure that you know when a given AP may be unable to handle more connections; in this case, you may wish to add additional APs to your existing infrastructure in order to support your increasing demand. Alternatively, you may also attempt to reduce the workload by eliminating some unnecessary connections, if possible. You can use the Infrastructure screen to determine which devices are connecting to a given AP, and by using this knowledge, narrow down which devices (if any) may be removed from your network.

Channel Overloaded by Voice Traffic

Alarm Description & Possible Causes

As per the IEEE 802.11e standard for QoS, the QoS basic service set (QBSS) is a basic service set (BSS) that supports LAN applications with quality of service (QoS) requirements by providing a QoS facility for communication via the wireless medium. With the introduction of the IEEE 802.11e standard, there have been a few changes to the format of the original 802.11 frames. Amongst many other frames, the beacon and the probe response frame now include new entries if the information is pertaining to Quality of Service (QoS).

Usage	Order	Information	Note
Always Present	1	*Timestamp*	
	2	*Beacon interval*	
	3	*Capability information*	
	4	*SSID*	
	5	*Supported rates*	
Present if required by PHY type, BBS type, or an active point coordinator (see notes)	6	*FH parameter Set*	*The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency hopping PHYs.*
	7	*DS Parameter Set*	*The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.*
	8	*CF Parameter Set*	*The CF Parameter Set information element is present within Beacon frames generated by APs with an active PC or by QAPs.*
	9	*IBSS Parameter Set*	*The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.*
	10	*TIM*	*The TIM information element is only present within Beacon frames generated by APs in QAPs.*
Multiple regulatory domains	11	*Country Information*	*The Country Information element shall be present when dot11MultipleDomainCapbilityEnabled is true.*
	12	*FH Parameters*	*FH Parameters as specified in clause 7.3.2.13 may be included if dot11MultipleDomainCapbilityEnabled is true.*
	13	*FH Pattern Table*	*FH Pattern Table information as specified in clause 7.3.2.13 may be included if dot11MultipleDomainCapbilityEnabled is true.*
QBSS	14	*QBSS Load*	*The QBSS Load information element is only present within Beacon frames generated by QAPs.*
	15	*QOS Parameter Set*	*The QOS Parameter Set information element is only present within Beacon frames generated by QAPs.*

Beacon frame format as suggested by IEEE 802.11e

Usage	Order	Information	Note
Always Present	1	Timestamp	
	2	Beacon interval	
	3	Capability information	
	4	SSID	
	5	Supported rates	
Present if required by PHY type, BBS type, or an active point coordinator	6	FH parameter Set	The FH Parameter Set information element is present within Probe Response frames generated by STAs using frequency hopping PHYs.
	7	DS Parameter Set	The DS Parameter Set information element is present within Probe Pesponse frames generated by STAs using direct sequence PHYs.
	8	CF Parameter Set	The CF Parameter Set information element is present within Beacon frames generated by APs with an active PC or by QAPs.
	9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Probe Response frames generated by STAs in an IBSS.
Multiple regulatory domains	10	Country Information	Included if dot11MultipleDomainCapbilityEnabled is true.
	11	FH Parameters	FH Parameters as specified in clause 7.3.2.13 may be included if dot11MultipleDomainCapbilityEnabled is true.
	12	FH Pattern Table	FH Pattern Table information as specified in clause 7.3.2.13 may be included if dot11MultipleDomainCapbilityEnabled is true.
	13-n	Requested information elements	Elements requested by the Request information element of the Probe Request frame.
QBSS always present	10	QBSS Load	The QBSS Load information element is only present in Probe Request frames generated by QAPs.
	11	Error Statistics	The Error Statistics information element is only present in Probe Request frames generated by QSTAs in a QBSS.
QBSS present if required	12	Listen Epoch	The Listen Epoch information element is only present in Probe Response frames generated by QSTAs in a QBSS which have an assigned listen epoch.
	13	Extended Capabilities	The Extended Capabilities information element is only present in Probe Response frames generated by QSTAs with Capability Information bit 15=1.

Probe Response frame format as suggested by IEEE 802.11e

Both these frames include the QBSS Load element. The QBSS Load element contains information on the current station population and traffic levels in the QBSS.

Load Element Format

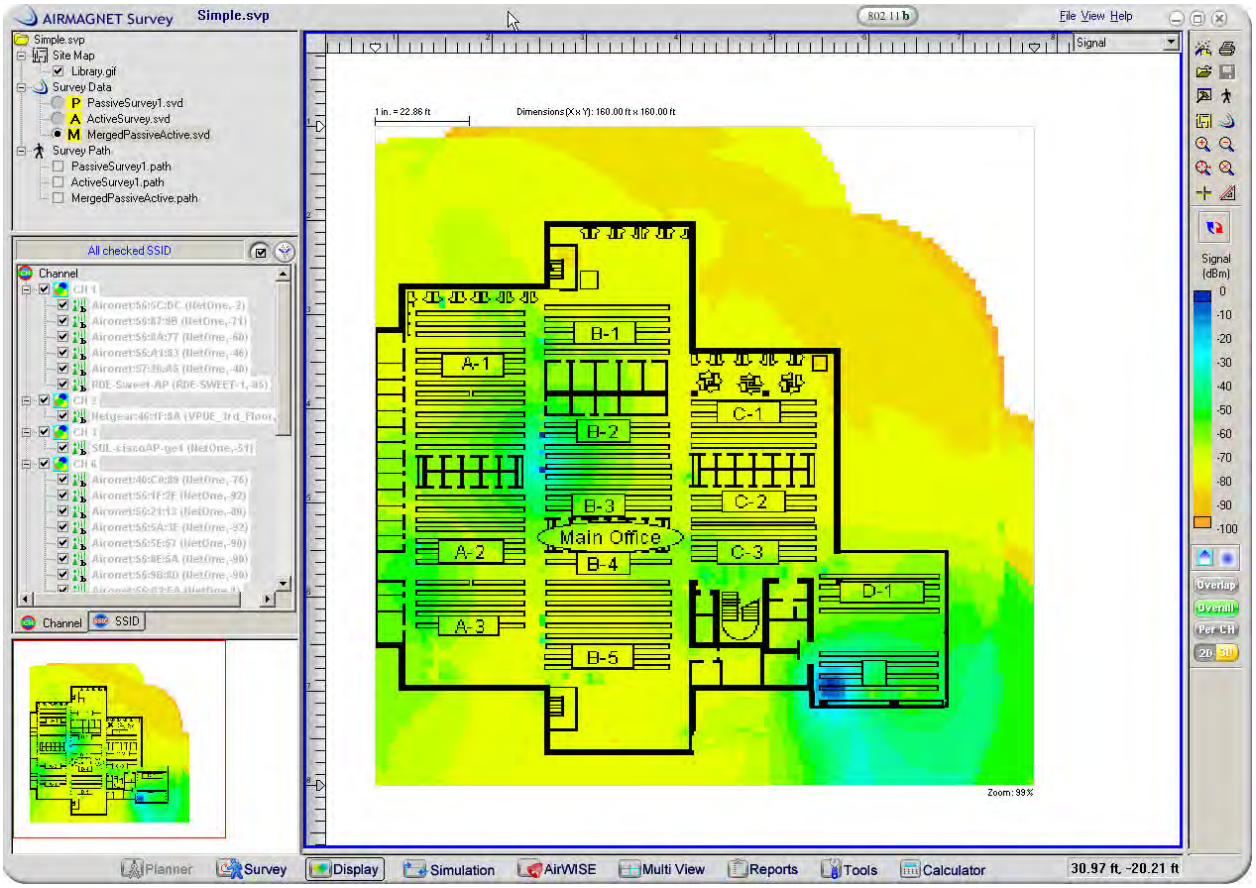
The Channel utilization field indicates the portion of available wireless medium bandwidth currently used to transport traffic within this QBSS.

AirMagnet Solution

AirMagnet recommends keeping the channel utilization to a minimum. One of the simplest ways of doing this is by reducing the number of client devices that talk to a single AP. The other option that is being widely used is going for Dense AP Deployments - a procedure in which APs are installed densely all over the company premises. Though APs are getting cheaper, the overall architecture deployment price is still high.

AirMagnet Survey, part of the AirMagnet WiFi Analyzer Family can help the users implement such a dense deployment. With AirMagnet Survey, networking professionals can:

- Ensure Proper Overall Signal Coverage
- Determine Ideal AP Placement and Power Settings
- Quantitatively Analyze Sources of RF Interference and Noise
- Identify Client Roaming Areas
- Emulate Client Experience to Measure Real-World Connection Speed, Retry Rate and Packet Loss
- Ensure Adequate Bandwidth and Speed for any WLAN



AirMagnet Survey product

Power-Save DTIM Setting not Optimised for Voice

Alarm Description & Possible Causes

The DTIM value plays a major role in VoWLAN applications. Any mis-configurations here may lead to choppy traffic and dissatisfied VoWLAN users, as in the case of higher DTIM values. Most vendors prefer a lower value, which provides satisfactory results for VoWLAN applications. The only downside to this is that the rapid DTIM responses may have a tremendous impact on the battery life of the voice phones or devices. According to the 802.11 standard, the stations have the option of operating in the Power save mode. In this mode, the stations doze off for a specific period of time (based on the number of beacons) and wake up to receive beacons and look for their own identifier in each beacon's Traffic Indication Map. In this way, the stations that wake up find out if there is any traffic buffered for them at the AP once the beacon arrives. After the AP transfers the DTIM, it will transfer the buffered data.

Traffic Indication Map Information Element

The important parameter here is the DTIM period, which indicates how often the AP will transmit the buffered data. This value is directly derived from the beacon interval. For example, if the Beacon period is 100msec and the DTIM value is 3, then the AP will transfer the buffered data every 300msec. Each vendor has their own suggested DTIM value for their APs.

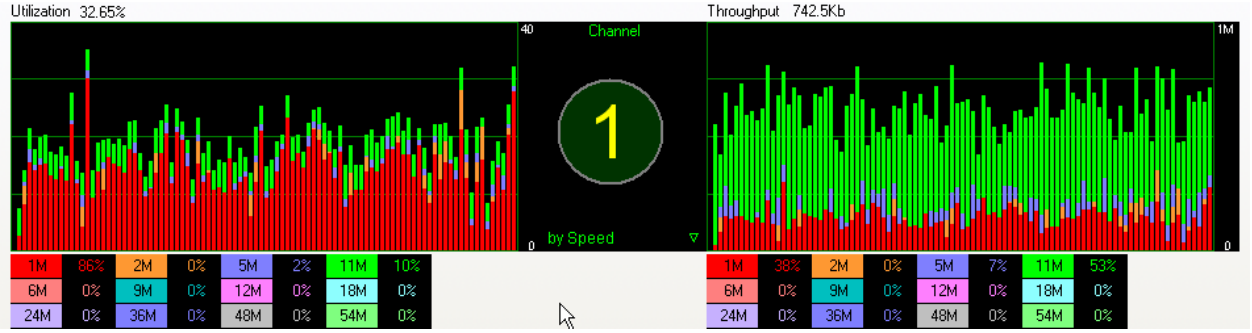
AirMagnet Solution

AirMagnet WiFi Analyzer alerts the WLAN administrator if it sees the DTIM value to be different than the one specified in the alert threshold. Please refer to your AP's documentation to specify a value. AirMagnet recommends checking for proprietary implementation (if available) for improving the functionality of the APs in handling VoWLAN traffic. Some applications allow VoWLAN traffic to bypass the queuing process and be available for immediate transmission.

Excessive Bandwidth Usage

Alarm Description & Possible Causes

The WLAN spectrum is a shared medium with a limitation on bandwidth. Be it 802.11b at 11 Mbps or 802.11a/g at 54 Mbps, bandwidth utilization should be closely monitored on a per channel and per device basis to ensure sufficient WLAN provisioning for all client devices. Please note that high bandwidth consumption does not mean high WLAN throughput. The sample AirMagnet Wi-Fi Analyzer Channel page screen shot below demonstrates 32% utilization but less than 1 Mbps throughput. The problem lies in the low speed transmission, which is also graphically illustrated below by the 1 Mbps traffic bar in the utilization chart. The problem could be due to an authorized user who is downloading music or movies from the Internet causing the bandwidth of the corporate network to choke.



WiFi Analyzer tracks WLAN bandwidth utilization on a per channel and per device basis

AirMagnet Solution

AirMagnet WiFi Analyzer tracks bandwidth utilization based on channel and wireless device. AirMagnet WiFi Analyzer's bandwidth calculation includes the PLCP (Physical Layer Convergence Procedure) header, preamble, and the actual frame payload. Because of the CSMA collision avoidance protocol, it is practically impossible to get even close to 100% utilization. Sixty to seventy percent utilization should be considered extremely high and requires better provisioning or improved efficiency such as strict high speed transmission. When the user-defined threshold (in percentage of utilization) is exceeded, AirMagnet Wi-Fi Analyzer raises this alarm. Take appropriate steps to tackle this problem. This could include finding users who may be causing this due to excessive file downloading from the Internet.

VoWLAN Multicast Traffic Detected

Alarm Description & Possible Causes

An 802.11 Access Point must transmit any multicast/broadcast frames immediately if no mobile stations in the Power Save Polling (PSP) mode are detected. In an enterprise environment, there may often be at least one client in the power saving mode. In such situations, the frames will be queued and transmitted on a Delivery Traffic Indication Map (DTIM) frame interval. This interval can vary (depending on different AP vendors) by as much as 1-2 seconds. Multicast VoWLAN traffic would consequently be delivered when that DTIM period expires, which may lead to choppy voice calls. Further, multicast traffic takes place at lower data rates when a device is associated to the access point, which may lead to degradation of the performance of the wireless LAN network.

There are two different ways of dealing with this issue:

- **Reduce the DTIM value:** Most products allow the user to set this value very low. Though this is a simple solution, rapid DTIM responses may have a tremendous impact on the battery life of the voice phones or devices.
- **Proprietary solutions:** Proprietary solutions can be implemented at the access point level. Some APs allow users to specify a multicast MAC address to identify the voice frame. Once recognized, the AP will allow the frames to bypass the queuing process and make it available for immediate transmission. Other non-specified multicast/broadcast frames will be handled with the normal DTIM procedures. This solution provides a good balance between satisfactory voice quality and battery life. The only disadvantage is that they are proprietary solutions, and thus will only be available on specific devices.

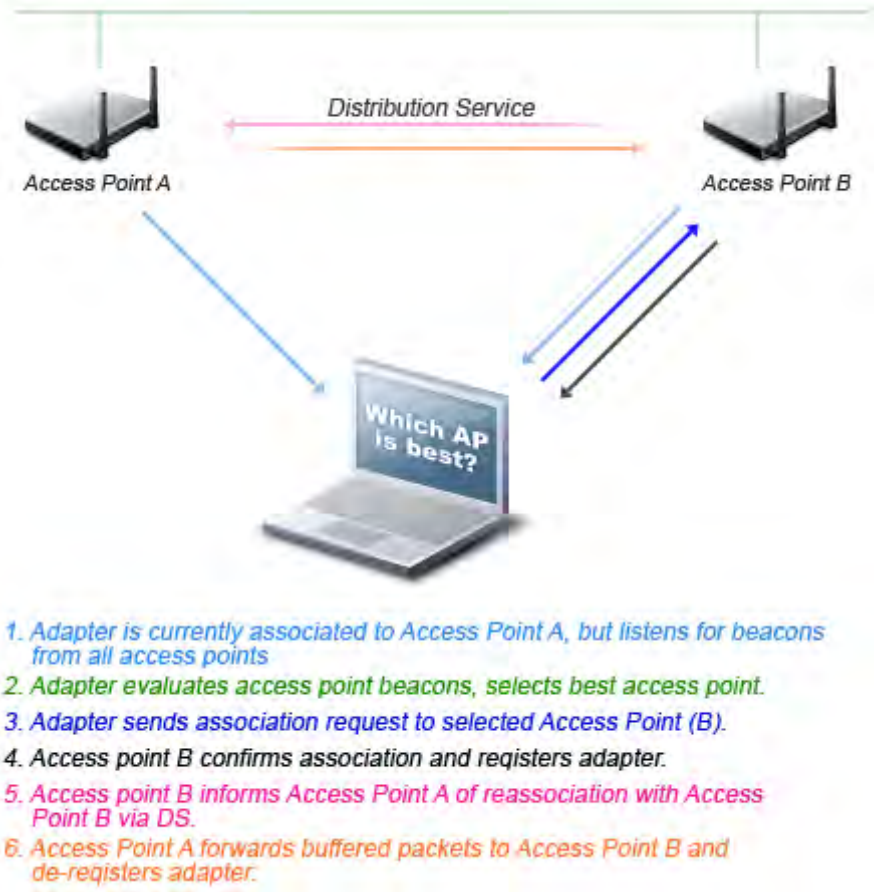
AirMagnet Solution

AirMagnet W-Fi Analyzer detects APs sending out multicast traffic. We recommend avoiding use of multicast traffic for voice applications such as Music on Hold (MoH: A Music on Hold system plays a pre-recorded program for callers to listen to while they are on hold. The system plays music, a voice message, or a combination of both). The user can choose either of the two solutions mentioned above: a) reducing the DTIM value or b) using proprietary solutions (if available).

Excessive Roaming Detected on Wireless Phones

Alarm Description & Possible Causes

After successfully associating with an AP, VoWLAN client devices start using the wireless connection for communication but continue to search for better wireless services (such as another AP with stronger signal strength, less channel noise, or higher supported speed).



A VoWLAN roams to the Best AP for Quality Communication

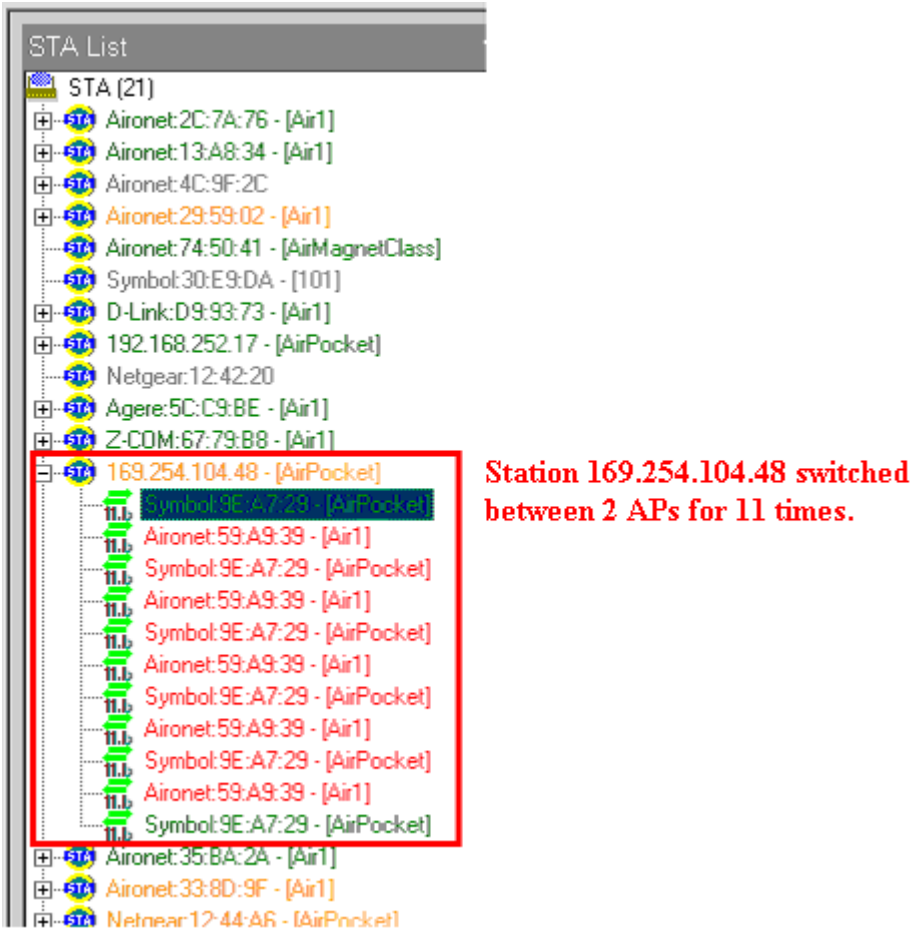
Once an AP with better service is identified, the client station will associate with the new AP and break the association with the original AP. Mobile roaming devices (such as VoWLAN phones and bar code scanners) on a WLAN frequently perform such a re-association act. As the phones roam from one AP to another, the calls may be dropped and the phones may need to undergo a new probe, re-association, and re-authentication. When VoWLAN devices move out of range from one AP and into the range of another, the handoff latency could be anywhere from 400 to 600ms. This is a significant delay, which is not acceptable for Voice transmissions, and will cause the call connection to be dropped. This can be very troublesome to VoWLAN phone users. Further, the existing security standards do not help much in the case of fast roaming; the emerging 802.11r working group is still being developed to improve VoWLAN roaming. Its focus is to reduce the time required to authenticate when roaming, which will help support real-time applications, such as voice. With more advanced WLAN management technologies (such as the ones listed below), client stations are increasingly prone to association changes to adjust to the dynamic RF environment:

- AP load balancing and bandwidth allocation
- Dynamic channel selection to avoid RF interference and dedicated channel bandwidth
- Automatic AP output power adjustment for optimized coverage and capacity

All these technologies improve WLAN efficiency. However, vendor implementations and fine-tuning are not on par with each other. Immature new products may cause confused client stations to frequently re-associate, resulting in disrupted service.

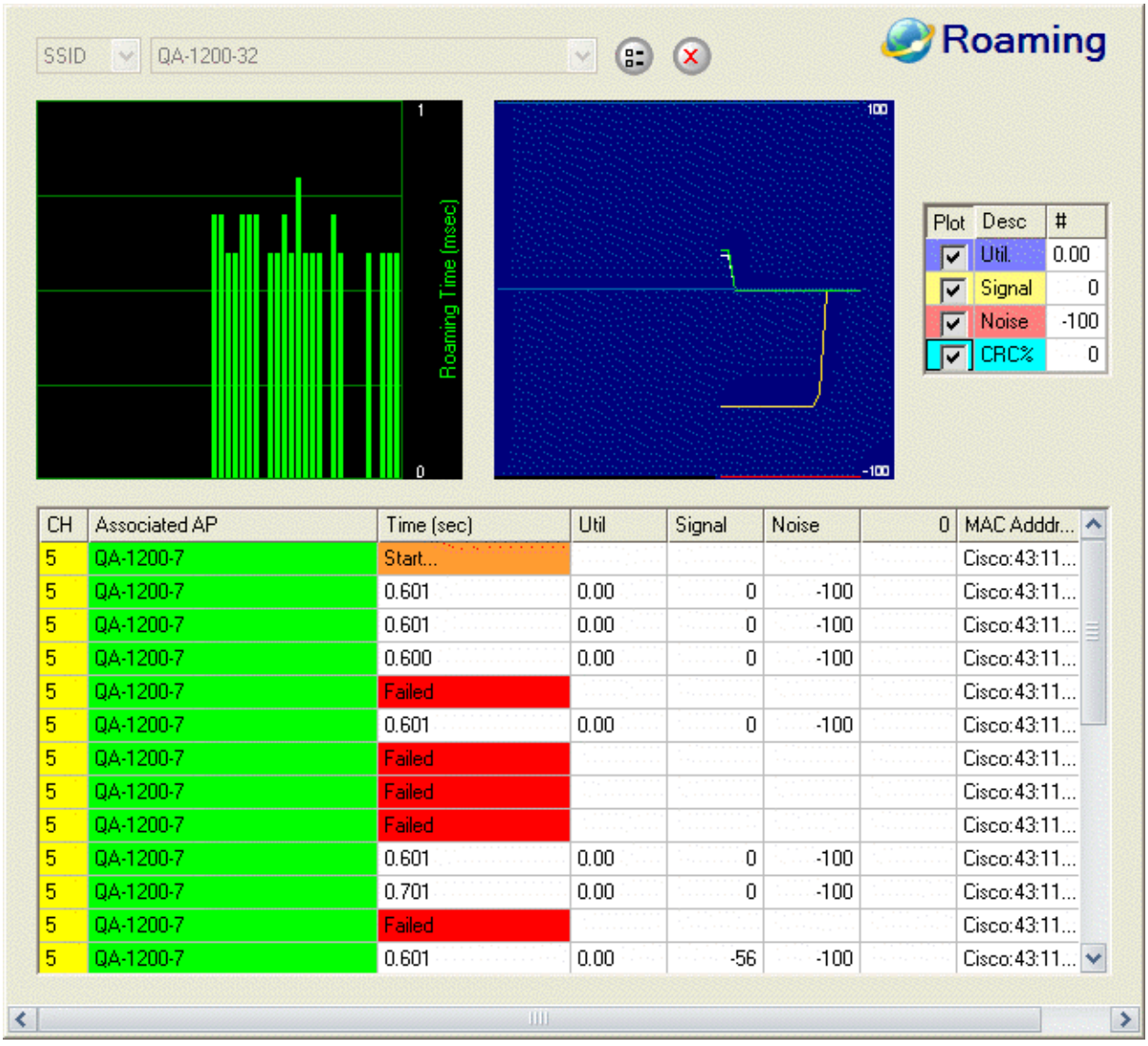
AirMagnet Solution

Stationary devices (such as wireless printers and wireless desktops) are not expected to have repeated re-associations. AirMagnet WiFi Analyzer monitors for excessive VoWLAN re-associations by tracking association counts and APs. Once detected and reported by AirMagnet WiFi Analyzer, this problem can be further investigated by using the station-list to display APs and session characteristics involved (refer to the sample below).



Using the Infrastructure Page *station-List* to investigate excessive roaming problem

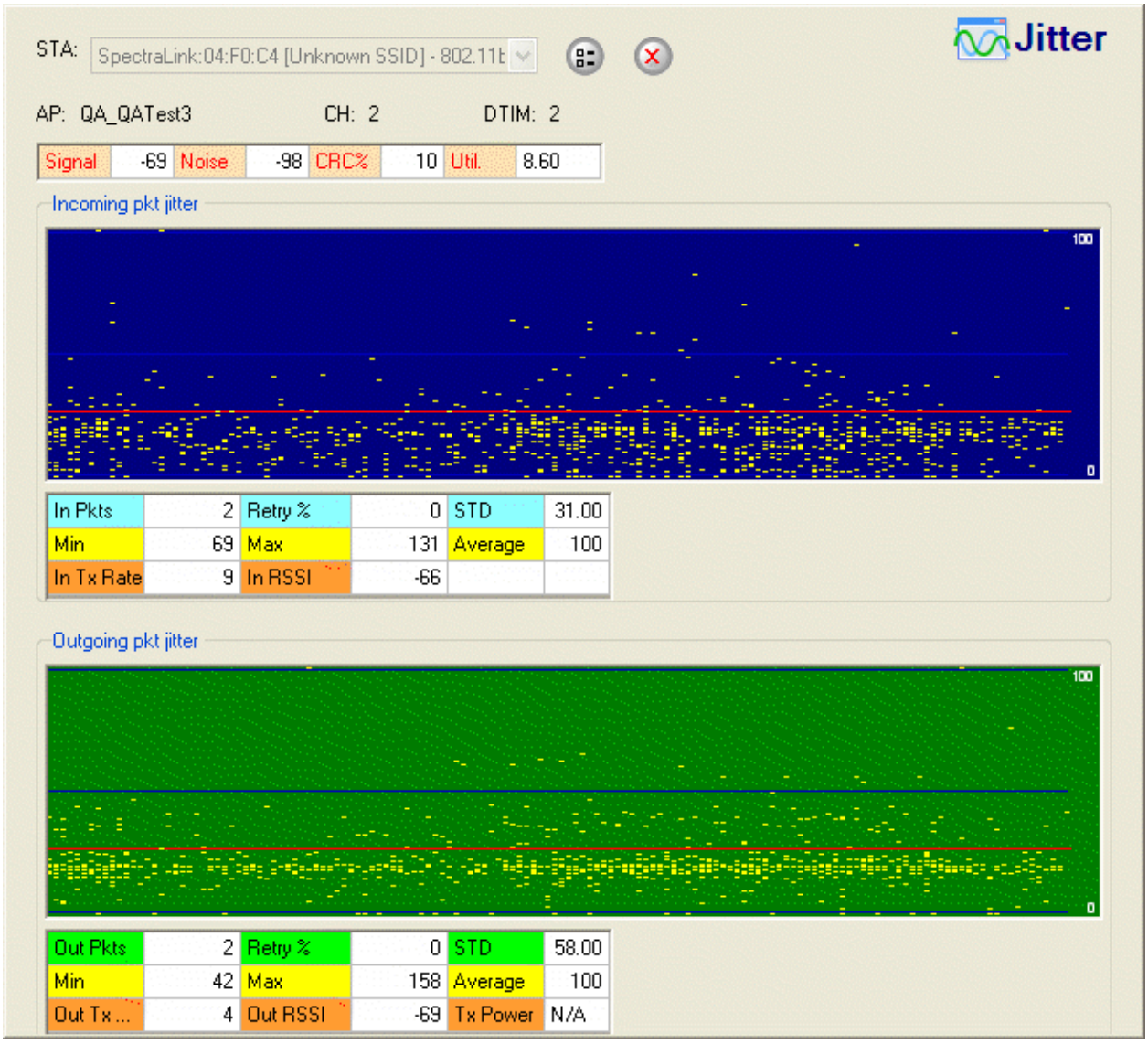
The AirMagnet Roaming Tool is designed to measure the roaming delay when a station disassociates from one access point and then tries to associate with another access point.



CH	Associated AP	Time (sec)	Util	Signal	Noise	0	MAC Adddr...
5	QA-1200-7	Start...					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.600	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.701	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	-56	-100		Cisco:43:11...

AirMagnet Roaming tool to measure roaming delays

Also, the AirMagnet Jitter tool allows the user to effectively measure RF signal jitter in both incoming and outgoing WLAN traffic between an access point and a station. Based on this information, the user can make the appropriate changes to the configuration or the placement of the APs to reduce the interference.

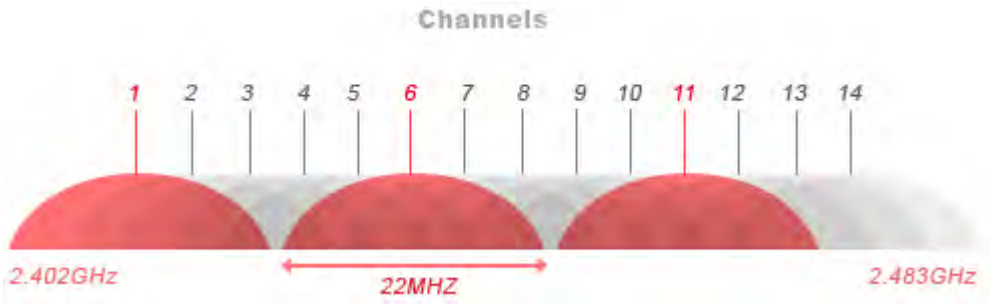


AirMagnet Jitter tool to measure jitter

Voice Quality Degradation Caused by Interfering APs

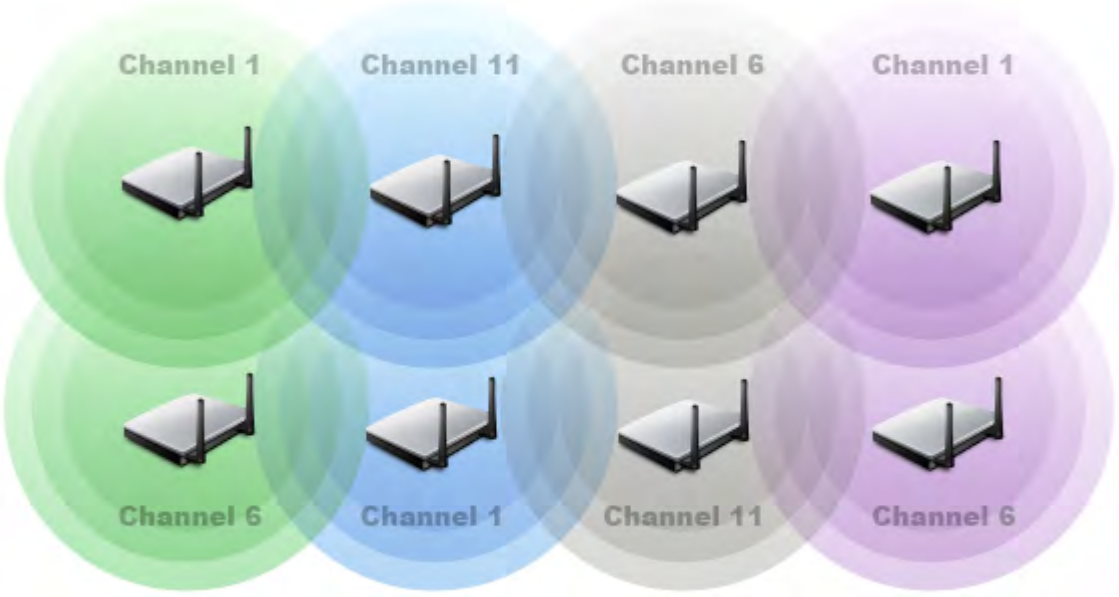
Alarm Description & Possible Causes

802.11b and 11g devices operate in the RF frequency range of 2.4GHz. A total of 14 channels are defined by the IEEE standard in this frequency range with each channel occupying 22 MHz. Adjacent channels overlap with each other in RF frequency usage (see illustration below).



802.11b and 11g Channel Allocation and Frequency Overlaps

Wireless devices operating in adjacent channels (channel numbers less than 5 apart) have their RF frequencies overlapped and will interfere with one another. Ideally, APs should be 5 channels apart to avoid such a problem. Refer to the sample channel allocation and AP deployment below.

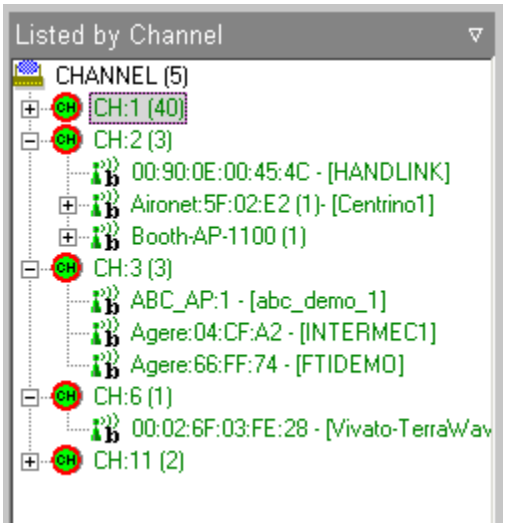


Site Survey Allocates Non-overlapping Channels to Physically Adjacent APs

This AP interference can be very critical for VoWLAN applications. This may cause packet loss, which leads to a choppy call and the VoWLAN clients to drop their connection with the AP, thus disconnecting the voice call. Now, the clients may have to re-associate and re-authenticate to continue the ability to make the voice calls. This process gets tougher in an environment where higher security standards such as WPA and 802.11i are in place. Additional time will consequently be required for the handshake process and receiving the new encryption key for this server-based method of authentication. This increased delay makes these security mechanisms unattractive for VoWLAN applications. Weaker mechanisms (such as WEP) that support faster hand-off mechanisms may behave slightly better in terms of latency, jitter, and lost information.

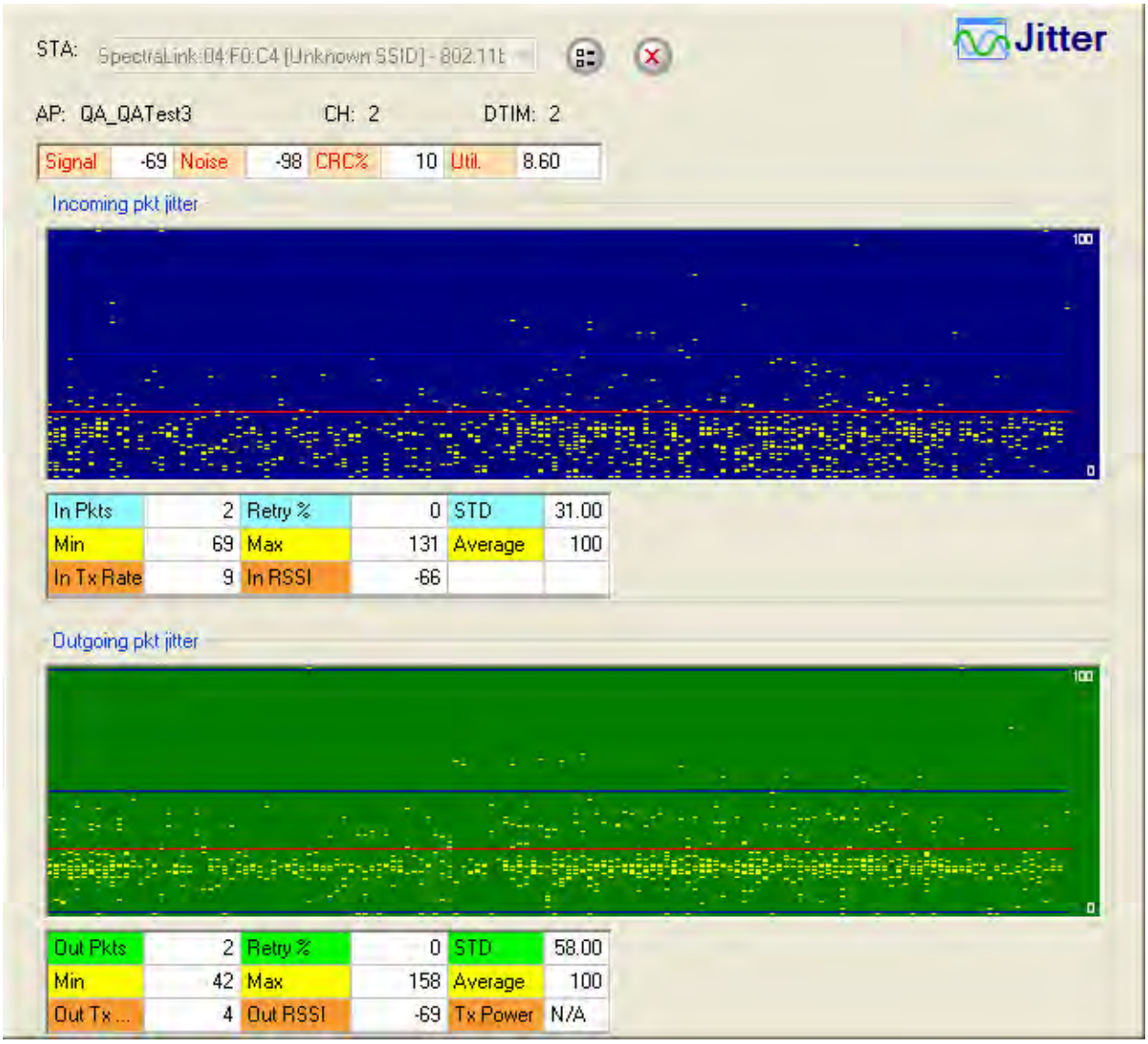
AirMagnet Solution

AirMagnet WiFi Analyzer analyzes channel allocation and usage to detect their mutual interference and the alarm is generated when a channel frequency is overlapped by more than the tolerable number (the user-configurable alarm threshold) of APs. For example, if AirMagnet WiFi Analyzer detects 5 APs operating in channel 1, 2, 3, 4, 5, and 6 individually, it would generate this alarm to indicate that these APs all interfere with each other, which exceeds the default threshold of 3 APs with overlapping frequency usage. Most experts advise the use of channels 1, 6 and 11, while some recommend the use of only channels 1 and 11. The user can use the AirMagnet Infrastructure view to further investigate current channel usage and take counter measures. (illustrated below)



AirMagnet Infrastructure View (List by Channel) Shows Channel Allocation

Also, the AirMagnet Jitter tool allows the user to effectively measure RF signal jitter in both incoming and outgoing WLAN traffic between an access point and a station. Based on this information, the user can make the appropriate changes to the configuration or the placement of the APs to reduce the interference.



AirMagnet Jitter tool to measure jitter

AP Configuration Changed (Security)

Alarm Description & Possible Causes

Typically, for an AP that is operating without any sort of encryption mechanism, there can be unauthorized clients without encryption keys that can associate with the AP and obtain access to the enterprise wired network. This not only risks the user's data privacy but also exposes the corporate wired network access. The same applies for networks that are using weaker security mechanisms like WEP or not using any security at all.

Sudden changes in the security configuration on your AP may indicate that:

an unauthorized person has gained access to the APs and has made those changes (For example, moving from a stronger security setting like WPA2 to a weaker one like WEP or changing from WPA2-Enterprise to WPA-2 Personal). This situation could be very harmful to the confidentiality or privacy of the network with valid clients potentially locked out of the network and intruders connecting to it.

Changes could be made to enhance the security of the network by the Access Point administrator (For example, moving from a weaker security setting like WEP to a stronger one like WPA2).

AirMagnet Solution

AirMagnet WiFi Analyzer also alerts the user for any sudden changes in the security setting of the access point. This may indicate that an intruder has control over the access point and has modified the security configuration. This can cause all valid clients to get is connected from the AP as they now are not talking on the same network and may also lead to a network.

Please connect to the AP whose configuration has changed and assign a stronger password for the access point login and change the security setting back to the original one and undertake stringent actions to prevent this occurrence in the future.

Also if the security settings have been changed on purpose by the network administrator to enhance the security, please take appropriate action in informing the users to re-configure their wireless security settings based on the corporate wireless policy.

Excessive Missed AP Beacons

Alarm Description & Possible Causes

WLAN Access Points transmit beacon frames at a fixed rate (typically 10 beacons per second) to advertise their service and configuration parameters. Wireless clients use these beacon frames to learn of available WLAN services and their characteristics in order to make crucial decisions regarding association and roaming. The beacon frame includes information on SSID, supported rates, traffic indication maps, optional IBSS parameters, synchronization information, and so on

AirMagnet Solution

AirMagnet WiFi Analyzer monitors beacon frames to track the WLAN service quality. This particular alarm tracks the beacon arrival rate per AP to compare against the advertised **fixed rate** by the AP. Missed beacons indicate receive errors that may be caused by interference, multipath, noise, collisions, and so on. Excessive missed beacons warrant careful investigation, as it may indicate that your network may be experiencing excessive interference. You may use the RF Interference page of AirMagnet WiFi Analyzer to determine if the interference is caused by other 802.11 traffic, and identify which devices may be causing the problem.

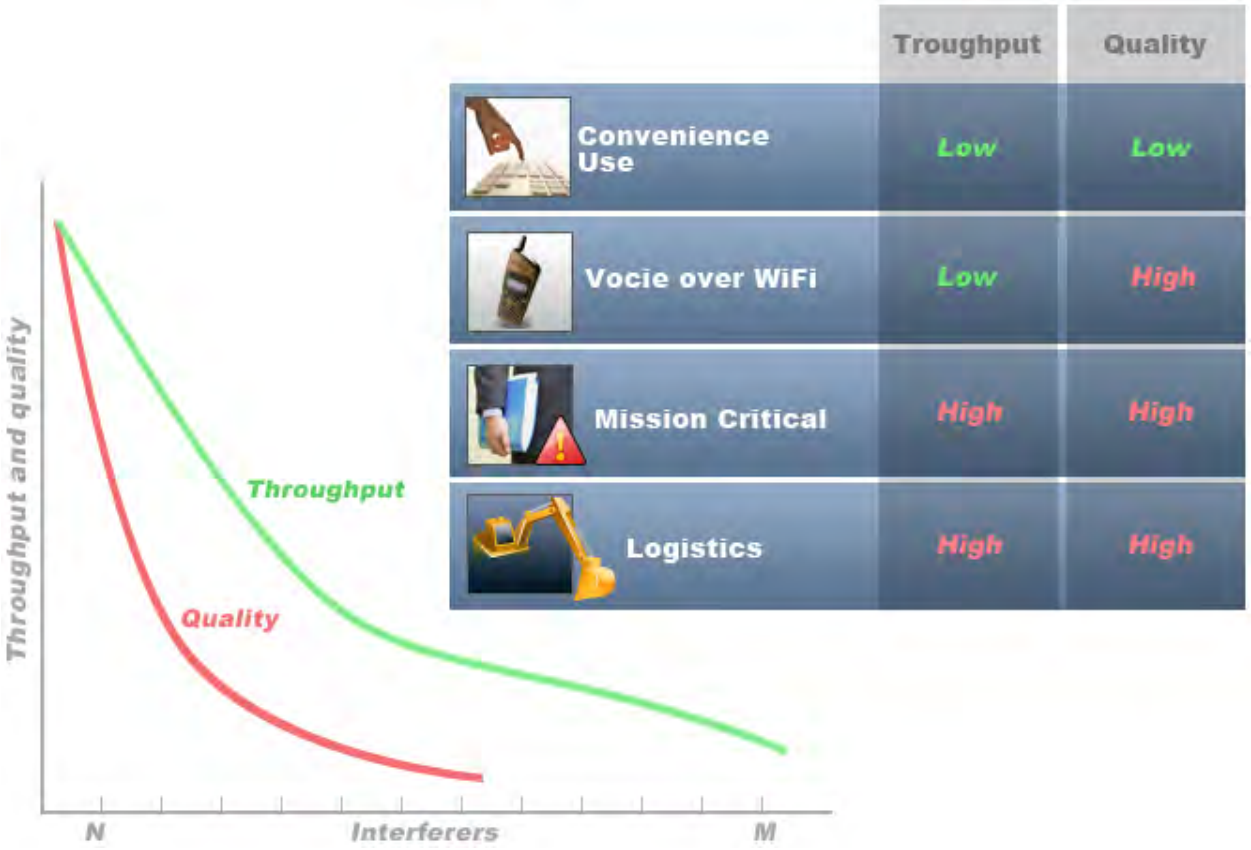
Non-802.11 Interfering Source Detected

Alarm Description & Possible Causes

Because WLANs operate in the unregulated 2.4 and 5 GHz frequency bands, they are subject to interference from all devices operating in this same frequency spectrum. These include, but are not limited to, microwave ovens, cordless phones and headsets, wireless surveillance cameras, garage door openers, Bluetooth technology, and other devices. There can also be co-channel and/or adjacent channel interference caused by APs and stations from neighboring WLANs. Excessive RF interference can degrade 802.11 network performance, resulting in unacceptably slow data rates and excessive packet re-transmissions. Since the current WLAN technologies can only detect 802.11 devices such as APs and stations on the network, WLAN system administrators lack sufficient awareness of the RF environment in which their APs and stations operate. They have no way to detect those non-802.11 sources emitting RF interference in the unlicensed bands, which can cause disruption of network connections and many other problems. The lack of awareness of the entire RF spectrum makes it impossible for network administrators to apply appropriate, adaptive responses to improve their WLAN performance in the face of interferers and competing networks.

Non-802.11 Sources of Interference

AirMagnet WiFi Analyzer integrated with AirMagnet Spectrum Analyzer includes sophisticated technology to detect and classify sources of RF activity. Using this data, network engineers can take a variety of actions to enhance WLAN performance and reliability.



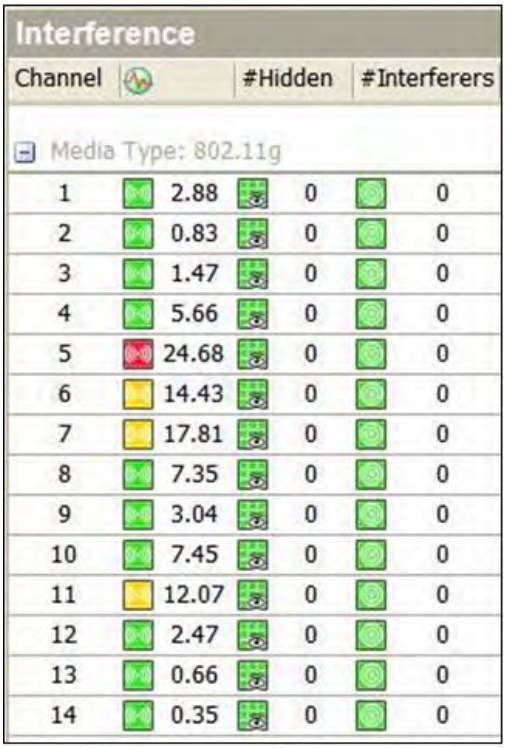
Throughput and Quality vs. Interference

AirMagnet Solution

The AirMagnet WiFi Analyzer and Spectrum Analyzer integration allows AirMagnet users to get a layer 1 perspective to all of their WLAN troubleshooting screens, making it easy to see when the network is facing a fundamental RF problem. AirMagnet Spectrum Analyzer can automatically identify the presence of non-802.11 sources of interference such as microwave ovens, Bluetooth devices, cordless phones, etc. If a certain part of the frequency spectrum is in constant use by other devices, AirMagnet recommends that the network engineer configure the WLAN to avoid transmitting over those channels. Conversely, by deliberately searching for “clean” channels, WLAN devices can be set to broadcast over those channels.

Also, AirMagnet Wi-Fi Analyzer’s Interference screen allows users to visualize the consolidated picture of interference that impacts Wi-Fi "air" quality. Wi-Fi Interference occurs due to co-channel or adjacent channel interference from the corporate or neighboring WLANs, hidden nodes in the Wi-Fi environment, or sources outside of the 802.11 band. Interference causes degraded network Wi-Fi users, leading to slower

application usage and reduced user productivity. The Interference Status Indicator (2nd column from the left as shown in the figure below) lists the overall interference status for each Wi-Fi channel, calculated based on the Wi-Fi interference score for the devices contributing to the interference, hidden nodes, and non Wi-Fi devices.



Interference

Channel		#Hidden	#Interferers
Media Type: 802.11g			
1	2.88	0	0
2	0.83	0	0
3	1.47	0	0
4	5.66	0	0
5	24.68	0	0
6	14.43	0	0
7	17.81	0	0
8	7.35	0	0
9	3.04	0	0
10	7.45	0	0
11	12.07	0	0
12	2.47	0	0
13	0.66	0	0
14	0.35	0	0

Channel interference status shown AirMagnet WiFi Analyzer Analyzer's Interference screen

Understanding the Interference status for all the channels enables AirMagnet users to plan future Wi-Fi deployments or make modifications to their existing to increase network performance.

- Green indicates that the interference on the selected channel is within tolerable limits and has minimal impact on the Wi-Fi network performance.
- Yellow indicates that the channel is experiencing higher than normal interference and that the source of interference should be located and actions undertaken to bring it within permissible or desirable limits.
- Red indicates that the interference on that channel is beyond advisable limits and is potentially causing significant impact to the wireless network performance.

Higher Speed Not Supported

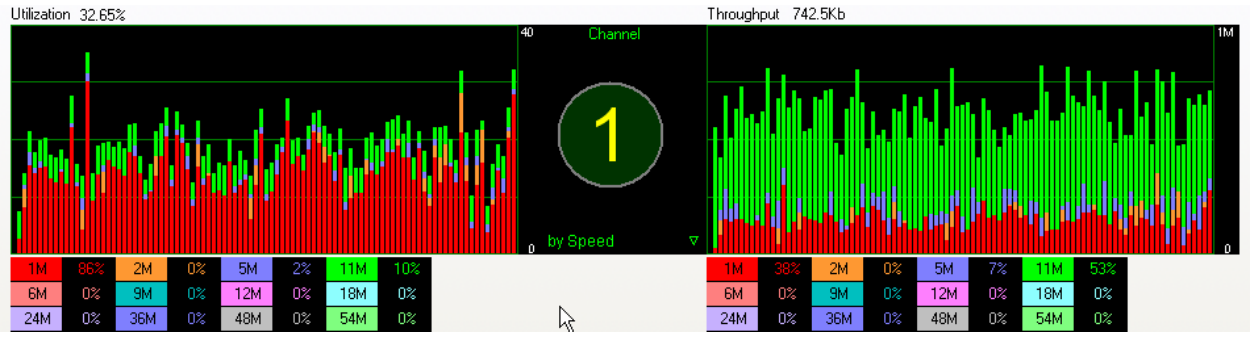
Alarm Description & Possible Causes

802.11a, 11b or 11g devices use several different transmit speeds from frame to frame. Higher speed transmission consumes less bandwidth and allows higher throughput. Transmit speed optimization is a key factor during the WLAN site survey and deployment process. It is typically impacted by signal quality and distance. See the table below for all the supported speeds and what AirMagnet Enterprise considers to be high speed for the selected standard.

Speed	802.11b (mbps)	802.11g (mbps)	802.11a (mbps)
Supported Speed	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54	6, 9, 12, 24, 36, 48, 54
AirMagnet Enterprise Considered High Speed	11	54	54

Supported Speeds and AirMagnet Considered 'High' Speed

However, high speed transmission requires better signal quality to achieve the same low error rate as compared to the low speed transmissions. The transmit speed selection is a decision made by the transmitter that will also detect reception problems from the lack of acknowledgements. The transmitter may vary the transmit speed to increase reliability. When this scenario occurs too often, the WLAN slows down and the throughput degrades. See the problem illustrated by an AirMagnet WiFi Analyzer screen shot below. It shows excessive low speed transmission (1mbps), high utilization (32%), and low throughput (931kbps).



Bandwidth utilization, Throughput, and Transmit Speed Relationship

AirMagnet Solution

AirMagnet WiFi Analyzer detects the highest speed supported by a device to ensure optimum levels of WLAN performance. When the 'high' speed transmit rate (see the table above) is not supported by a device, AirMagnet WiFi Analyzer raises this alarm for further investigation. Check AP configuration settings to ensure that the high speeds are supported and are enabled.

Potential Pre-802.11n Device Detected

Alarm Description & Possible Causes

In January 2004, the IEEE announced that it had formed a new 802.11 Task Group (TGn) to develop a new amendment for the existing standard for wireless local-area networks. It was expected to provide transmission speeds greater than 100 Mb/s, but this proposal has come a long way, with even higher speeds being possible at this time: it may even reach the theoretical value of 540 Mb/s. It is also expected to provide a larger range than the 802.11a/g standards and will operate in the 2.4 Ghz band shared with 802.11b/g devices.

Initially, there were two proposals to the standard:

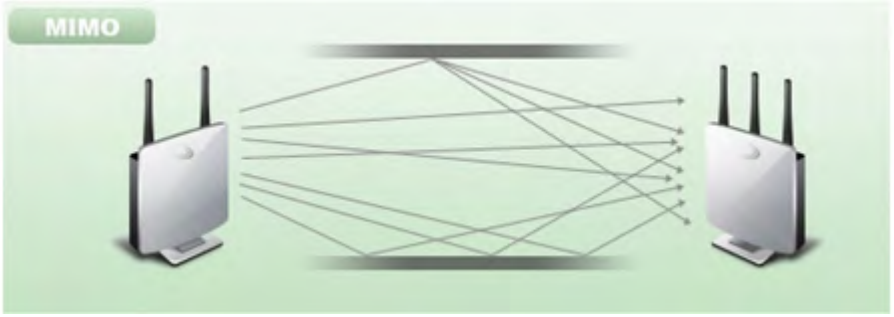
- WWiSE (World-Wide Spectrum Efficiency), backed by companies such Airgo, Broadcom, Conexant, and Texas Instruments, and
- TGn Sync, backed by Intel, Atheros, Marvell, Agere, and Philips.

Both the proposals are similar, though they differ in terms of their goals: increasing peak data rates versus improving efficiency. The proposals:

- Make use of multiple-input/multiple-output (MIMO) technology,
- Backward compatible with 802.11b/g devices,
- Support operation in the current 20 MHz channels and can use the double-width 40 MHz channels for increased throughput, and
- Block acknowledgements or frame bursting.

MIMO Technology

In the 802.11 standard, even though diversity was employed, only one antenna was used for transmitting or receiving, as there was only a single component available for processing the signal. With the new MIMO technology, there are multiple components attached to each antenna (2 or more) for signal processing. This technology also takes the advantage of multipath propagation. This is a stark contrast to the disadvantages multipath users have complained about. Multiple antennas are used to divide a single fast signal into multiple slower signals. These signals are sent over different antennas and reassembled by the receiver after sorting out the non-required signals.



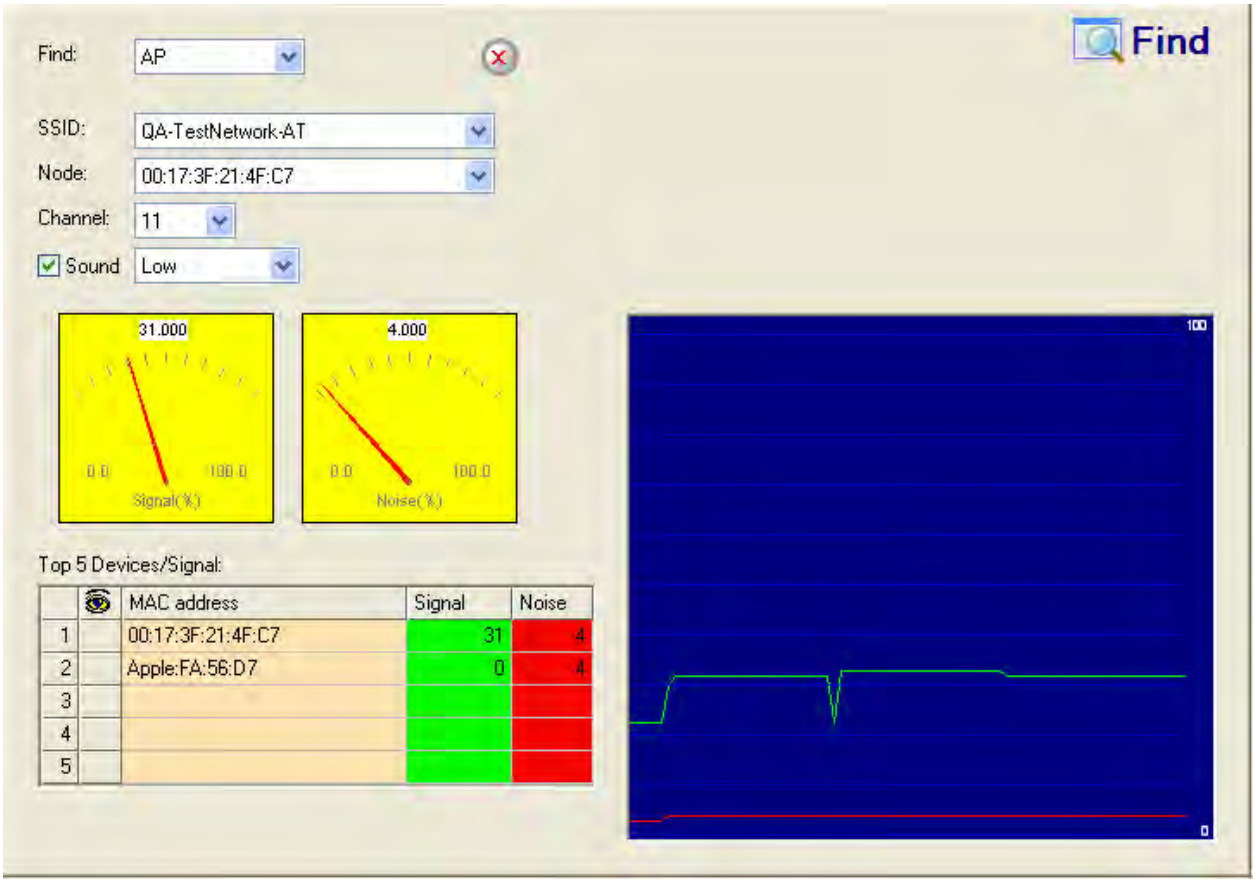
MIMO access points communicating with each other

The proposals were merged and a new draft was prepared and submitted for approval by the IEEE 802.11n Task Group. The IEEE Working Group voted not to forward this draft. It is expected that the 802.11n standard will not be approved until July 2007.

Meanwhile, different vendors have come up with their own version of "Pre-n" access points. This standard is not the final "802.11n" standard and hence could be incompatible with devices once the standard is ratified. Also, initial tests by industry experts have shown that though these devices may provide higher speeds at closer ranges, their performance may decrease rapidly as the distance increases. Some tests have proved that if there are 802.11g devices operating in channels adjacent to pre-n devices, the performance of both products is severely affected.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts the WLAN administrator if it detects a Pre-11n device in the wireless environment. The presence of such devices may cause severe performance degradation issues to the current wireless setup due to inter-operability problems between various standards. AirMagnet recommends that the users wait for the standard to be ratified and the Wi-Fi certification is implemented. If this AP is not a known device, please use the FIND tool to locate it.

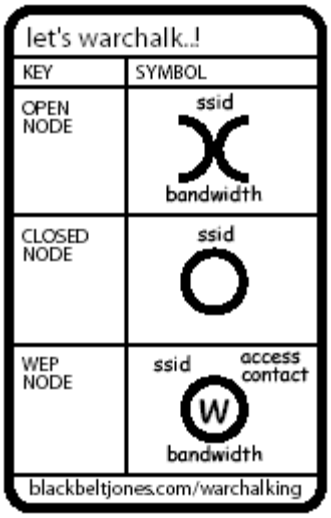


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

NetStumbler Victim Detected

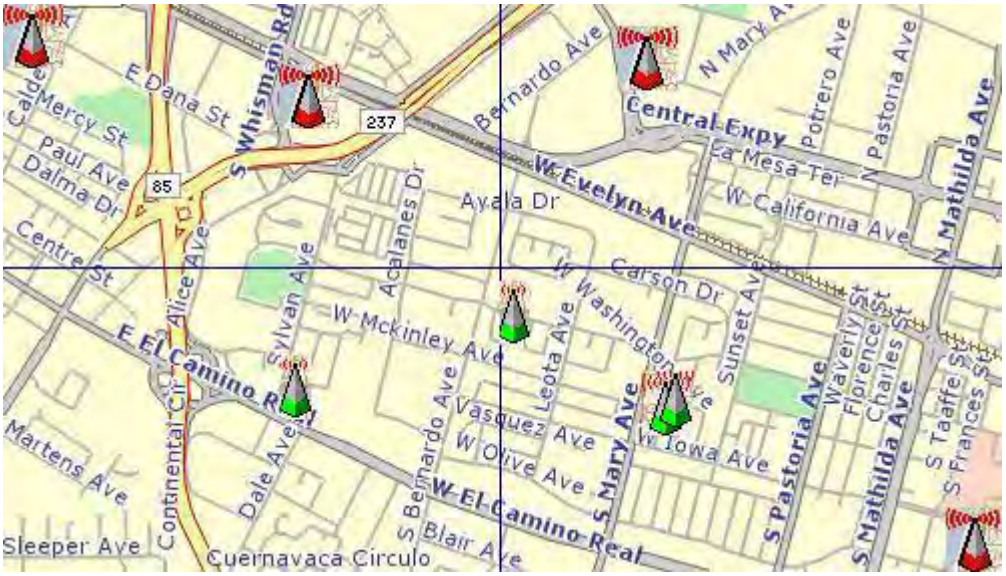
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer detects a wireless client station probing the WLAN for an anonymous association (that is, association request for an AP with any SSID) using the NetStumbler tool. The Device probing for AP alarm is generated when hackers use newer versions of the NetStumbler tool. For older versions, AirMagnet WiFi Analyzer generates the NetStumbler detected alarm.



War-chalker publishing a discovered WLAN and its configuration at the WLAN location

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover APs and publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the APs' geographical location information. War-chalkers discover WLAN APs and mark the WLAN configuration at public locations with universal symbols as illustrated above. You can think of war-walking as war-driving, but the hacker conduct his illegal operation on foot instead of by car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is, just as its name implies, sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

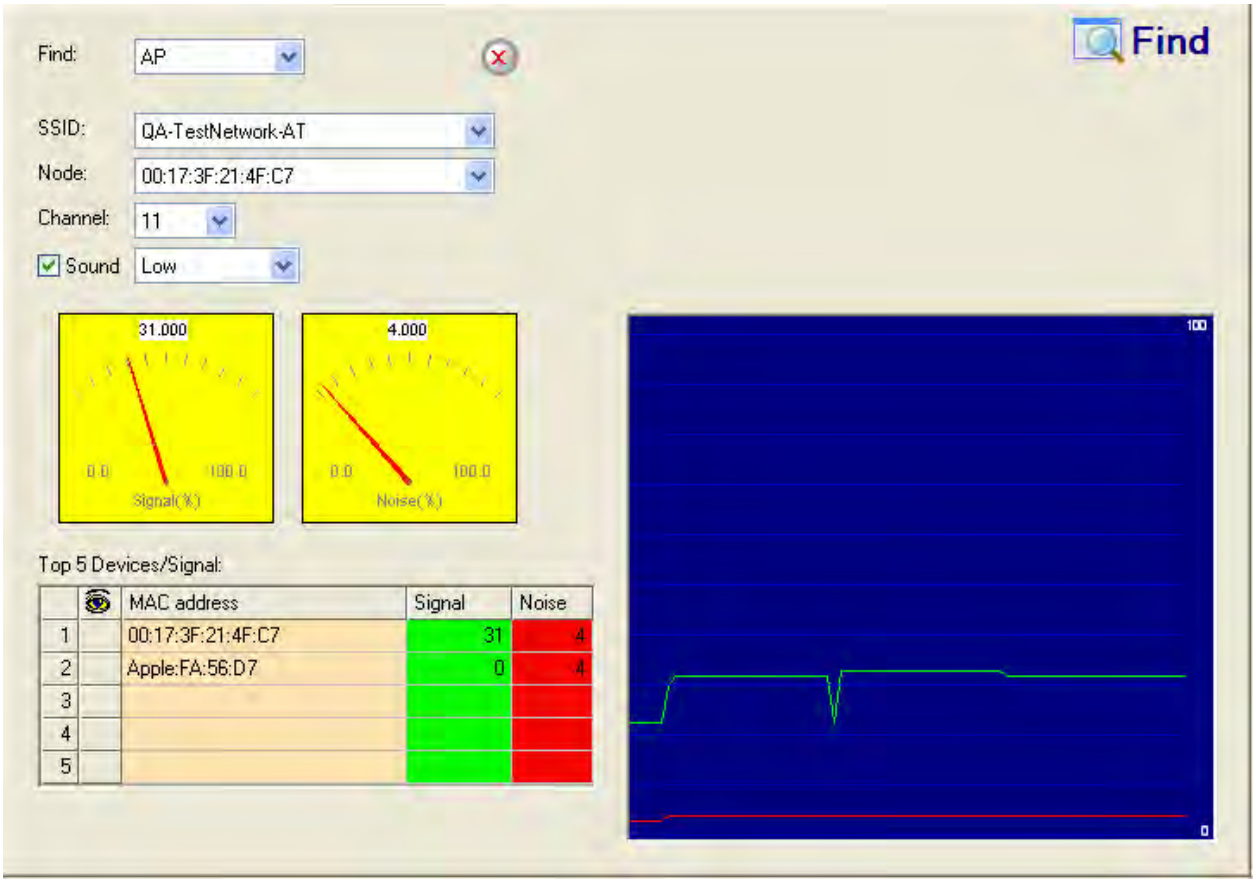


802.11 APs location posted on the Internet by war-driving groups

AirMagnet WiFi Analyzer alerts the user when it observes a station running Netstumbler, associated to a corporate AP.

AirMagnet Solution

To prevent your APs from being discovered by these hacking tools, you can configure your APs to not broadcast its SSID. You can use AirMagnet WiFi Analyzer to see which of your APs is broadcasting (announcing) its SSID in the beacons. Furthermore, you can use the Find tool in AirMagnet WiFi Analyzer to physically locate the station that is running Netstumbler or the corporate AP it is associated with. Refer to the illustration below.

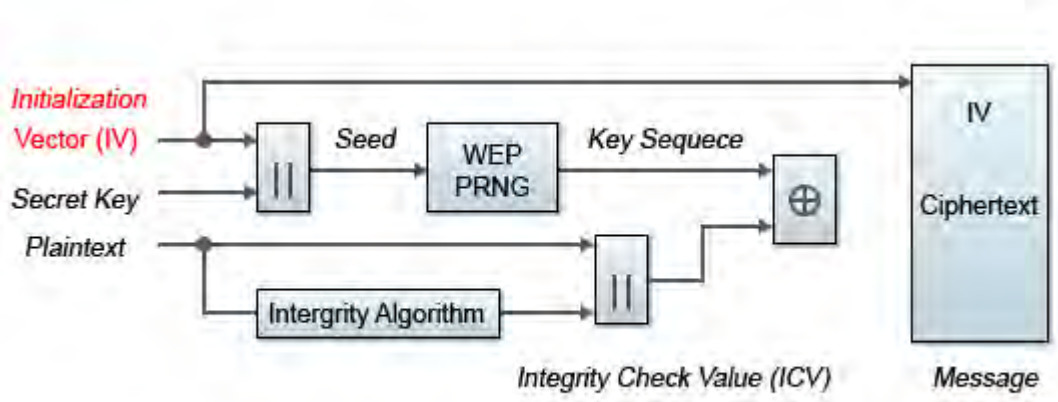


AirMagnet WiFi Analyzer's Find tool used for tracking down wireless devices

Potential Chopchop Attack in Progress

Alarm Description & Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.



WEP Encipher Process Block Diagram

A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (some vendors also offer 152-bit encryption), is a secret key specified by the user, concatenated with the 24-bit IV (Initialization Vector). The chopchop tool was written for the Linux operating system by Korek to exploit a weakness in WEP and decrypt the WEP data packet. However, the chopchop tool only reveals the plaintext. The attacker uses the packet capture file of a previously injected packet during the initial phase and decrypts the packet by retransmitting modified packets to the attacked network. Once the attack is completed, the chopchop tool will produce an unencrypted packet capture file and another file with PRGA (Pseudo Random Generation Algorithm) information determined during the decryption process. The PGRA is then XORed with the cyphertext to obtain the plaintext.

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

Where:

- **-4 means the chopchop attack**
- **-h XX:XX:XX:XX:XX:XX is the MAC address of an associated client or your card's MAC if you did fake authentication**
- **-b YY:YY:YY:YY:YY:YY is the access point MAC address•ath0 is the wireless interface name**

Commands for Initiating a Chopchop Attack

There are a few access points that may not be vulnerable to this kind of attack. They drop data packets shorter that 60 bytes. If an access point drops packets shorter than 42 bytes, aireplay will try to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet. A

chopchop attack also works against dynamic WEP configurations. AirMagnet Wi-Fi Analyzer is able to detect potential attacks using the chopchop tool.

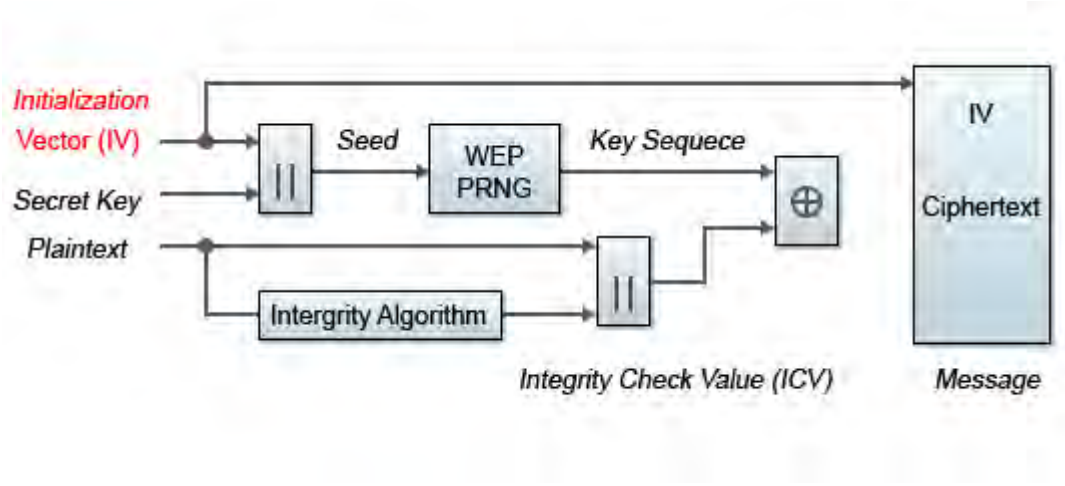
AirMagnet Solution

AirMagnet WiFi Analyzer alerts on detecting a potential chopchop attack in progress. AirMagnet recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Potential Fragmentation Attack in Progress

Alarm Description & Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

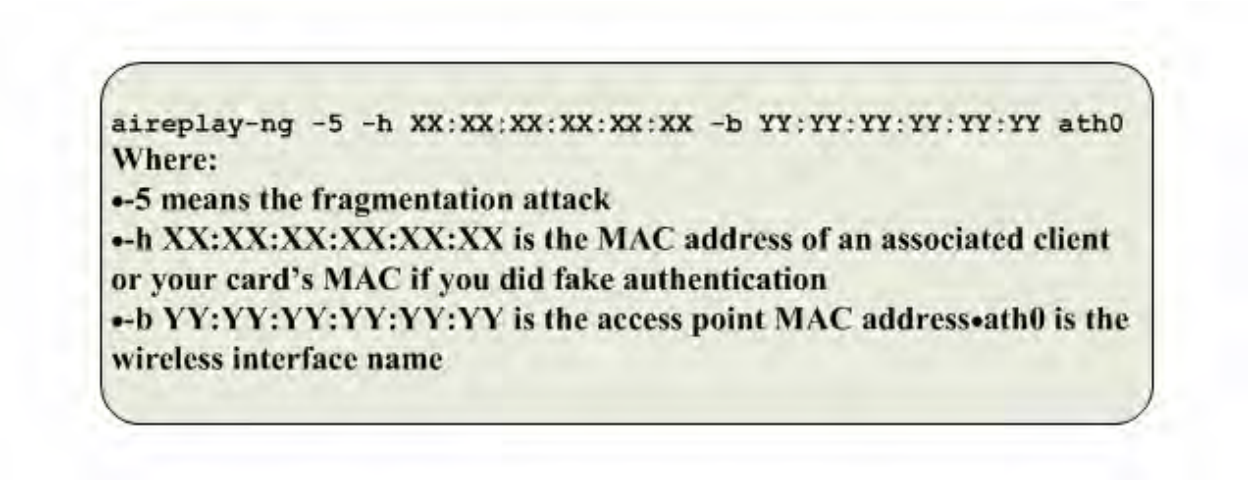


WEP Encipher Process Block Diagram

A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption), is the secret key specified by the user and concatenated with the 24-bit IV (Initialization Vector).

According to *http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation*, the aircrack program obtains a small amount of keying material from the packet and then attempts to send ARP and/or LLC packets with known information to an AP. If the packet gets successfully echoed back by the AP, then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes (less in some cases) of PRGA are obtained.

This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with “packetforge-ng” which can be used for various injection attacks.



Commands to run the fragmentation attack

AirMagnet WiFi Analyzer detects potential fragmentation attacks in progress against the Wi-Fi network.

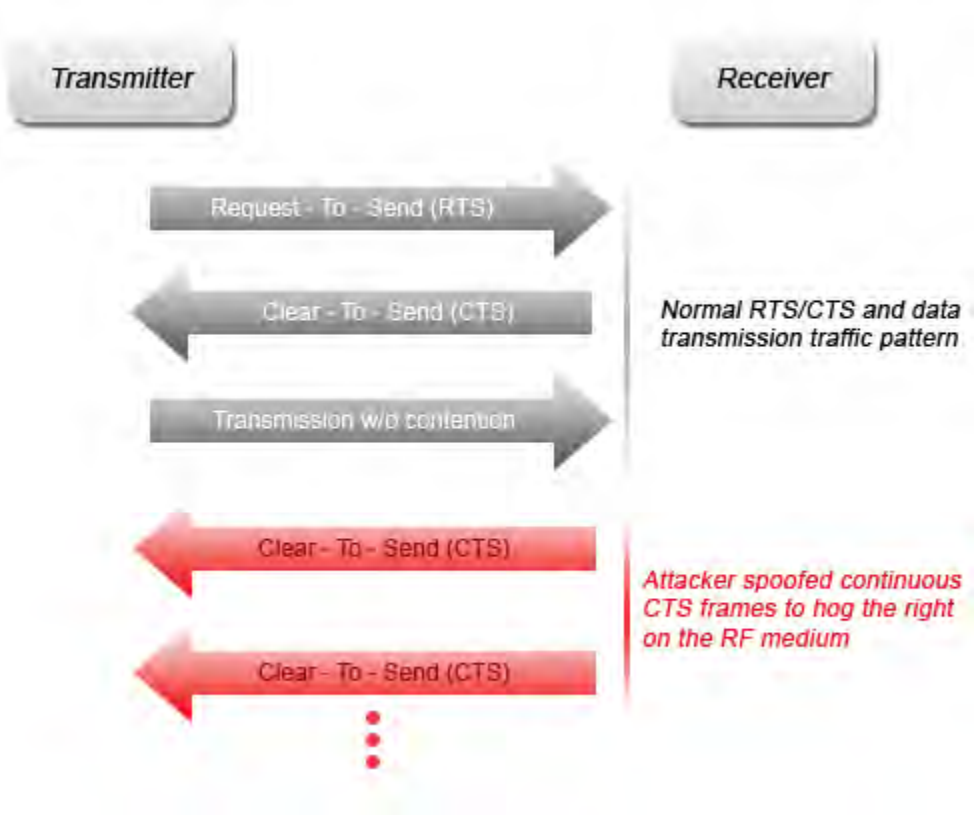
AirMagnet Solution

AirMagnet WiFi Analyzer alerts on detecting a potential fragmentation attack in progress. AirMagnet recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Denial of Service: RTS Flood

Alarm Description & Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame in order to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention. See the illustration below.

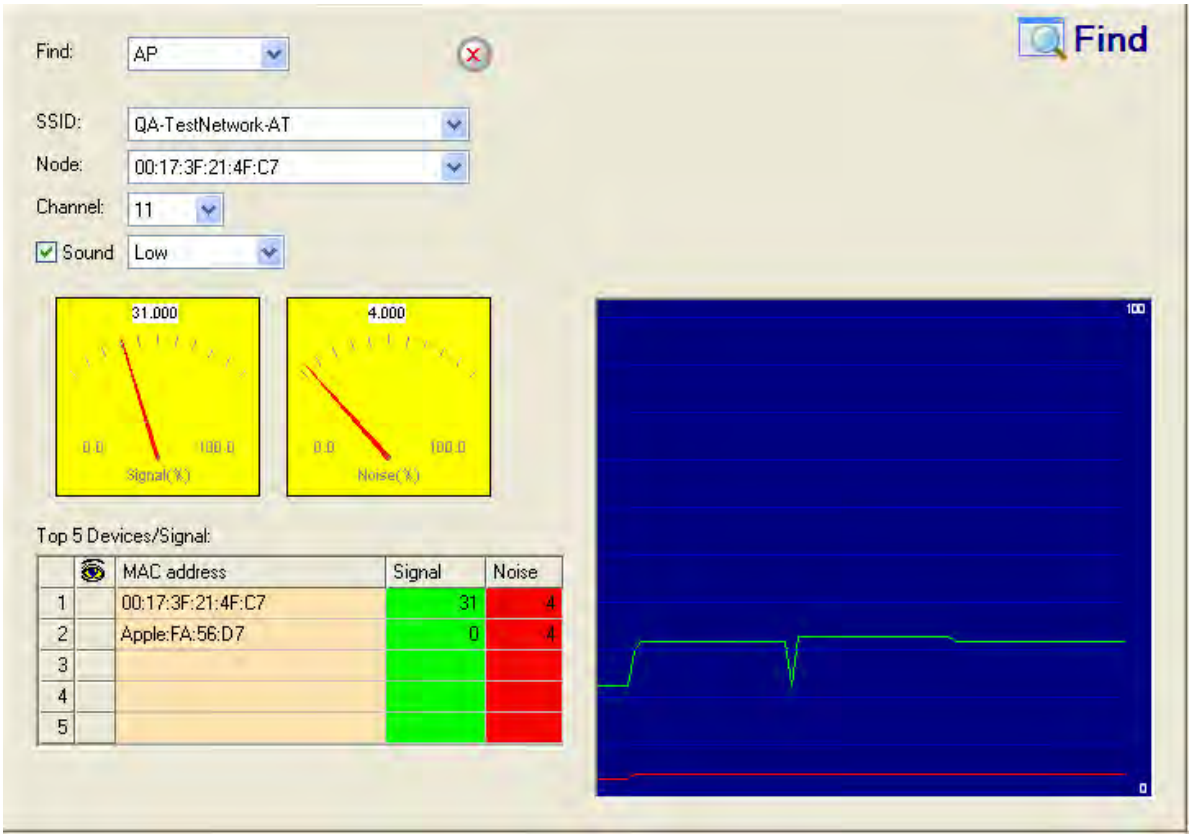


Standard RTS/CTS mechanism vs. intruder-injected RTS denial-of-service attack

A wireless denial-of-service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration field, an attacker can reserve the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

AirMagnet Solution

AirMagnet WiFi Analyzer detects the abuse of **RTS** frames for a denial-of-service attack. Similar to an RF jamming attack, security personnel can use the AirMagnet Wi-Fi Analyzer's **FIND** tool to locate the source of the excess **RTS** frames.



AirMagnet WiFi Analyzer's Find tool locating the source of an RTS flood attack

Device Unprotected by EAP-TTLS

Alarm Description & Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known as Tunneled Transport Layer Security (TTLS). EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled.

Devices configured to use the EAP protocol but not the TTLS authentication mechanism can represent potential insecure connections to the wireless network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data as a result. EAP exchanges that are not secured by TTLS authentication can be easier for attackers to intercept and decode, potentially resulting in sensitive data sent from a valid user being leaked.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors EAP transactions to detect any devices that are not implementing the EAP-TTLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. We recommend that IT personnel locate the device triggering the alarm and configure it to use the EAP-TTLS mechanism.

AP Using WPA Migration Mode

Alarm Description & Possible Causes

Cisco Access points support WPA Migration Mode. This gives the ability for WEP and WPA clients to associate to an Access Point using the same SSID. The following client device types are allowed to connect to the access point using the same SSID:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS capable of authenticated key management but not TKIP)
- Static-WEP clients not capable of TKIP or authenticated key management

WPA Migration Mode exposes the WEP protocol which has numerous weaknesses. Hackers can then run the classic WEP attack to obtain the Wep key and gain access to the wireless network. This attack is currently built into the popular Aircrack-ng suite of wireless tools.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the WLAN environment and will alert the WLAN administrator if it detects one or more Cisco Access Points operating in WPA Migration Mode. WPA Migration Mode should be temporary. When WPA Migration mode is not neccessary, it should be disabled.

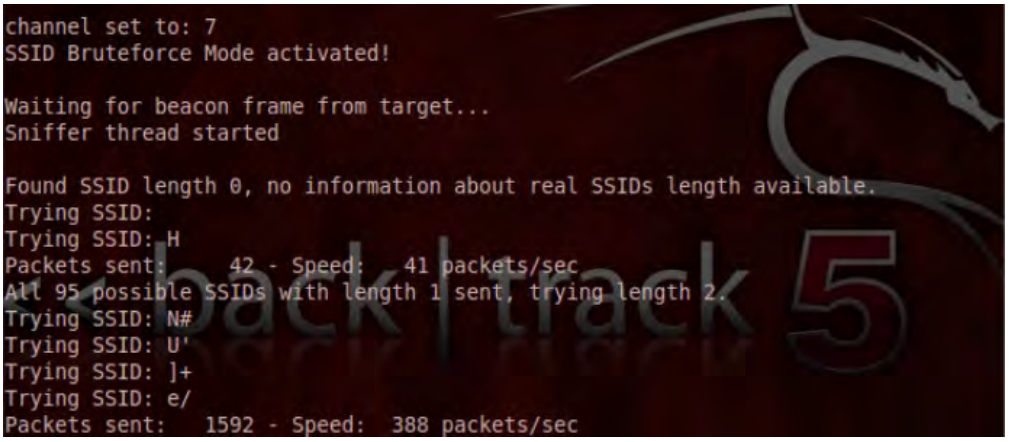
Brute Force Hidden SSID

Alarm Description and Possible Causes

A common practice amongst WLAN Administrators is to disable broadcasting of the SSID for an Access Point. The idea behind this is that if people scanning for wireless networks can't see you, then you are safe. Basically you would need to know the SSID in order to connect to that wireless network. This protects your wireless network from casual drive by users who don't have the tools to extract the SSID from hidden networks. But hackers are a different story. They have the tools, the time and energy to extract the SSID from hidden networks. There are many tools to perform this type of snooping. If a hidden SSID is not found through normal methods, hackers can use a brute force method to perform a Dictionary attack or a word list attack on the hidden network to extract the SSID.

Common Tools

Mdk3 is a popular denial of service WLAN tool that can perform many different types of wireless attacks. One of them is the ESSID Bruteforcing mode. Within this mode, Mdk3 utilizes a character dictionary to probe for various combinations of SSID's, waiting for a reponse from the AP.



AirMagnet Solution

AirMagnet Enterprise monitors the wireless network for potential traffic that is consistent with a brute force attack against a hidden SSID and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan

screen. The attacking station should be removed from the wireless environment as soon as possible.

Device Unprotected by any Selected Authentication Methods

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer monitors on 802.1x transactions and their specific EAP (Extensible Authentication Protocol) methods. When a specific EAP method is not used, it will trigger an alarm.

AirMagnet Wi-Fi Analyzer supports the following EAP methods for this alarm.

- Leap - This is a proprietary EAP method developed by Cisco. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out.
- PEAP - The Protected Extensible Authentication Protocol, is also known as Protected EAP. It is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.
- EAP-TLS - EAP-Transport Layer Security (EAP-TLS). The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis.
- EAP-TTLS - EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled.
- EAP-FAST - Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.
- EAP-MD5 - This is a password based authentication method that offers minimal security. EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors EAP transactions to detect any devices that are not implementing the enabled authentication methods and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will

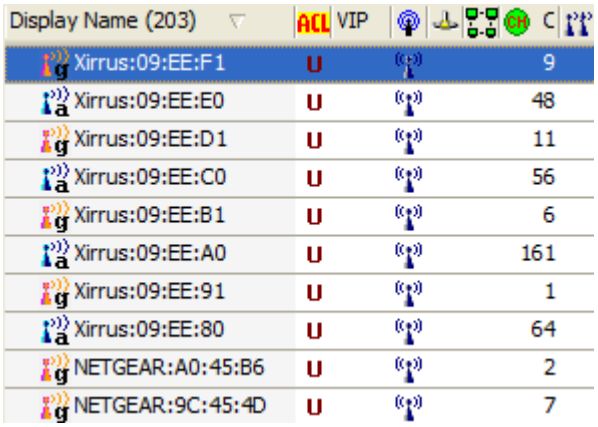
identify the problematic device. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the correct authentication method.

Device with Invalid IEEE OUI

Alarm Description & Possible Causes

A Vendor OUI (Organizationally Unique Identifier) is a 24 bit number that is purchased from the IEEE (Institute of Electrical and Electronics Engineers) which can identify a vendor or manufacturer to a block of assigned addresses. In 802.11, this would be the MAC address of the device. Companies purchase blocks of addresses in order to assign their company ID to them.

AirMagnet Enterprise queries the OUI list from the IEEE website once per day and uploads any new vendor OUI's to the sensors. When devices are detected and uploaded to the AirMagnet Enterprise server, the MAC addresses are converted to vendor OUIs so they are easily identifiable to the end user.



If a MAC addresses is not found in the IEEE Vendor database, it is a good indication that the MAC address for that device has been dynamically generated and not assigned by the vendor. This can indicate a possible attack is under way since most hackers will modify the MAC address of their wireless card so they are not easily identifiable before starting an attack.

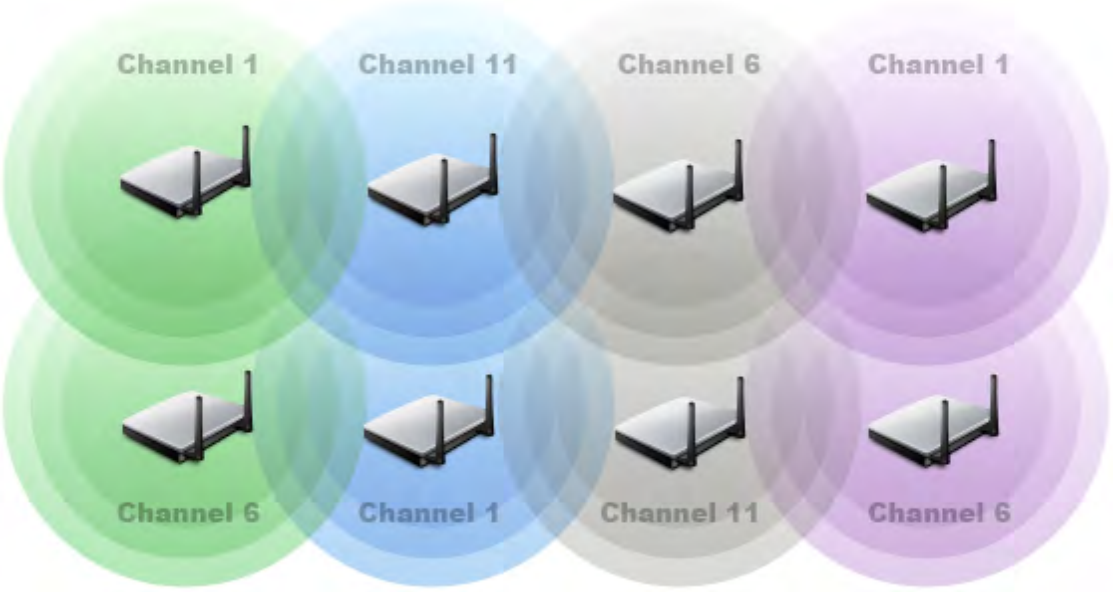
AirMagnet Solution

AirMagnet Smartedge sensors scan the WLAN for devices that have MAC addresses with unassigned Vendor OUI's. When one is detected, AirMagnet Enterprise alerts the WLAN administrator for this violation. It is recommended that the device be located to determine if it is valid.

Channel With Overloaded APs

Alarm Description & Possible Causes

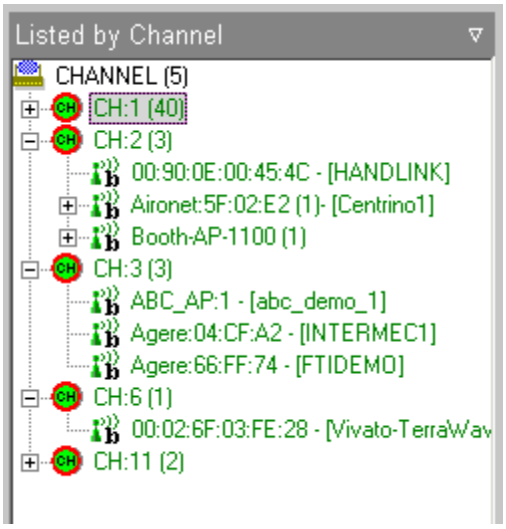
The RF spectrum is a shared medium where devices (802.11a, 11b, or 11g) operating in the same channel (RF frequencies) share the channel bandwidth. Not only bandwidth is shared; channels with over-populated devices have a higher possibility of transmission collisions, hidden node problems, interference, and so on. A typical site survey assigns non-overlapping channels to physically adjacent APs to avoid co-channel interference. The figure below shows a sample channel allocation to APs in the same area.



Site Survey Allocate Non-overlapping Channels to Physically Adjacent APs

AirMagnet Solution

AirMagnet WiFi Analyzer monitors channel allocation and usage and raises this alarm when a channel is populated by more than the pre-defined maximum number of APs (the configurable alarm threshold is 3). This alarm considers only APs operating in the exact same channel; another AirMagnet WiFi Analyzer alarm (AP With Mutual Interference) analyzes interference caused by APs operating in adjacent channels. Users can use the AirMagnet WiFi Analyzer's Infrastructure view to further investigate current channel usage and take counter measures (illustrated below).



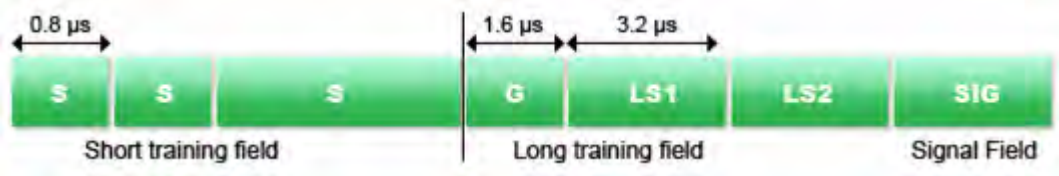
Infrastructure view (List by Channel) shows Channel Allocation

Overlapping Legacy BSS Condition (OLBC) Exists on Channel

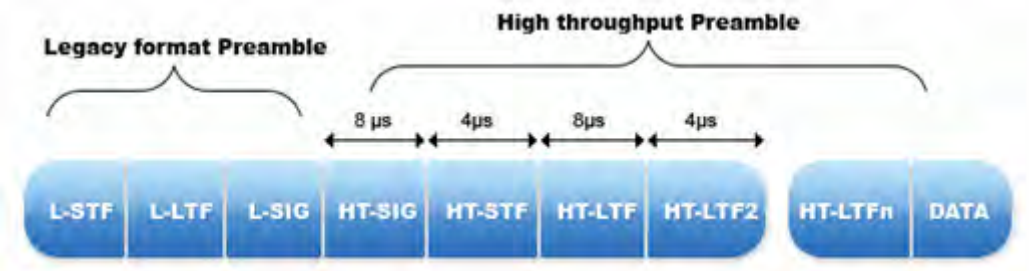
Alarm Description & Possible Causes

Even though, 802.11n APs are designed to be backward-compatible with stations built using the legacy 802.11a/b/g standards, 802.11n users have the option of operating in the so-called Greenfield mode. An 802.11n Greenfield deployment is an 802.11n network deployed and operating in such a way that backwards compatibility with legacy 802.11a/b/g devices is not required. This is the most efficient mode of an 802.11n network, as it allows full use of the 802.11n feature set. Data rate penalties are paid at both the PHY and MAC layers of 802.11n when legacy protection is required.

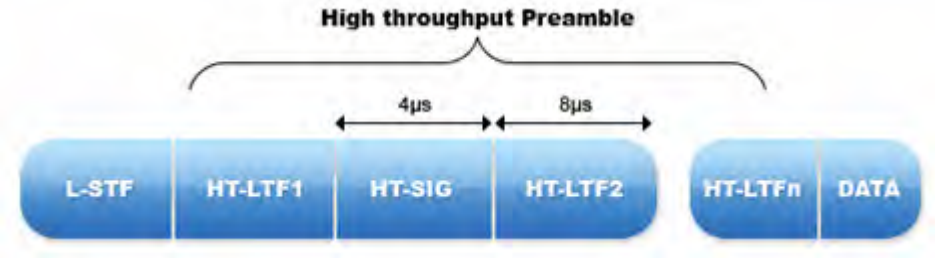
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



HT Preamble

An even larger penalty is paid at the MAC layer, as 802.11n HT transmissions must be preceded by low-speed, legacy format CTS-to-self, RTS/CTS or similar frame exchanges, in order for the virtual carrier sense mechanisms in the legacy nodes to function. Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. This means that, when protection is required, the HT transmission (potentially) uses more time for the "protection" frames than it does for its own data. Even though RTS and CTS type frames are relatively short, it takes more time to transmit an RTS/CTS exchange at a legacy rate of 6 Mbps than it does to transmit 500 bytes at the highest 802.11n data rate.

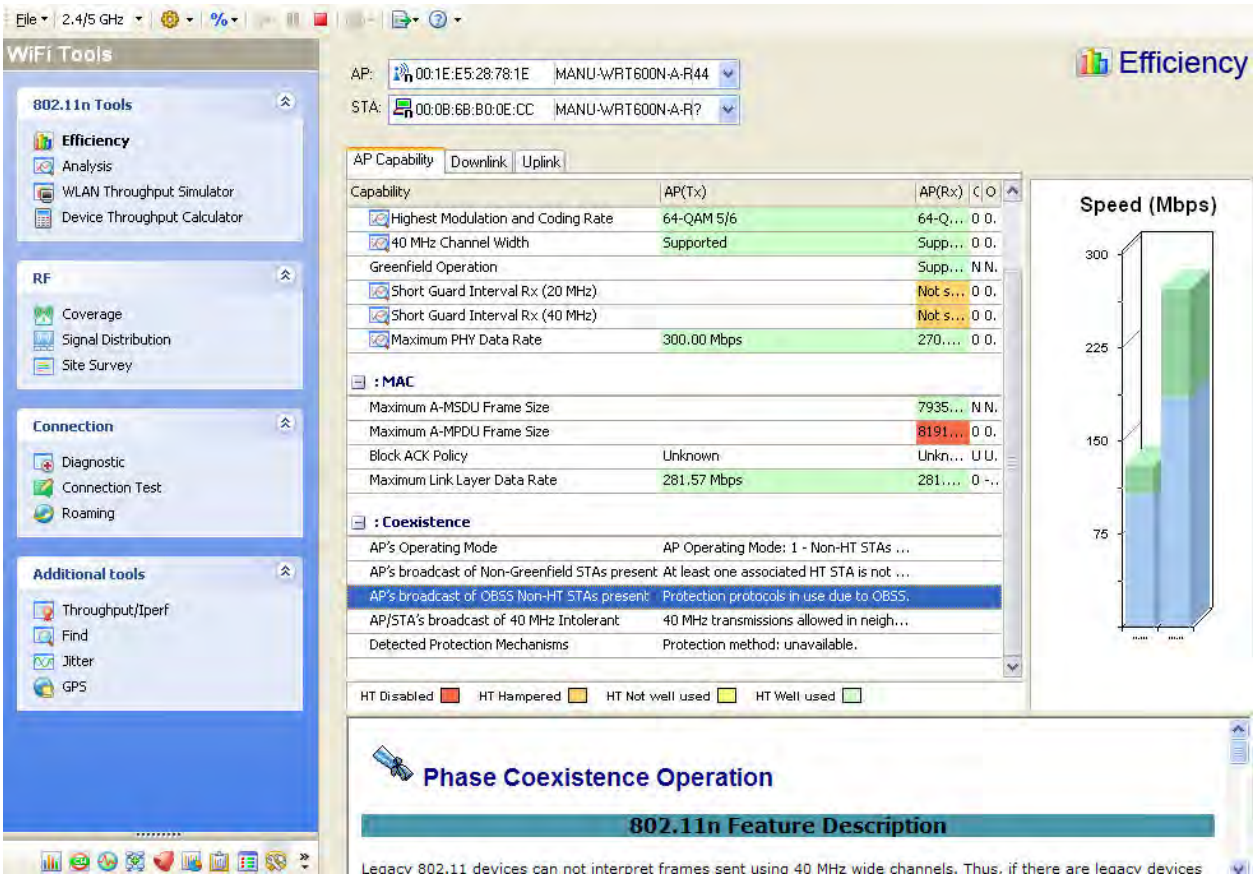
It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

OLBC (Overlapping Legacy BSS Condition) refers to a situation in which a legacy (that is, 802.11a/b/g) BSS is detected in the vicinity of an 802.11n BSS to the extent that the 802.11n AP can hear beacons from the neighboring BSS.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on the channel when it detects beacons from legacy BSS operating within range of an HT AP (AP is implementing protection mechanisms as described above) on that channel or an overlapping channel. AirMagnet recommends that the 802.11n and legacy networks be physically separated, or at a minimum, separated by operating channel(s).

AirMagnet WiFi Analyzer's Efficiency Tool analyzes the capabilities of the 802.11n AP and will inform the user for any co-existence issues with legacy 802.11 a/b/g devices.



AirMagnet WiFi Analyzer's Efficiency tool indicating co-existence issues

AirMagnet will alert the user on multiple co-existence issues, such as:

1. There are Non-HT Stations present in the primary or the secondary channel
2. If there are associated stations that are not Greenfield capable.
3. There are non-HT Stations present in the overlapping BSS
4. Overlapping BSSs allow 40 MHz transmissions.

AirMagnet WiFi Analyzer users can also view the co-existence summary view (information such as Non-HT Stations detected and more) for the 802.11n APs by clicking **Easy View>View by 802.11n** on the **Start** screen.

SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
	Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
20/40	None	20	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
20/40	Below	Any	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
40	Below	Any	Non-HT STAs present	0	N	Prohibited	N	N	0	N	SM e
40	None	20	Non-HT STAs present	0	Y	Prohibited	N	N	0	N	SM e
	Below	Any	One ore more non-HT S...	0	Y	Prohibited	N	N	0	N	SM e
	Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	Stati
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e

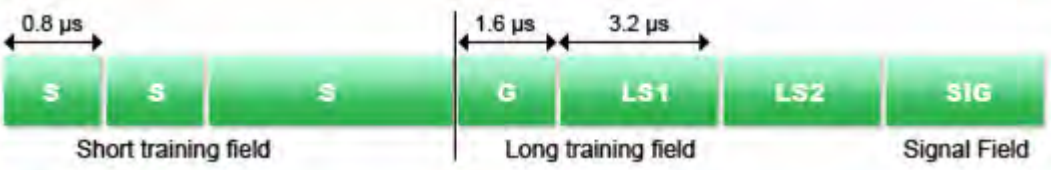
AirMagnet WiFi Analyzer's 802.11n Easy View

HT-Enabled AP with OLBC

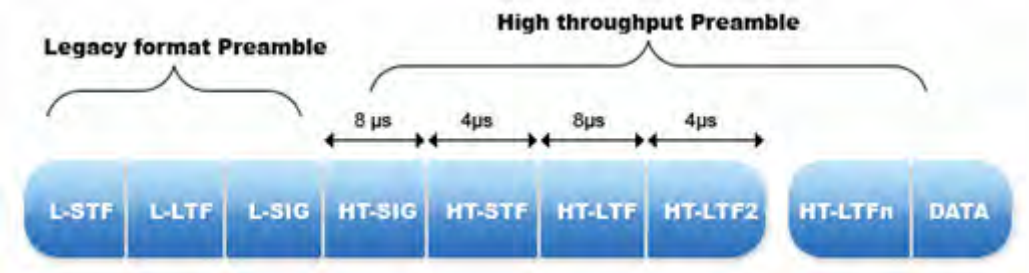
Alarm Description & Possible Causes

Even though, 802.11n APs are designed to be backward-compatible with stations built using the legacy 802.11a/b/g standards, 802.11n users have the option of operating in the so-called Greenfield mode. An 802.11n Greenfield deployment is an 802.11n network deployed and operating in such a way that backwards compatibility with legacy 802.11a/b/g devices is not required. This is the most efficient mode of an 802.11n network, as it allows full use of the 802.11n feature set. Data rate penalties are paid at both the PHY and MAC layers of 802.11n when legacy protection is required.

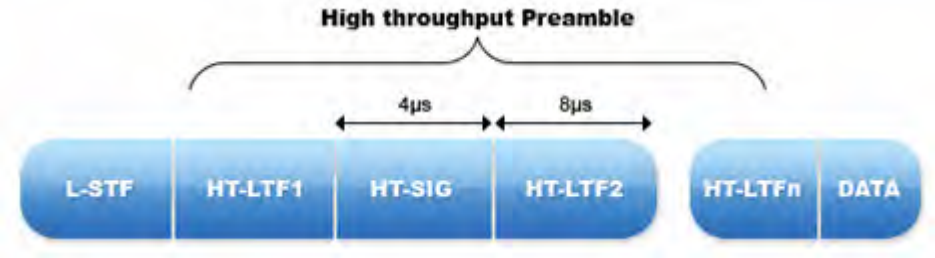
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



HT Preamble

An even larger penalty is paid at the MAC layer, as 802.11n HT transmissions must be preceded by low-speed, legacy format CTS-to-self, RTS/CTS or similar frame exchanges, in order for the virtual carrier sense mechanisms in the legacy nodes to function. Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. This means that, when protection is required, the HT transmission (potentially) uses more time for the “protection” frames than it does for its own data. Even though RTS and CTS type frames are relatively short, it takes more time to transmit an RTS/CTS exchange at a legacy rate of 6 Mbps than it does to transmit 500 bytes at the highest 802.11n data rate.

It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

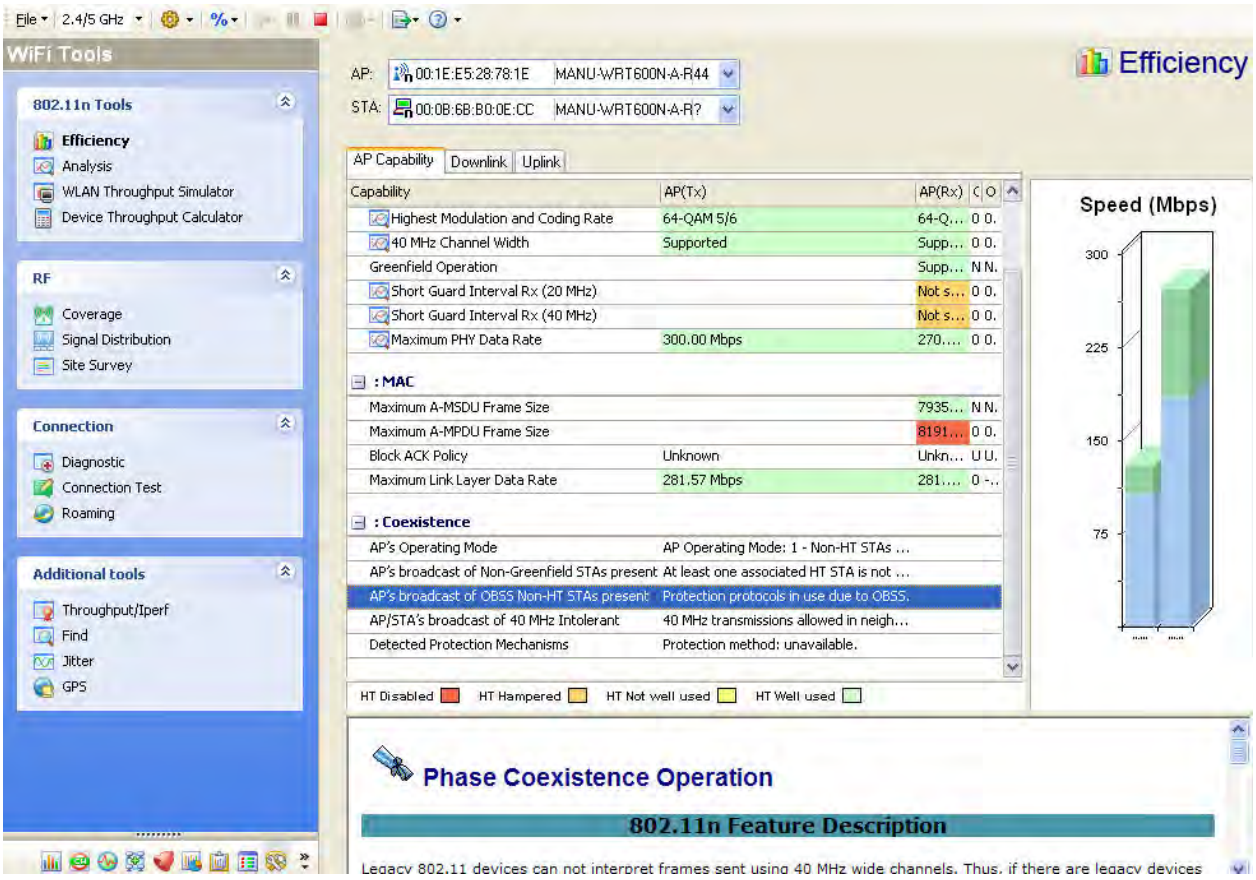
OLBC (Overlapping Legacy BSS Condition) refers to a situation in which a legacy (that is, 802.11a/b/g) BSS is detected in the vicinity of an 802.11n BSS to the extent that the 802.11n AP can hear beacons from the neighboring BSS.

AirMagnet Solution

AirMagnet Wi-Fi Analyzer alerts on the AP (implementing protection mechanisms as described above) and the channel when it detects beacons from legacy BSS operating within range of an HT-enabled AP (AirMagnet has detected the AP sending HT traffic) on the same channel or an overlapping channel. This condition leads to potential throughput problems as protection mechanisms are implemented. AirMagnet recommends that the 802.11n and legacy networks be physically separated, or at a minimum, separated by operating channel(s).

AirMagnet Wi-Fi Analyzer detecting HT traffic from an 802.11n AP

AirMagnet Wi-Fi Analyzer's Efficiency tool analyzes the capabilities of the 802.11n AP and will inform the user for any co-existence issues with legacy 802.11 a/b/g devices.



AirMagnet Wi-Fi Analyzer's Efficiency Tool indicating co-existence issues

AirMagnet will alert the user on multiple co-existence issues, such as:

1. There are Non-HT Stations present in the primary or the secondary channel.

2. If there are associated stations that are not Greenfield capable.

3. There are non-HT Stations present in the overlapping BSS.

4. Overlapping BSSs allow 40 MHz transmissions.

AirMagnet Wi-Fi Analyzer users can also view the co-existence summary view for the 802.11n Access Points by clicking **Easy View>View by 802.11n** from the Start screen.

SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
	Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
20/40	None	20	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
20/40	Below	Any	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
40	Below	Any	Non-HT STAs present	0	N	Prohibited	N	N	0	N	SM e
40	None	20	Non-HT STAs present	0	Y	Prohibited	N	N	0	N	SM e
	Below	Any	One ore more non-HT S...	0	Y	Prohibited	N	N	0	N	SM e
	Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	Stati
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e

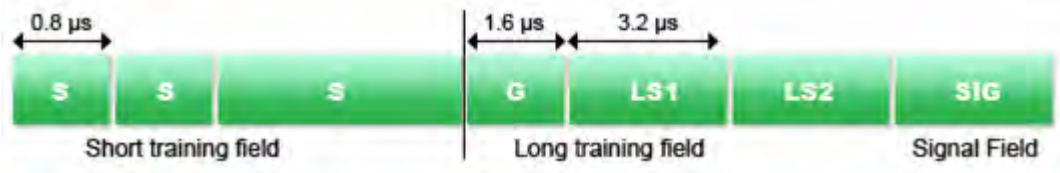
AirMagnet Wi-Fi Analyzer's 802.11n Easy View

OLBC Detected on Channel Not Implementing Protection Mechanisms

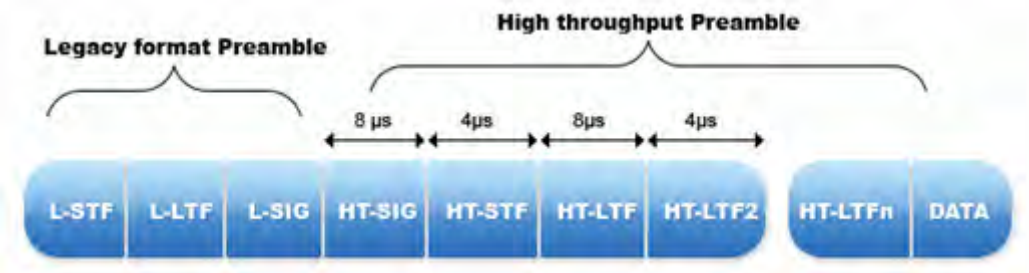
Alarm Description & Possible Causes

Similar to 802.11g devices that needed protection mechanisms to maintain backwards compatibility with 802.11b devices, the 802.11n devices also must employ various protection mechanisms to protect their transmission from legacy 802.11 a/b/g devices. 802.11n devices send signals that cannot be understood by the legacy devices. To prevent collisions and unwanted interference, it is very critical that protection mechanisms be implemented in the network.

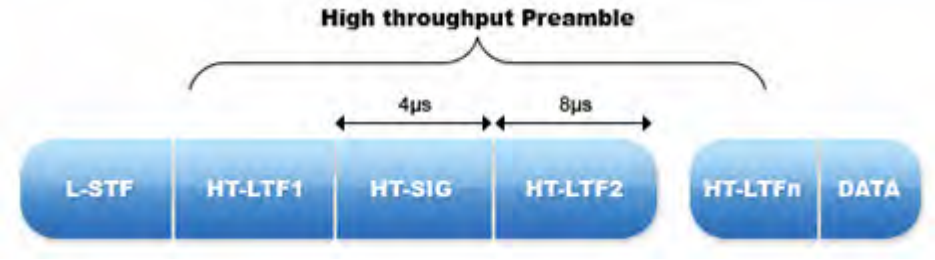
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



HT Preamble

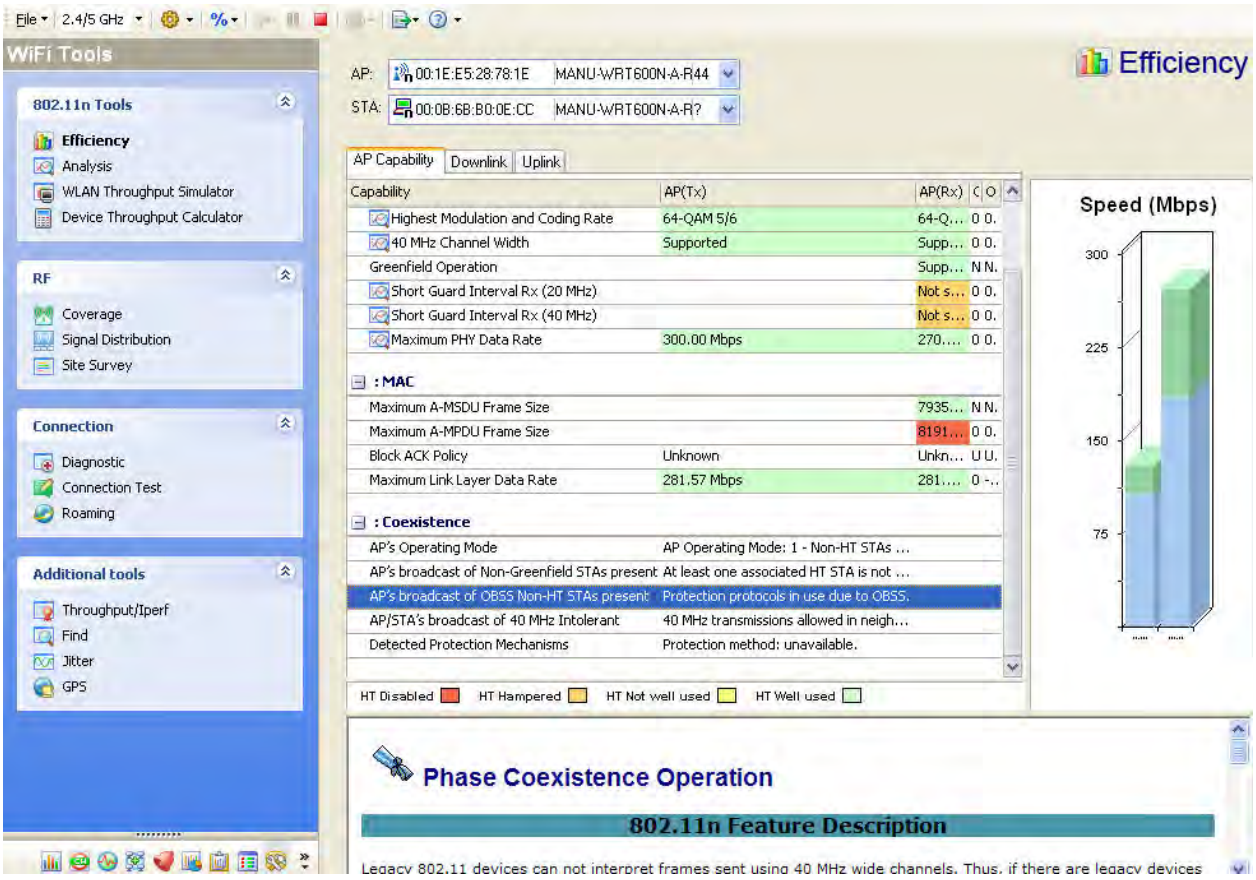
Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play.

OLBC (Overlapping Legacy BSS Condition) refers to a situation in which a legacy (that is., 802.11a/b/g) BSS is detected in the vicinity of an 802.11n BSS to the extent that the 802.11n AP can hear beacons from the neighboring BSS.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on the channel when it detects beacons from legacy BSS operating within range of an HT-enabled AP (AirMagnet has detected the AP sending HT traffic) on that channel or an overlapping channel and that AP is not implementing any protection mechanism to protect its transmission from legacy devices. AirMagnet recommends that the 802.11n and legacy networks be physically separated, or at a minimum, separated by operating channel(s).

AirMagnet WiFi Analyzer's Efficiency Tool analyzes the capabilities of the 802.11n AP and will inform the user for any co-existence issues with legacy 802.11 a/b/g devices.



AirMagnet WiFi Analyzer's Efficiency tool indicating co-existence issues

AirMagnet WiFi Analyzer will alert the user on multiple co-existence issues, such as:

1. There are Non-HT Stations present in the primary or the secondary channel
2. If there are associated stations that are not Greenfield capable.
3. There are non-HT Stations present in the overlapping BSS
4. Overlapping BSSs allow 40 MHz transmissions.

AirMagnet WiFi Analyzer users can also view the co-existence summary view for the 802.11n Access Points by using the "802.11n easy view" from the START page.

	SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
		Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
	20/40	None	20	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
	20/40	Below	Any	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
	40	Below	Any	Non-HT STAs present	0	N	Prohibited	N	N	0	N	SM e
	40	None	20	Non-HT STAs present	0	Y	Prohibited	N	N	0	N	SM e
		Below	Any	One ore more non-HT S...	0	Y	Prohibited	N	N	0	N	SM e
		Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
		Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	Stati
		None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e

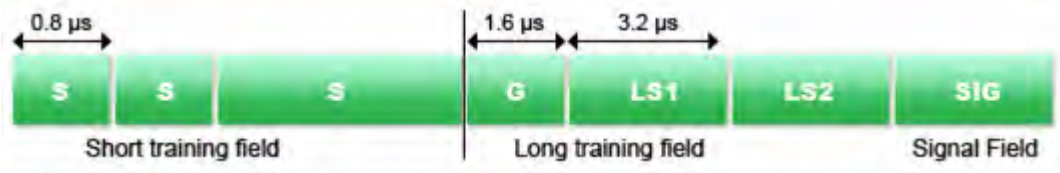
AirMagnet WiFi Analyzer's 802.11n Easy View

Non-Required Protection Mechanism Detected

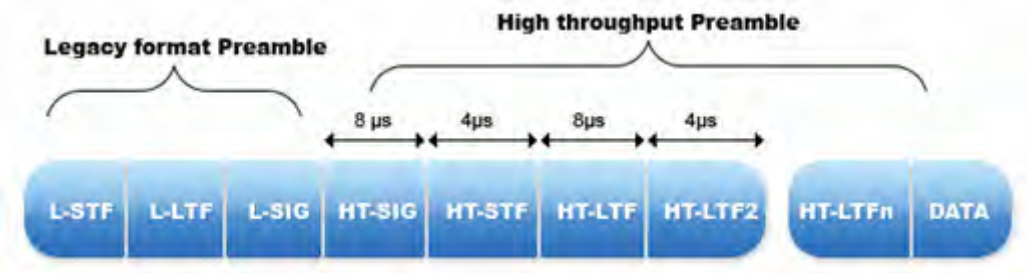
Alarm Description & Possible Causes

Similar to 802.11g devices that needed protection mechanisms to maintain backwards compatibility with 802.11b devices, the 802.11n devices also must employ various protection mechanisms to protect their transmission from legacy 802.11 a/b/g devices. 802.11n devices send signals that cannot be understood by the legacy devices. To prevent collisions and unwanted interference, it is very critical that protection mechanisms be implemented in the network.

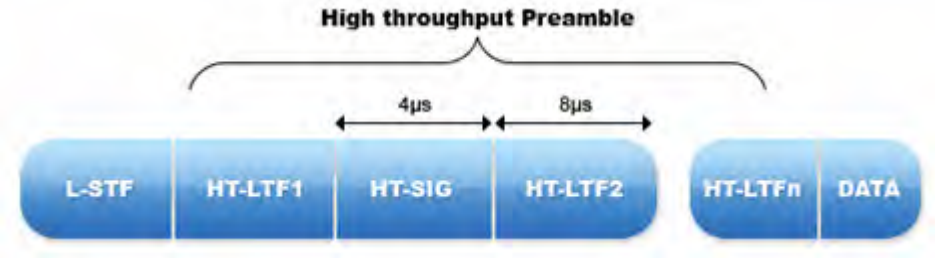
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



HT Preamble

Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on the AP and the channel when it does not detect any legacy APs operating on the same channel as an HT-enabled AP (AirMagnet has detected the AP sending HT traffic), but detects the following situations:

1. A protection mechanism has been detected, or
2. The APs beacon says OBSS Non HT STAs are present, or
3. The APs beacon says the operating mode is 1 (non HT STAs present in primary or secondary channel).

AirMagnet WiFi Analyzer users can also view the co-existence summary view for the 802.11n access points by using the **Easy View>View by 802.11n** from the Start screen. See the illustration below.

Type		Device	MAC	S	SSID	Non HT OBSS	Tx Ch Width	Rx Ch Width	PCO		SGI
.11: n											
AP	11	D-Link:62:A6:F0	00:1B:11:62:A6:F0	41	QA-dlinkdraft2-jav	N	20/40	20	N	N	40
AP	11	Cisco-Linksys:95:48:E9	00:1D:7E:95:48:E9	11	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	11	Belkin:21:4F:C7	00:17:3F:21:4F:C7	50	QA-TestNetwork-AT	N	20/40	20/40	N	N	40
AP	11	Cisco-Linksys:26:AA:59	00:1E:E5:26:AA:59	48	QA-TestNetwork-SW	Y	20/40	20/40	N	Y	
STA	?	Wistron Neweb:B0:0...	00:0B:6B:B0:0E:E1	31		N	20/40	20	N	N	40
STA	11	Wistron Neweb:B0:0...	00:0B:6B:B0:05:74	43		N	20	20	N	N	
AP	153	ciscoap1250	00:17:DF:A6:5B:DE	21	QA-1250-MV-2	N	20/40	20/40	N	N	20/40
AP	149	Apple:FA:B8:CE	00:19:E3:FA:B8:CE	44	QA-TestNetwork-BC	N	20/40	20/40	N	N	40
AP	153	ciscoap1250	00:17:DF:A6:5B:DD	21	QA-1250-MV-3	N	20/40	20/40	N	N	20/40
AP	44	Cisco-Linksys:28:78:C9	00:1E:E5:28:78:C9	31	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	48	Cisco-Linksys:95:E4:44	00:1D:7E:95:E4:44	52	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	11	ciscoap1250	00:17:DF:A6:5B:D0	0	QA-1250-MV-1	N	20/40	20/40	N	N	20/40
STA	48	Cisco-Linksys:03:29:F2	00:1D:7E:03:29:F2	0							

Start screen showing APs with Non-HT OBSS stations present

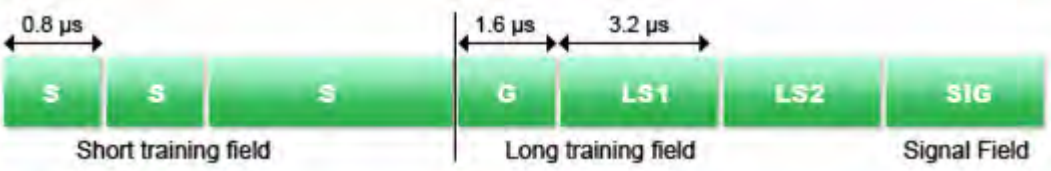
AP Operating in Mixed-Mode

Alarm Description & Possible Causes

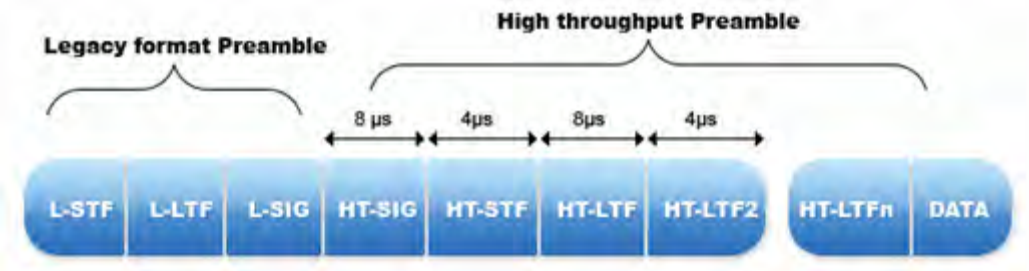
802.11n users have the option of operating in the so-called Greenfield mode where an 802.11n network deployed and operating in such a way that backward s compatibility with legacy 802.11a/b/g devices is not required. This is the most efficient mode of an 802.11n network, as it allows full use of the 802.11n feature set. Data rate penalties are paid at both the PHY and MAC layers of 802.11n when legacy protection is required.

However, the mandatory HT Mixed mode will be the most common 802.11n AP operating mode for the next year or so. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode.

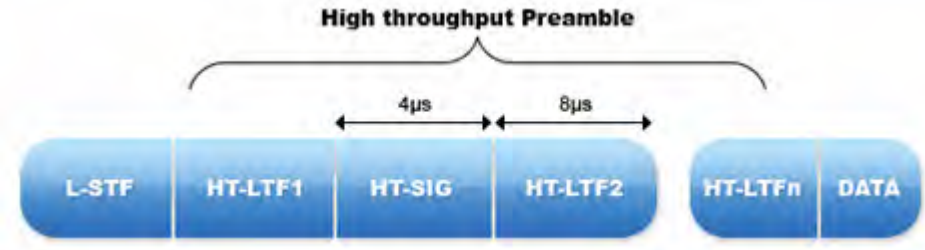
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



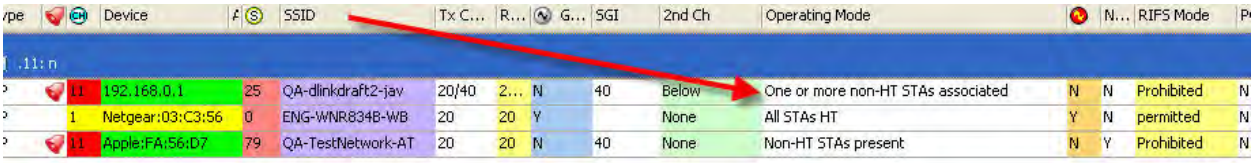
HT Preamble

An even larger penalty is paid at the MAC layer, as 802.11n HT transmissions must be preceded by low-speed, legacy format CTS-to-self, RTS/CTS or similar frame exchanges, in order for the virtual carrier sense mechanisms in the legacy nodes to function. Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. This means that, when protection is required, the HT transmission (potentially) uses more time for the “protection” frames than it does for its own data. Even though RTS and CTS type frames are relatively short, it takes more time to transmit an RTS/CTS exchange at a legacy rate of 6 Mbps than it does to transmit 500 bytes at the highest 802.11n data rate.

It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

AirMagnet Solution

AirMagnet alerts on the AP and its operating channel when it detects an AP beaconing an operating mode of 3 (one or more non-HT STAs associated), or it detects non-HT STAs associated to the AP.



AirMagnet WiFi Analyzer's 802.11n easy view indicating AP with non-HT STAs associated to it

AirMagnet WiFi Analyzer users can this information for the 802.11n Access Points by clicking **Easy View>View by 802.11n** from the Start screen.

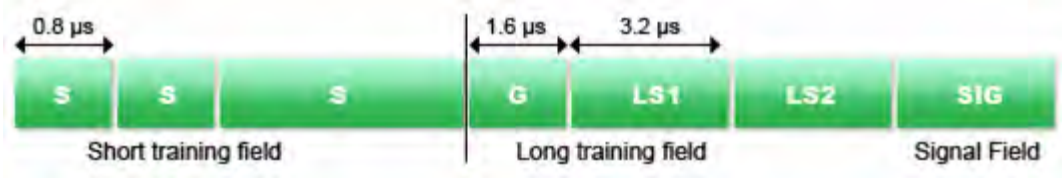
Mixed-Mode AP Not Implementing Protection Mechanism

Alarm Description & Possible Causes

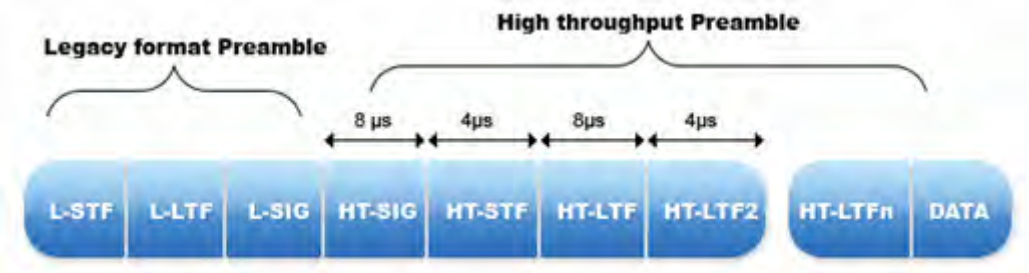
802.11n users have the option of operating in the so-called Greenfield mode where an 802.11n network deployed and operating in such a way that backward s compatibility with legacy 802.11a/b/g devices is not required. This is the most efficient mode of an 802.11n network, as it allows full use of the 802.11n feature set. Data rate penalties are paid at both the PHY and MAC layers of 802.11n when legacy protection is required.

However, the mandatory HT Mixed mode will be the most common 802.11n AP operating mode for the next year or so. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode.

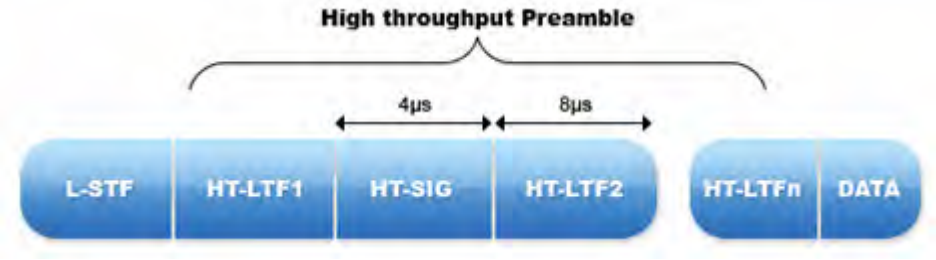
In the PHY layer, 802.11n devices must transmit a mixed mode preamble, even with HT (802.11n High Throughput) transmissions, when legacy protection is required. This mixed mode preamble is essentially a legacy format preamble, followed by an HT preamble. This allows legacy stations which do not understand the HT preamble to still recognize the transmission and defer the medium. In a Greenfield deployment, only the HT preamble is used:



Legacy Preamble



Mixed Mode Preamble



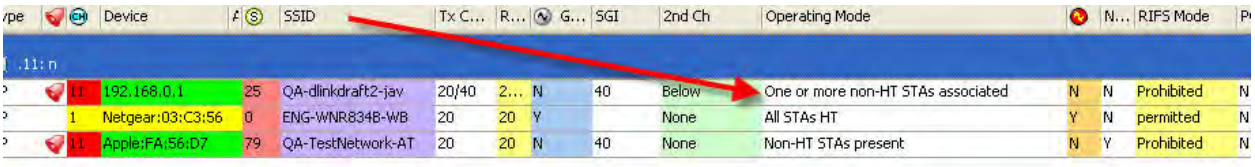
HT Preamble

An even larger penalty is paid at the MAC layer, as 802.11n HT transmissions must be preceded by low-speed, legacy format CTS-to-self, RTS/CTS or similar frame exchanges, in order for the virtual carrier sense mechanisms in the legacy nodes to function. Legacy nodes update their Network Allocation Vector (NAV), which is used to virtually determine when the medium will become free again, based upon the Duration/ID fields present in these frames. This means that, when protection is required, the HT transmission (potentially) uses more time for the "protection" frames than it does for its own data. Even though RTS and CTS type frames are relatively short, it takes more time to transmit an RTS/CTS exchange at a legacy rate of 6 Mbps than it does to transmit 500 bytes at the highest 802.11n data rate.

It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

AirMagnet Solution

AirMagnet Wi-Fi Analyzer alerts on an HT-enabled AP (AirMagnet has detected the AP sending HT traffic) and its operating channel when it detects an AP beaconing an operating mode of 3 (one or more non-HT STAs associated), or it detects non-HT STAs associated to the AP, but is not implementing any protection mechanism to protect its transmission from legacy devices.



AirMagnet Wi-Fi Analyzer's 802.11n easy view indicating HT- enabled AP with non-HT STAs associated to it

AirMagnet Wi-Fi Analyzer users can this information for the 802.11n APs by clicking **Easy View>View by 802.11n** on the Start screen.

Greenfield-Capable BSS Operating in Mixed Mode

Alarm Description & Possible Causes

802.11n users have the option of operating in the so-called Greenfield mode where an 802.11n network deployed and operating in such a way that backward s compatibility with legacy 802.11a/b/g devices is not required. This is the most efficient mode of an 802.11n network, as it allows full use of the 802.11n feature set. Data rate penalties are paid at both the PHY and MAC layers of 802.11n when legacy protection is required.

However, the mandatory HT Mixed mode will be the most common 802.11n AP operating mode for the next year or so. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode. It should be noted that a legacy station does not even have to be associated with an 802.11n BSS, in order for these protection mechanisms to come into play. Merely the presence of frames from legacy devices causes 802.11n Greenfield networks to downgrade performance to mixed mode operation.

A Clause 20 STA (hereinafter referred to as an HT STA) advertises information about what types of STAs are observed to be present, using the Beacon and Probe Response frames. These frames carry the HT Information Element, which include the following fields:

- Operating Mode
- Non-Greenfield STAs Present
- OBSS Non-HT STAs Present

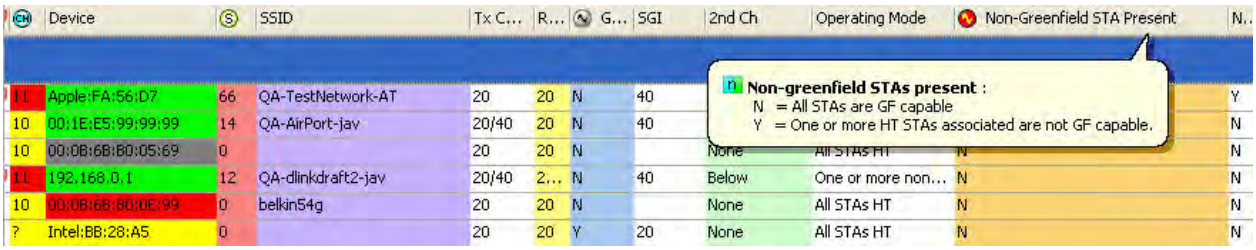
The Operating Mode field indicates the operating mode of the BSS, and may take one of four possible values:

- 0: All STAs in the BSS are HT STAs (no non-HT STAs are present in the BSS)
- 1: Non-HT STAs are present in the primary and/or the secondary channel
- 2: All STAs in the BSS are HT STAs, however at least one STA supports only 20 MHz operation
- 3: One or more non-HT STAs are present in the BSS

The non-Greenfield STAs present field indicates whether or not all HT STAs that are associated are Greenfield capable.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on the AP and its operating channel when it detects an AP beaconing an operating mode of 3 (one or more non-HT STAs associated), or using one of the 802.11n protection mechanisms, but all of its associated STAs are Greenfield capable or the AP has beaconed that there are no non-GF STAs associated. To enjoy some of the high throughput benefits of 802.11n, AirMagnet recommends that all Greenfield Capable devices should be operating in the Greenfield mode.



AirMagnet WiFi Analyzer's 802.11n easy view displaying devices that are Greenfield-capable

Diversity Insufficient for MIMO

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer has detected poor MIMO throughput, which may be due to insufficient Tx Antenna or Tx Path diversity. MIMO systems take advantage of spatial multiplexing (and potentially space-time code blocks) for throughput gains. This gain can be diminished if the spatial signatures of each received stream is not sufficiently diverse. This may be an environmental or Tx Antenna spacing effect.

AirMagnet Solution

TBD – May not be implemented, depending on further testing and analysis.

Missing Performance Options

Alarm Description & Possible Causes

The IEEE 802.11b standard defines several optional device capabilities to improve performance levels:

- **Short preamble**: The preamble refers to the header information in a packet. Generally, a longer preamble time simply gives the device decoding the packet more time to work. A shorter preamble is usually intended to improve efficiency by generating less delay during the decode process (this becomes important in systems that are particularly sensitive to delays, such those implementing Voice-over-IP).
- **PBCC RF modulation**: Packet Binary Convolutional Coding is a proprietary setting in some devices that can potentially increase network speeds above

the standard theoretical limit on 802.11b performance. While this can improve your network performance, it may require you to use only APs and access cards from a specific vendor.

- **Channel agility**: This setting on your AP allows the device to scan for the least-congested channel during its initial configuration. A device without this feature may be implemented on an overloaded channel, thus resulting in interference.

AirMagnet Solution

During the WLAN design and deployment process, you may decide to take advantage of and rely on these optional capabilities. If you enable this alarm, AirMagnet WiFi Analyzer monitors on them and raises alarms if any wireless devices do not support these options.

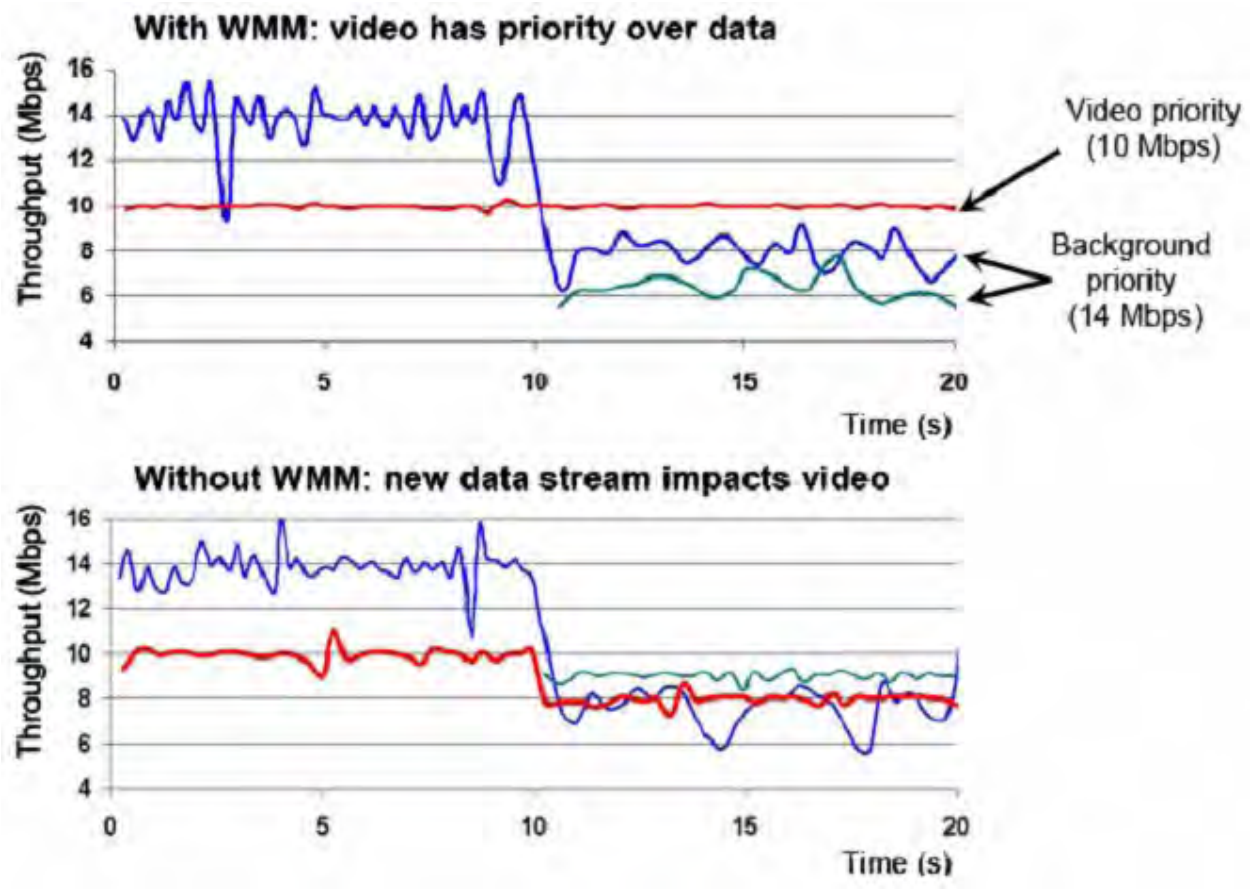
QoS Disabled on 802.11n AP

Alarm Description & Possible Causes

According to the 802.11 standard, all WLAN users share the network's capacity, and no packet gets priority over any other. This usually does not cause a problem with typical data applications (for example, e-mail, Web, file transfers), but it becomes very critical in the case of voice calls and streaming video where packets have to get across the network at the right time to avoid choppy or dropped calls. QoS helps guarantee priority for certain applications. With no QoS implemented and all packets having the same priority, all packets regardless of the application (data, voice, video) would have equal chances in being dropped in a congested transaction. This will be very critical for 802.11n networks where there could be multimedia applications like High-Definition video streams, supported as the same time as Voice streams and data transfers.

The 802.11 standard was designed with two communication methods: DCF (Distributed Coordination Function) and PCF (Point Coordination function). In the DCF mode, the stations have to ensure that the medium is quiet before it can transmit data or detect any collision. In the PCF mode, APs act as the point coordinators and periodically send parameters to the stations and poll them for data. Neither takes into account the type of traffic or priority. The IEEE 802.11e standard introduces EDCF (Enhanced Distributed Coordination Function) and Hybrid Coordination Function (HCF).

In EDCF, stations have various priority levels. Once the medium is idle, the stations wait for a period of time defined by the corresponding traffic priority level called the Arbitration Interframe Space (AIFS). A higher-priority traffic category will have a shorter AIFS than a lower-priority traffic category. Thus stations with lower-priority traffic wait longer than those with high-priority traffic before trying to access the medium. Collisions are further avoided by using additional time slots called the contention window before transmission. If a station detects another station transmitting data, it must wait till the next idle period and continue its countdown. With Hybrid Coordination Function (HCF), the hybrid controller will poll stations during a contention-free period and grant a station a specific start time and maximum transmission duration.



Effects of QoS implementation

AirMagnet Solution

AirMagnet WiFi Analyzer can detect 802.11n APs that are not implementing QoS, which could lead to higher priority traffic such as voice to be transmitted with a certain amount of delay. This can lead to choppy audio or dropped calls. AirMagnet recommends using the QoS feature, if available, on an AP when different types of traffic are serviced by the same AP.

40-MHz Channel Mode Detected in 2.4 GHz Spectrum

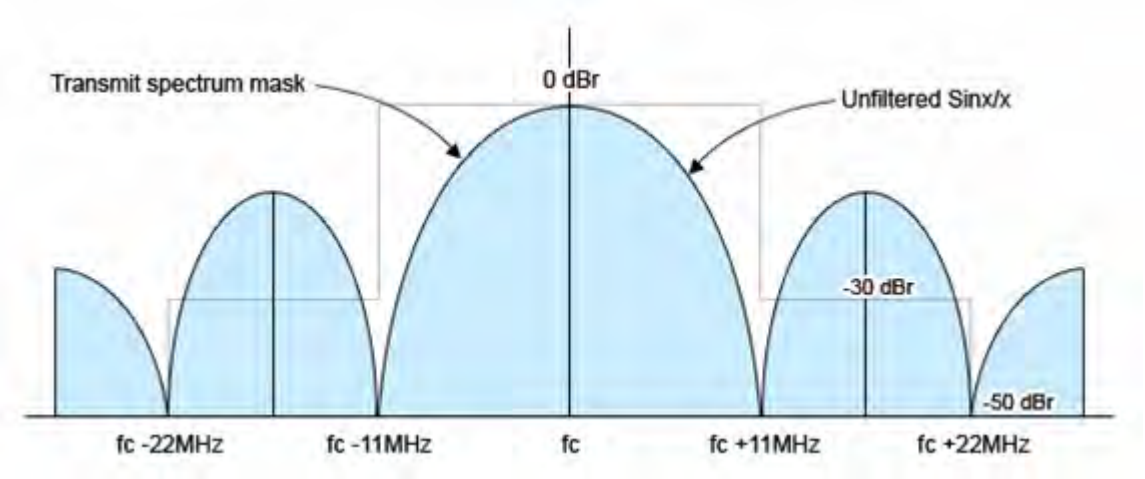
Alarm Description & Possible Causes

Legacy 802.11 systems operate on channels that are 20 MHz wide (actually the channels are 22 MHz wide, but generally referred to as 20 MHz). 802.11n defines both 20 MHz and 40 MHz wide channel operation. When operating in 40 MHz mode, the capacity of the channel is effectively double that of legacy systems. One may liken this to “doubling the number of lanes on a freeway so that twice as many cars may pass through”.

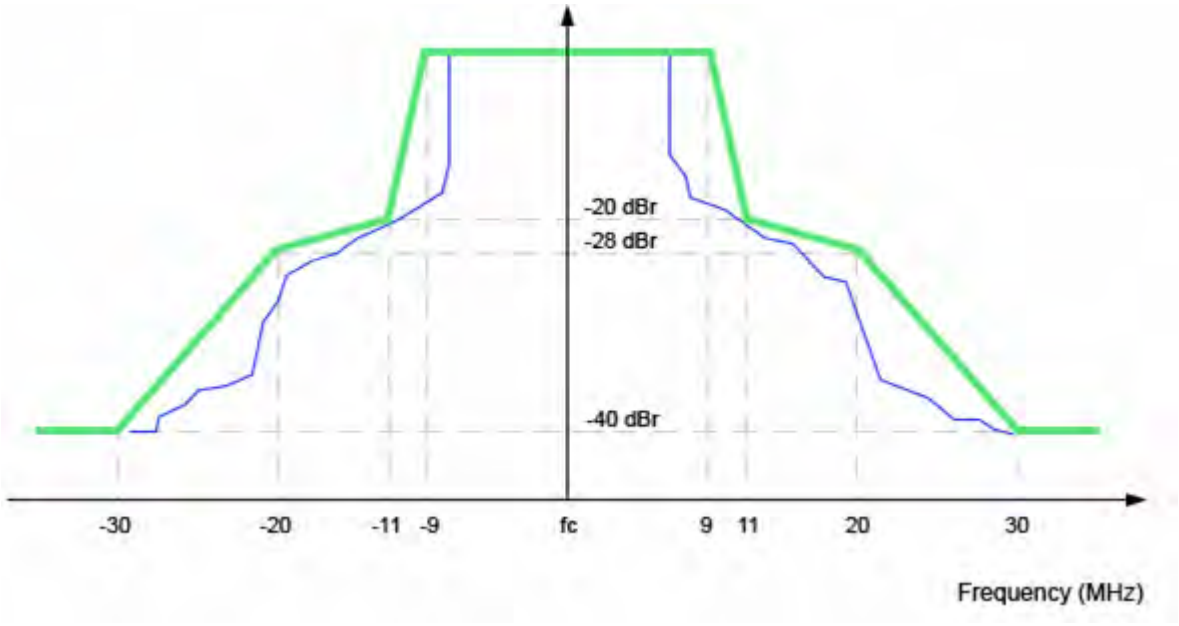
The fourteen 802.11 channels in the 2.4 GHz band (eleven usable channels in the US) are spaced 5 MHz apart, with center frequencies from 2412 MHz to 2477 MHz.

North American Channelization Scheme

RF channels do not have exact edges. The modulated portion of a (20 MHz) 802.11 RF signal “falls” into +/- 11 MHz of the center frequency (thus, it is 22 MHz wide); there is however some “bleed over”, or unmodulated RF energy, that is present to about +/- 30 MHz of the center frequency (at relatively much lower power levels). The spectrum mask defines how much RF energy may be present outside the channel boundary of +/- 11 MHz.



802.11b (DSSS/CCK) Spectrum Mask

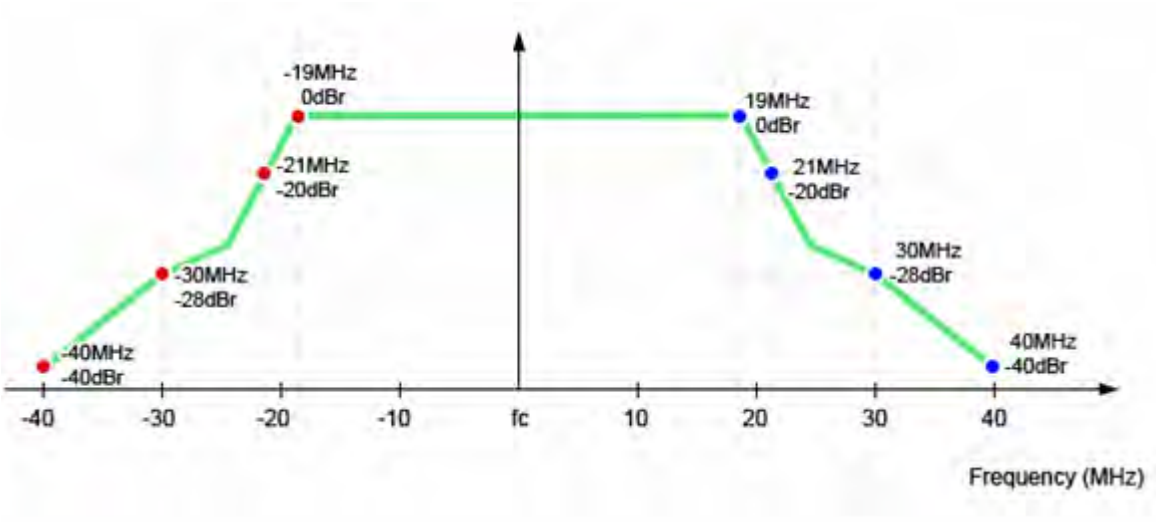


802.11g (OFDM) Spectrum Mask

An 802.11 transmission thus “takes up” 5 channels (the center, two left adjacent and two right adjacent channels). Depending on transmit power and receiver sensitivity; a transmission may even cause interference on several additional channels (up to 5 away from the center).

For instance, a device transmitting on channel 6 will certainly cause significant interference on channels 5 and 7, and some interference on channels 4 and 8. It may even cause (usually negligible) interference on channels 2, 3, 9 and 10 as well. This is why, in FCC regulated domains, there are effectively just 3 simultaneously usable 802.11 20 MHz channels in the 2.4 GHz band. A typical North American 802.11 b/g deployment will place APs on channels 1, 6 and 11 to cope with “bleed over”. This channel deployment scheme allows APs in close proximity to each other to minimize interference with each other.

Operating 40 MHz mode in the 2.4 GHz band exacerbates this problem significantly. As can be seen in the following figure, the 40 MHz spectrum mask (necessarily) allows higher signal energy to be present on adjacent channels.



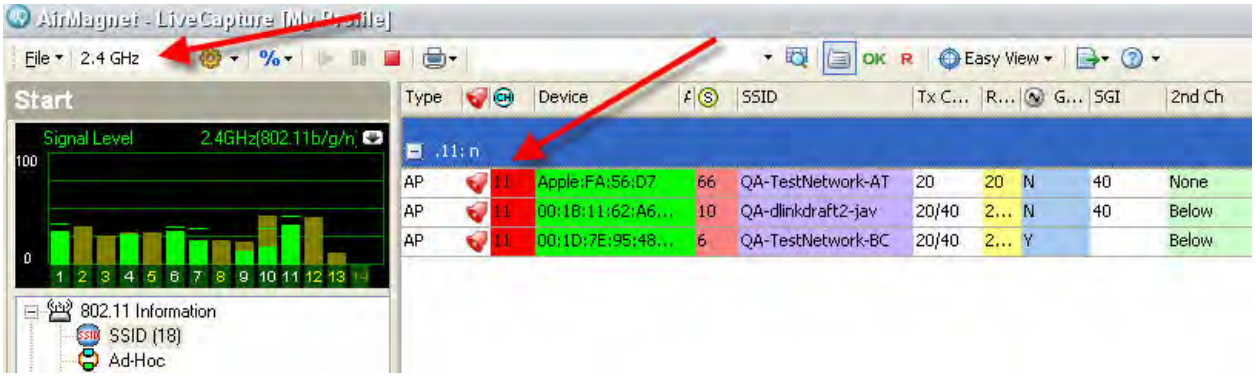
40 MHz Spectrum Mask

Thus, a 40-MHz 802.11 transmission in the 2.4-GHz band takes up 9 channels (the center, four left adjacent and four right adjacent channels). One may immediately see how 40- MHz transmission in the 2.4-GHz band may cause problems, where there are only 11 usable channels. Coexistence mechanisms help to address this, but designing and deploying an efficient multi-user network where a single transmission may use more than 80% of the available spectrum in the band, is difficult.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts the users when it detects a HT40 Upper or HT40 Lower AP operating in the 2.4-GHz spectrum.

AirMagnet recommends the use of 802.11n devices in the 5-GHz spectrum only. In most regulatory domains, there are many more useable channels in the 5 GHz band, and channels are spaced 20 MHz apart. This provides for much more “room” for 40 MHz wide channel operation. Additionally, it should be noted that the 2.4-GHz band is much more crowded than the 5-GHz band, as stations operating in the 2.4-GHz band must also contend with Bluetooth devices, microwave ovens and other common sources of 2.4-GHz interference, such as cordless phones.



AirMagnet WiFi Analyzer screen showing 802.11n APs operating in the 2.4 GHz spectrum

HT-Enabled AP Ignoring Legacy Devices

Alarm Description & Possible Causes

This alarm follows very similar logic to #164 and #167, with the exception that the entire channel (not just the BSS) is included in the search.

AirMagnet Solution

AirMagnet WiFi Analyzer has detected an HT enabled AP which is either not detecting, or ignoring the presence of legacy devices. Protection protocols may not be triggered in this case, causing the legacy device(s) to become hampered

Excessive Multicast/Broadcast on Node

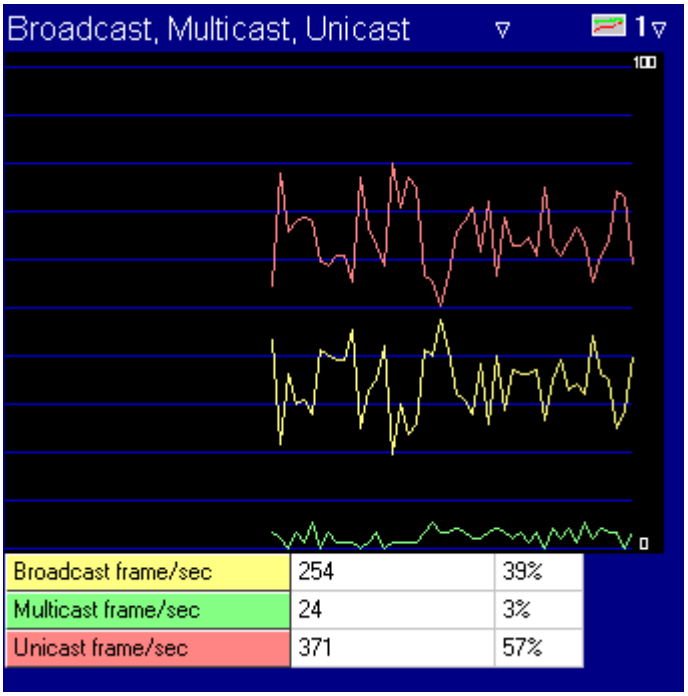
Alarm Description & Possible Causes

Just like the wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices on the WLAN. What makes the WLAN more sensitive to multicast and broadcast frames than the wired networks is the fact that all multicast and broadcast frames are transmitted at low speed (for example, 1 or 2 mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth.

Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 mpbs, which is a considerable delay for a voice application.

AirMagnet Solution

AirMagnet WiFi tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel. To further investigate this multicast and broadcast situation, the AirMagnet Wi-Fi Channel or Infrastructure views can be used to display the corresponding statistics as illustrated below. (The Channel and Infrastructure view are available via the Remote Analyzer of the Enterprise system as well as on the Laptop or Handheld analyzer).

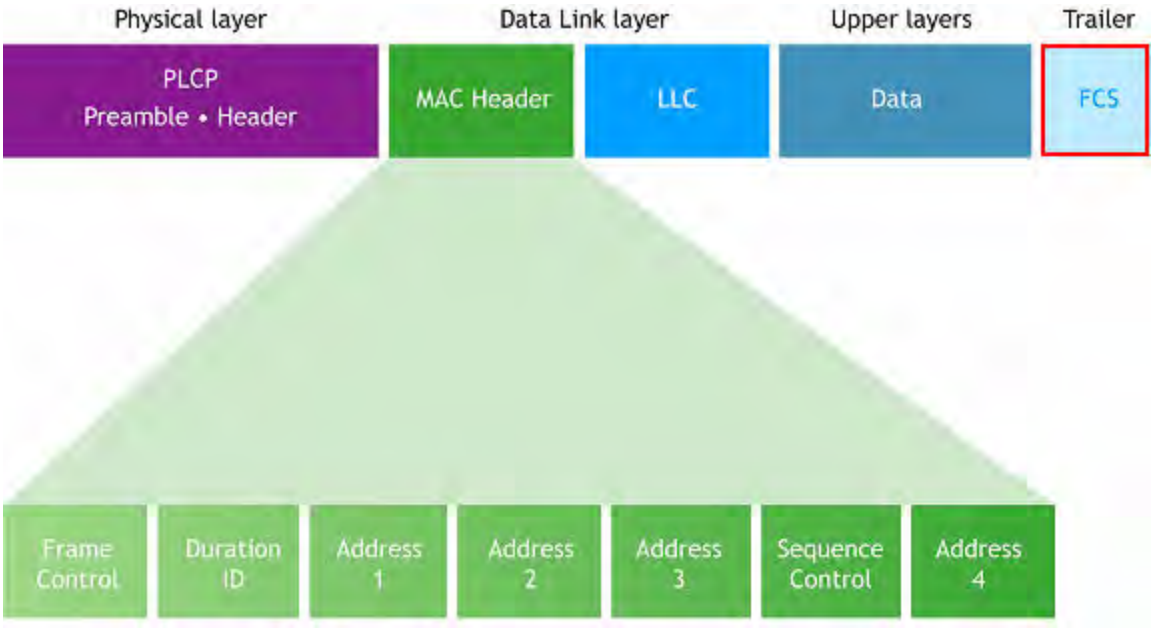


Multi-cast and Broadcast Frames To Raise Alarms on Abused Usage

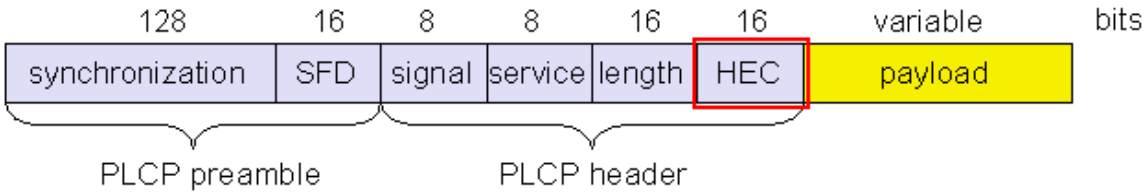
Excessive Frame Errors on Node

Alarm Description & Possible Causes

The WLAN RF spectrum is open, dynamic, shared, and is subject to noise, interference, packet collisions, multipath, hidden node syndrome, etc. IEEE 802.11 has a built in error checking mechanism to detect transmit and receive errors caused by any of the above mentioned issues. For example, the IEEE 802.11b **DSSS** (Direct Sequence Spread Spectrum) physical layer specification defines the PLCP (Physical Layer Convergence Protocol) header to include a HEC (Header Error Check) field for error detection (See illustration below). The receiver performs calculations on the synchronization, service and the length fields and compares it to the transmitted value. If the results do not match, the receiver has to make the decision of terminating the frame.



IEEE 802.11 Frame Includes Checksum in PLCP and FCS for Frame Header and Frame Body Respectively



HEC (Header Error Checksum) defined in PLCP Header

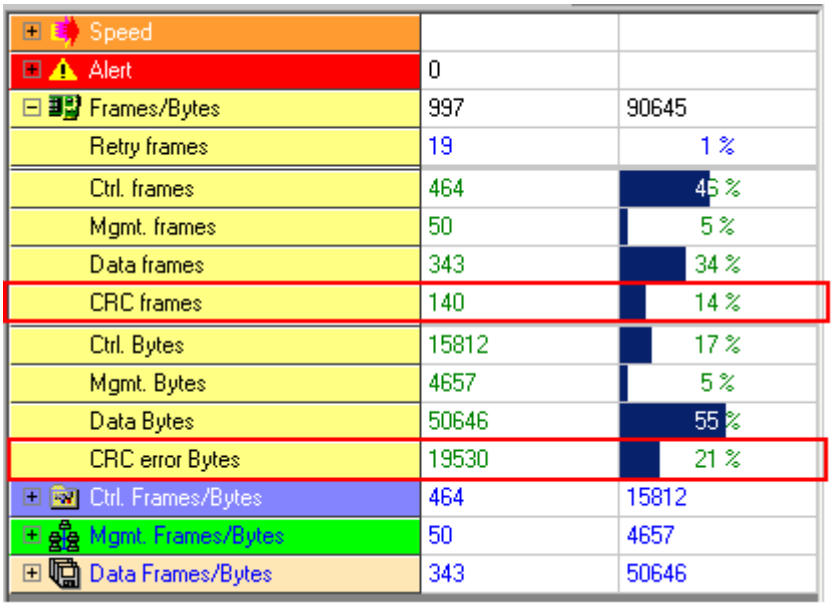
802.11 MAC layer protocol also defines the FCS (Frame Checksum) field at the end of a packet for error detection. See the illustration below:

Frame Control	Duration ID	Address1 (source)	Address2 (destination)	Address3 (rx node)	Sequence Control	Address4 (tx node)	Data	FCS
2	2	6	6	6	2	6	0 - 2,312	4

FCS (Frame Checksum) defined in 802.11 MAC Protocol format

AirMagnet Solution

AirMagnet WiFi Analyzer detects these error frames and tracks them based on per device and per channel orientation. See the illustration below:



Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	45 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

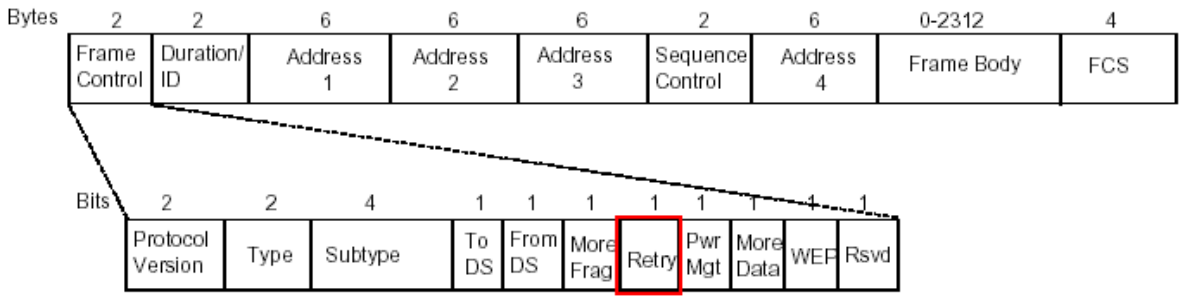
AirMagnet WiFi Analyzer CRC frame error tracking display for a channel or a device

When the CRC error frame to total frame ratio exceeds a user-definable threshold, AirMagnet Wi-Fi alerts the administrator to indicate a possible WLAN performance problem.

Excessive Frame Retries on Node

Alarm Description & Possible Causes

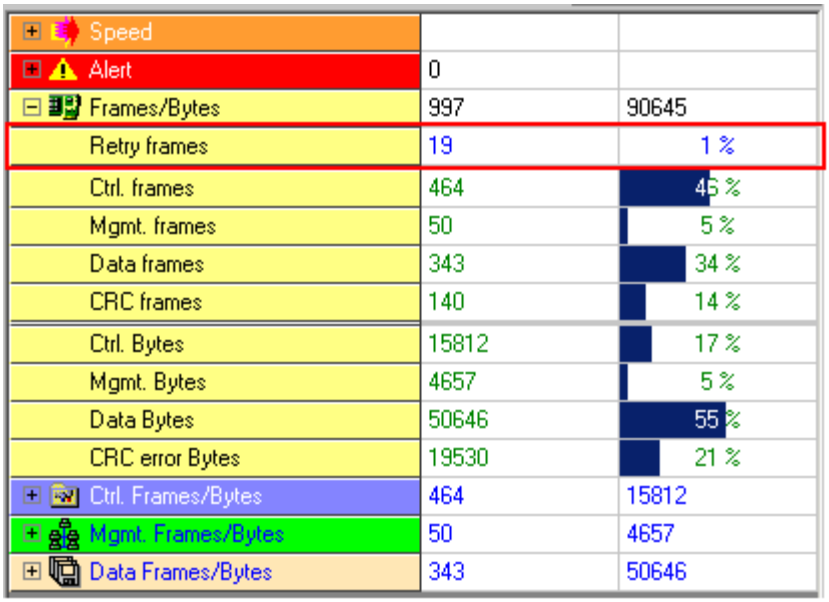
The WLAN RF spectrum is open, dynamic, shared, and is subject to noise, interference, packet collisions, multipath, hidden node syndrome, etc. When there are errors caused due to any of the above issues, the transmitter of the error frame would not receive an 802.11 control frame called an **acknowledgement** frame. When there is no acknowledgement observed, the transmitter assuming that the receiver did not receive the frame successfully would re-transmit the unacknowledged frame with the **Retry** bit in the frame set to one. This indicates a re-transmission. The figure below illustrates the **Retry** field in the 802.11 frame header.



802.11 Frame Header includes the Retry field to indicate frame re-transmission

AirMagnet Solution

AirMagnet WiFi Analyzer detects these retry frames and tracks them on a per device and per channel orientation. Refer to the illustration below:



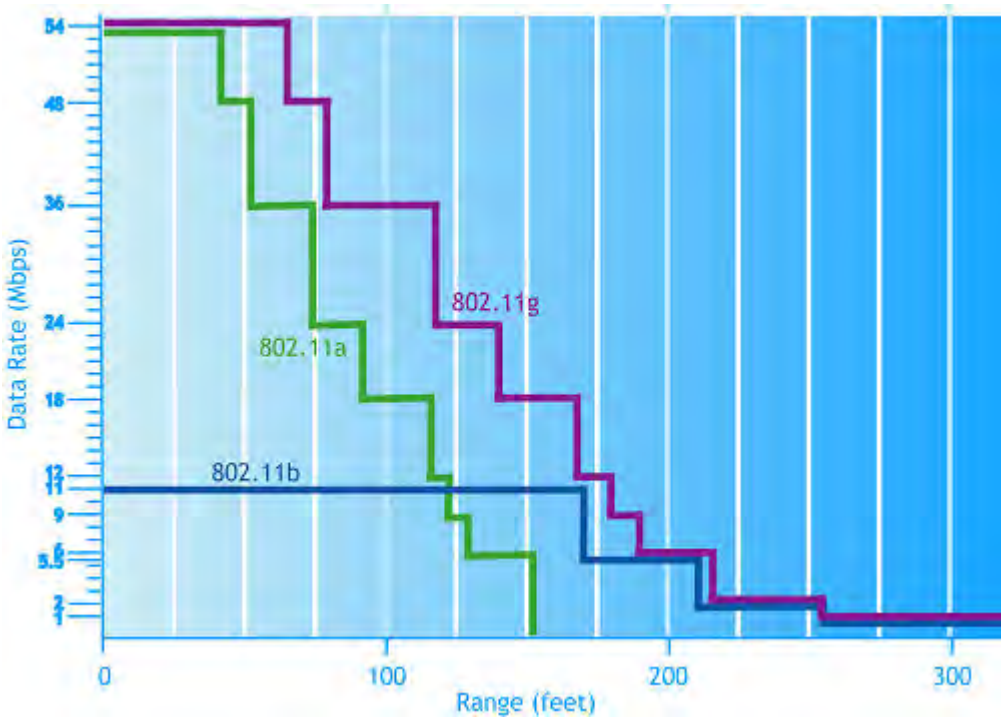
AirMagnet WiFi Analyzer Retry frame error tracking display for a channel or a device

When the retry frame to total frame ratio exceeds a user-definable threshold, AirMagnet Wi-Fi alerts the administrator to indicate a possible WLAN performance problem due to noise, interference, packet collisions, multipath, hidden node syndrome, etc. The administrator can take appropriate steps to avoid such problems.

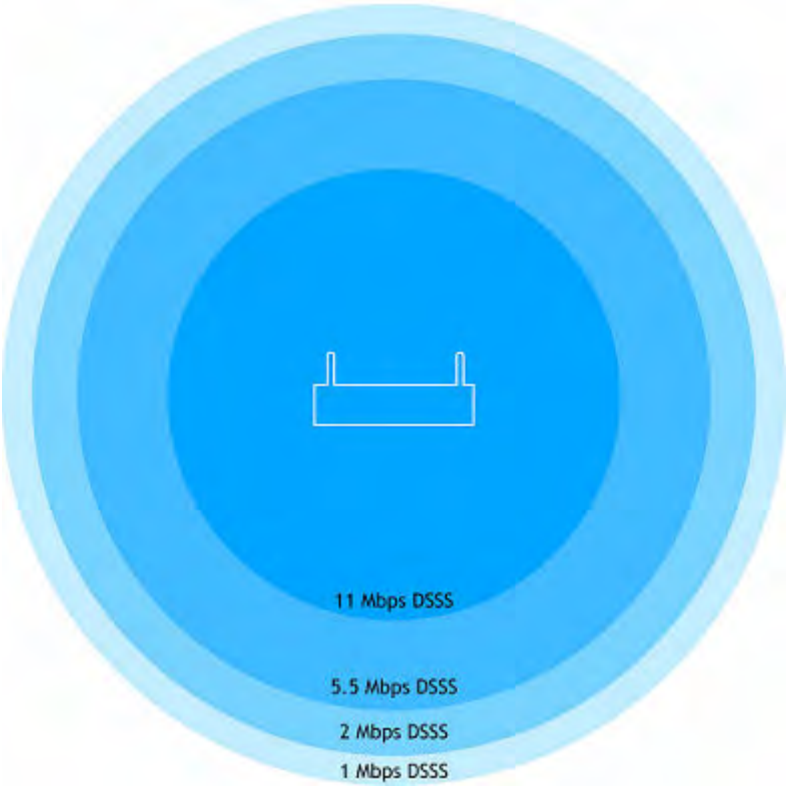
Excessive Low Speed Transmission on Node

Alarm Description & Possible Causes

802.11a, 11b or 11g devices use several different transmit speeds from frame to frame. Higher speed transmission consumes less bandwidth and allows higher throughput. Transmit speed optimization is a key factor during the WLAN site survey and deployment process. It is typically impacted by signal quality and distance.



802.11 a/b/g Speed and Range Correlation



802.11b Speed and Coverage correlation

Refer to the table below for all the supported speeds and what AirMagnet WiFi Analyzer considers to be low speed for the selected standard.

Speed	802.11b (mbps)	802.11g (mbps)	802.11a (mbps)
Support Speed	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54	6, 9, 12, 24, 36, 48, 54
AirMagnet Wi-Fi Considered Low Speed	1, 2	1, 2, 5.5, 6, 9, 11, 12, 24, 36,	6, 9, 12, 24, 36

Supported transmission Speed and AirMagnet WiFi Analyzer considered 'Low' Speed

However, high speed transmission requires better signal quality to achieve the same low error rate as compared to the low speed transmissions. The transmit speed selection is a decision made by the transmitter that will also detect reception problems from the lack of acknowledgements. The transmitter may vary the transmit speed to increase reliability. When this scenario occurs too often, the WLAN slows down and the throughput degrades. Refer to the problem illustrated by an AirMagnet WiFi Analyzer screen shot below. It shows excessive low speed transmission (1mbps), high utilization (32%), and low throughput (931kbps).

AirMagnet WiFi Analyzer Console screen shot on Bandwidth Utilization, Throughput, and Transmit Speed Relationship

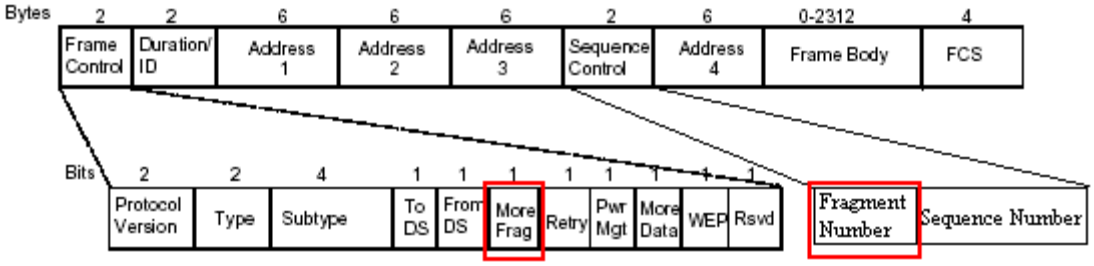
AirMagnet Solution

AirMagnet will alert the administrator if it sees a high amount traffic at lower speeds that may lead to excessive bandwidth usage and lower throughput. The administrator must take appropriate steps to ensure better signal quality to get higher speeds. Also it is important to note that distance of the stations from the AP should be appropriate to avoid lower speed transmissions.

Excessive Fragmentation on Node

Alarm Description & Possible Causes

The 802.11 MAC layer supports fragmentation and defragmentation. The process of partitioning a 802.11 frame into smaller frames for transmission is called fragmentation that helps in increasing reliability and reducing errors. This is accomplished by increasing the probability of successful transmission of the smaller and fragmented frames in cases where channel characteristics limit reception reliability for longer frames. Fragmentation is accomplished at each immediate transmitter before the actual start of transmission. The process of recombining fragmented frames into the original unfragmented longer frame is defined as defragmentation. The IEEE 802.11 standard defines the packet format to identify fragmented frames for defragmentation (illustrated below).



IEEE 802.11 Frame fields for frame fragmentation and defragmentation

The increased reliability for the smaller and fragmented frames come at the cost of frame transmission overhead. The frame is divided into different segments depending upon the fragmentation threshold. The placement of the fragments in the fragmentation process is decided by the "sequence control field" as shown in the figure above. The "more" field indicates if the fragment is the last fragment.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks the fragmentation statistics and alerts on abused fragmentation usage that could lead to degraded WLAN performance. The fragmentation threshold needs to be carefully set to balance the benefit and overhead. Typically, equipment vendors set the default fragmentation threshold to 1536.

Identical Send and Receive Address

Alarm Description & Possible Causes

All standard 802.11 frames transmitted in a wireless environment contain several basic structures which contain the data being transmitted. These structures can vary depending on the type of frame in question, but all frame types will share at least two basic components:

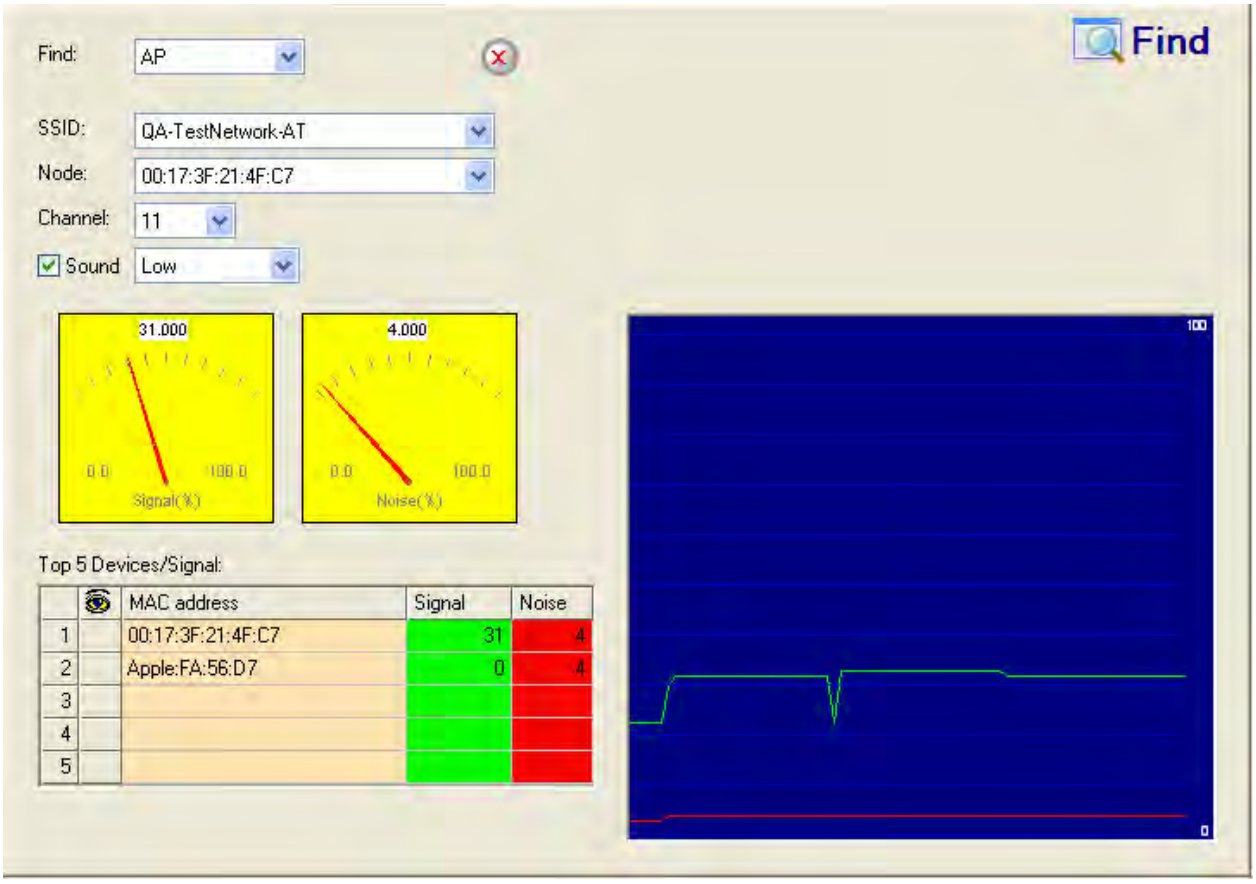
- **Header -** The frame header contains basic information about the device that originally transmitted the frame (for example, the "source") as well as the device to which the frame should be sent (for example, the "destination").
- **Payload -** The frame payload contains the bulk of the actual data being transmitted in the frame.

In order to inhibit wireless activity in a corporate network, attackers often modify wireless frames to emulate the characteristics of those transmitted by a legitimate user. These modifications can include changes to the frames' Source and Destination MAC information. In general, wireless traffic will always include both a valid source MAC (the device that transmitted the packet) and a valid destination MAC (the intended recipient of the packet). Since a device should never need to send a packet to itself, these fields should always contain different data.

To emulate a corporate user, attackers can create frames that appear to be transmitted from a valid device in which the source and destination data fields are identical. This can cause an increase in overall wireless traffic and may potentially result in reduced network throughput for actual users.

AirMagnet Solution

In a normal network environment, a frame's source and destination will never be identical. Consequently, when such traffic patterns are identified, AirMagnet WiFi Analyzer will trigger an alarm to alert IT personnel of the anomaly. It is recommended that administrators use the Find Tool to locate the problematic device and deactivate it or otherwise remove it from the enterprise environment.



Improper Broadcast Frames

Alarm Description & Possible Causes

All 802.11 communication is conducted using transmissions of wireless "frames", which contain the data being exchanged. When wireless devices transmit these frames, they can be sent via one of three mechanisms:

- **Broadcast -** Frames that are transmitted to all devices within the wireless environment are described as "broadcast frames". These frames are generally not intended for a single device. AP beacons are an example of a broadcast frame.
- **Multicast -** Frames that are sent to a group of multiple devices are known as "multicast frames". This mechanism allows an AP to send the same frame to multiple devices simultaneously, which can help reduce network utilization. Virtually any data frame can be transmitted via multicast; common examples are frames sent for media streaming purposes.
- **Unicast -** Frames that are intended for a single recipient are termed "unicast frames". In these transmissions, a destination address that identifies the

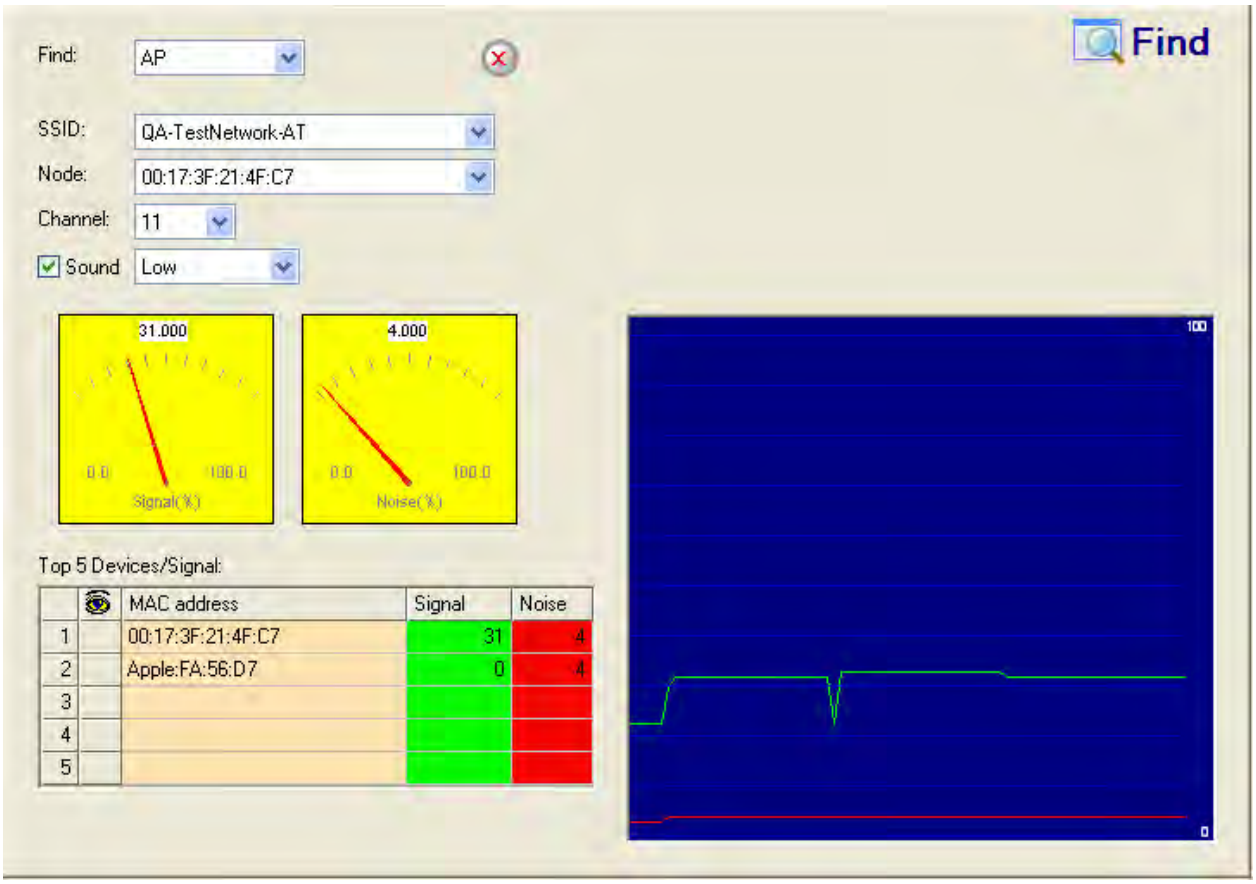
recipient is provided in the frame information. An ACK (acknowledgement) frame from an AP to a station is an example of a unicast frame.

Standard 802.11 deployments allow for some flexibility in the mechanisms used to transmit different frame types; however, if a large number of frames are transmitted via broadcast or multicast, it can reduce network transmit speed and create unnecessary noise in the wireless environment. For example, an Association Request frame is transmitted from a station to an AP when the user attempts to establish a wireless connection. This frame should never be transmitted via broadcast, as it only needs to be sent to the intended AP. Sending the frame as a broadcast will only force other devices in the deployment to scan the transmission in order to determine if they are the intended recipients.

An attacker can take advantage of the broadcast mechanism by flooding the wireless environment with unnecessary broadcast frames, which can prevent valid users from obtaining data or conducting standard wireless transactions. In addition, the speed at which the wireless network operates can be reduced due to the increase in traffic.

AirMagnet Solution

Although an Improper Broadcast Frames alarm can indicate a potential attack, it can often result from a misconfigured AP or wireless client. In either case, the source of the invalid frames should be located using the Find Tool.



After identifying the problematic device, contact IT personnel to ensure that it is reconfigured in accordance with the corporate wireless policy. After this process is complete, the device should function properly when re-deployed.

Simultaneous PCF and DCF Operation

Alarm Description & Possible Causes

IEEE 802.11 defines two medium access protocols:

- **PCF** - Point Coordination Function where an Access Point typically acts as the central coordinator to manage the right to transmit by a polling protocol. All wireless client stations inherently obey the medium access rules of the central coordinator.
- **DCF** - Distributed Coordination Function allows for automatic medium sharing through the use of CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) and a random backoff time following a busy medium condition. In addition, all directed traffic uses immediate positive acknowledgment (ACK frame) where re-transmission is scheduled by the sender if no ACK is received.

DCF is widely supported and deployed where **PCF** is quite the opposite. **DCF** and **PCF** may co-exist in the same RF environment, for example, you and your neighboring company can operate under **DCF** and **PCF** independently. However, by design, such co-existence is acquired through trading in the transmit priority of **DCF** devices to the **PCF** devices. More specifically, the central coordinator of the **PCF** WLAN can access the medium sooner than the **DCF** devices after a busy medium. Therefore, PCF WLAN statistically enjoys higher performance and bandwidth than DCF WLAN in a mixed mode environment. The difference may be more pronounced in a busy WLAN environment.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks the usage of **DCF** and **PCF** protocols. When both medium access protocols are used, AirMagnet WiFi Analyzer raises the awareness of the compromised DCF mode operation.

Reserved MGMT/CTRL Frames

Alarm Description & Possible Causes

Wireless traffic contains transmissions of small units of information known as "frames", which are sent between wireless-capable devices. The 802.11 specification classifies most wireless frames into three major types, as defined by a two-bit field contained in each frame's composition. The main types of frames defined are:

- **DATA -** Data frames (defined by bit code 10) are used for most actual data transmissions in the network.
- **CTRL -** Control frames (defined by bit code 01) are used to control devices' access to the wireless medium. Request-To-Send (RTS), Clear-To-Send (CTS), and Acknowledgement (ACK) transmissions are examples of CTRL frames.
- **MGMT -** Management frames (defined by bit code 00) carry information relating to transactions between wireless devices (such as authentications, supported speeds, etc.). Management frames include association requests, beacons, and probe responses, among others.

After a frame's type is established, it is then categorized into a subtype, defined by four bits following its type bit code (for example, a Probe Request frame uses the subtype bit code of 0100). Not all possible four-bit options are actually used in the 802.11 specification, but those that are not actively used are considered "reserved", and as such should never show up in wireless traffic. Frames detected utilizing a reserved subtype may indicate a misconfigured device or a wireless attacker attempting to remain undetected.

Due to the fact that they directly impact network activity, it is important that MGMT and CTRL frames utilize the appropriate subtypes as defined by the 802.11 specification. Frames using reserved subtypes can cause reduced throughput due to excess frames in the air, and at worst could potentially trigger malfunctions in some network devices.

AirMagnet Solution

Devices transmitting MGMT or CTRL frames using reserved subtypes may indicate a defect or mistake in the device's configuration. Such devices could cause the corporate network to be considered non-compliant with certain regional regulations. Consequently, it is important that the device be reconfigured to meet with 802.11 standard specifications.

EAP TLS Bad Packet

Alarm Description & Possible Causes

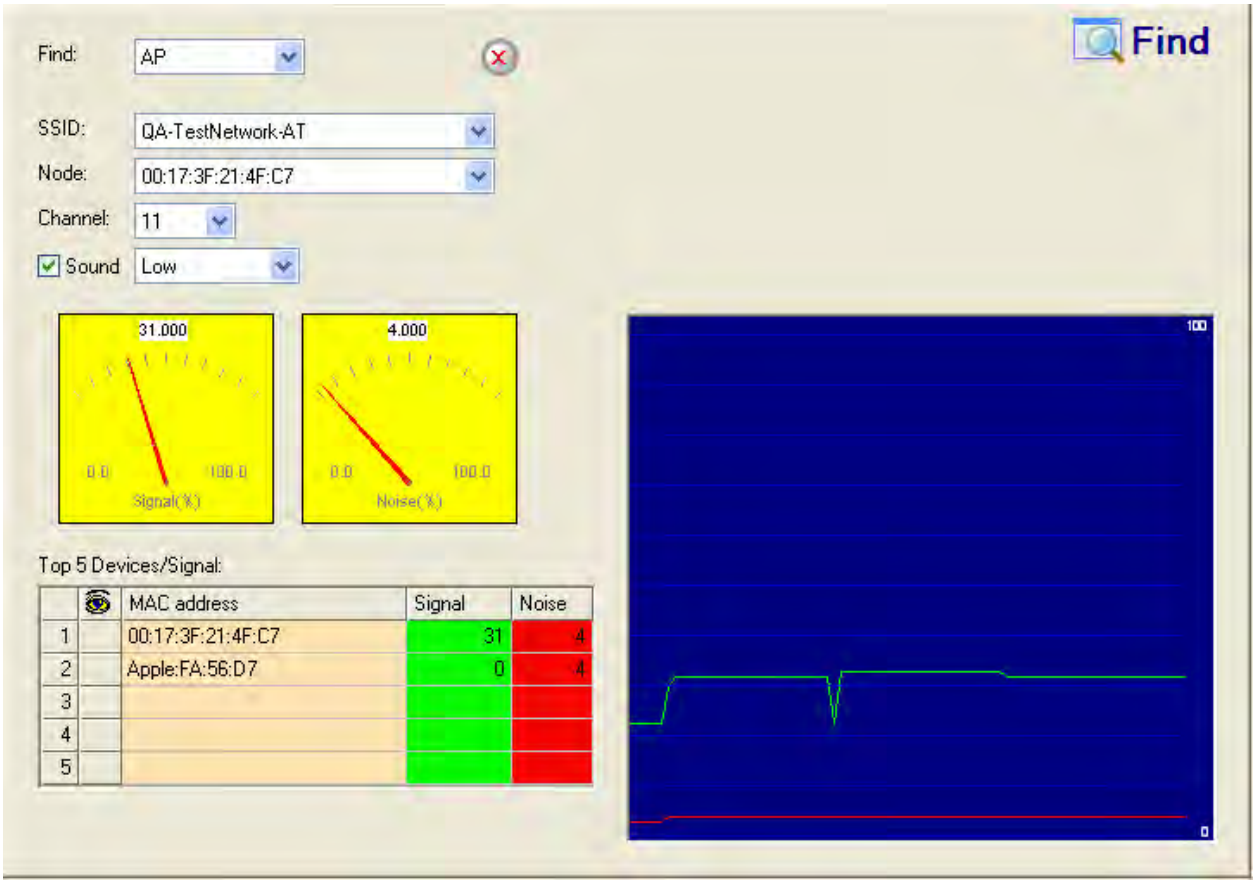
The Extensible Authentication Protocol (EAP) is a basic security framework that improves the encryption of 802.11 transactions. This framework can be paired with a wide variety of different authentication mechanisms, including a version known Transport Layer Security (TLS), a certificate-based protocol. The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis. This means that every active connection to an AP utilizing EAP-TLS authentication creates a new shared key specific to that connection, which makes the protocol significantly stronger than standard shared-key mechanisms against wireless attackers.

Each EAP frame contains a packet header that is composed of three basic flags: code, identifier, and length. Wireless attackers can spoof EAP packets in which these flags are manipulated to conduct several types of wireless penetration attempts, including one which can cause certain models of APs to crash when utilizing EAP-TLS authentication. An attacker

can take advantage of this vulnerability by transmitting defective frames to a corporate AP. By sending EAP-TLS packets with the identifier flag set to 'c0' and no defined TLS message length or data, APs from some vendors can be rendered inoperable until they are rebooted. During the reboot, attackers may have an opportunity to gain access to the corporate network, resulting in a security leak.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors EAP-TLS transmissions and triggers an alarm if defective or invalid frames are detected. Although this issue may not always represent a wireless attack, it is an issue that should be remedied in order to maintain the health of the wireless deployment. It is recommended that system administrators use the Find tool to track down the source of the offending frames and determine the root cause of the problem.



HT-Intolerant Degradation of Service

Alarm Description & Possible Causes

The introduction of the 802.11n wireless standard provides enterprises utilizing wireless communications with the potential for increased wireless range and speed over previous legacy (802.11a/b/g) implementations. This is due, in part, to the fact that 802.11n devices

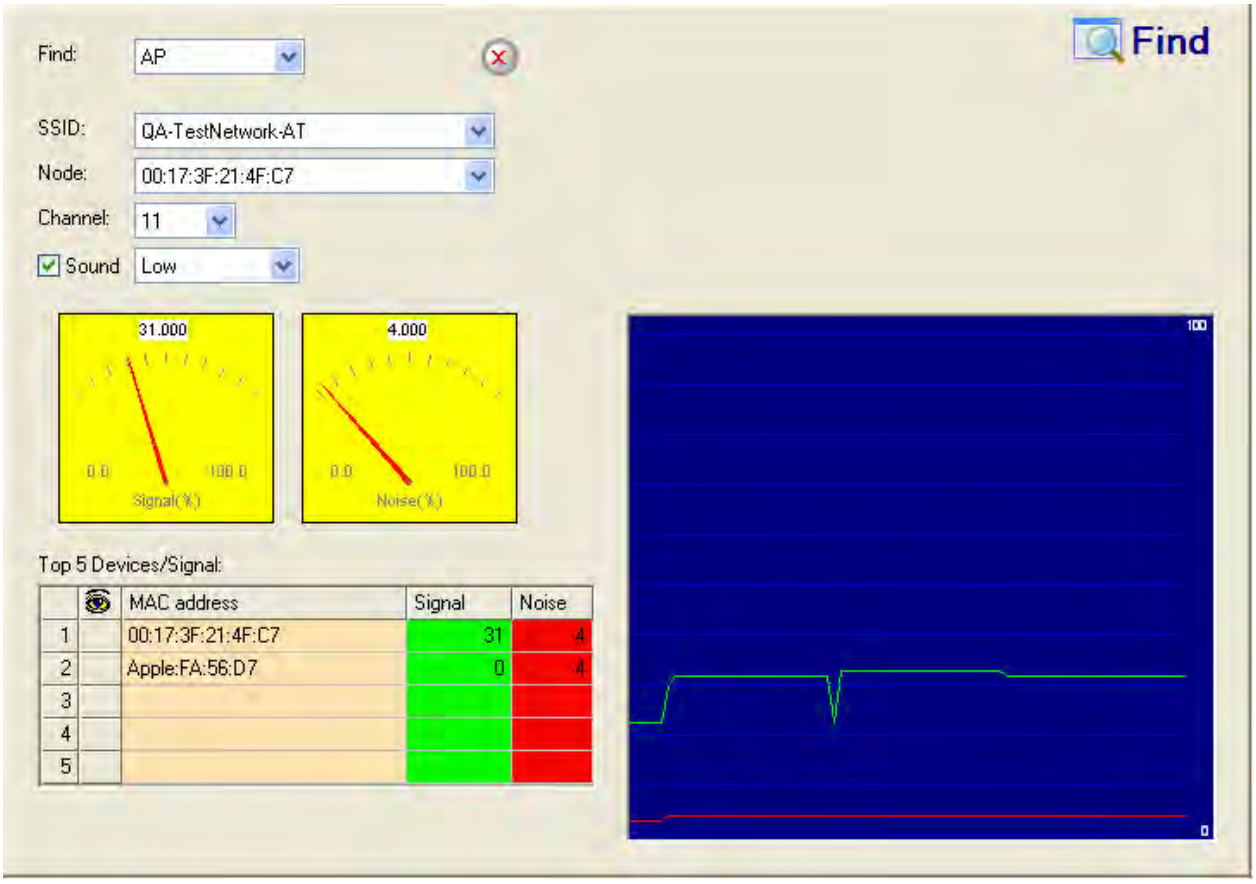
are capable of transmitting over a much wider channel frequency (40 MHz) than prior standards, which utilized 20 MHz channel widths.

However, in order to ensure proper backwards-compatibility with the legacy devices present in most wireless deployments, the 802.11n standard provides a mechanism for devices to specify whether they are utilizing 20 or 40 MHz channels. In a standard association request frame (which is transmitted any time a device attempts to associate with an AP), a device can transmit an "HT intolerant" flag that will cause the AP to revert to standard 20 MHz mode. While this allows the device to conduct wireless transactions with the AP, this switch forces the AP to remain in 20 MHz mode for at least 30 minutes (the 30 minute interval is reset every time an "HT intolerant" flag is received). During this time, devices that are capable of operating on the 802.11n-specific 40 MHz channels will also be forced into 20 MHz mode while associated to the AP. This eliminates the increased speed that is one of the primary benefits of 802.11n deployments.

Wireless attackers can take advantage of the "HT intolerant" flag by submitting an association request frame to an 802.11n AP, thereby forcing the AP to reduce its channel width (and consequently its maximum transmit speed). Note that the attacker **does not have to successfully associate to the AP**; the submission of the association request itself is enough to degrade service for all devices associated to the AP under attack.

AirMagnet Solution

It is important to ensure that legacy devices are either eliminated from an 802.11n deployment or associated with other legacy APs within the installation. Although this alarm doesn't necessarily indicate a wireless attack (as it may simply be due to a valid legacy device in the environment), the reduction in speed can impair overall network performance. In the case of a valid device causing the problem, it is recommended that IT personnel locate the problematic device and configure it to associate with other legacy devices. The Find tool can help users track down the source of the legacy frames to reach a quick resolution.



Denial-of-Service Attack: Block ACK

Alarm Description & Possible Causes

In legacy (pre-802.11n) deployments, devices are required to send an ACK frame for every frame received, resulting in a large percentage of traffic to be network overhead. This inefficiency was addressed in the 802.11n specification, which provides a new frame type called a Block ACK frame. The Block ACK mechanism allows an AP to acknowledge blocks of multiple frames with a single ACK, thereby reducing unnecessary network overhead.

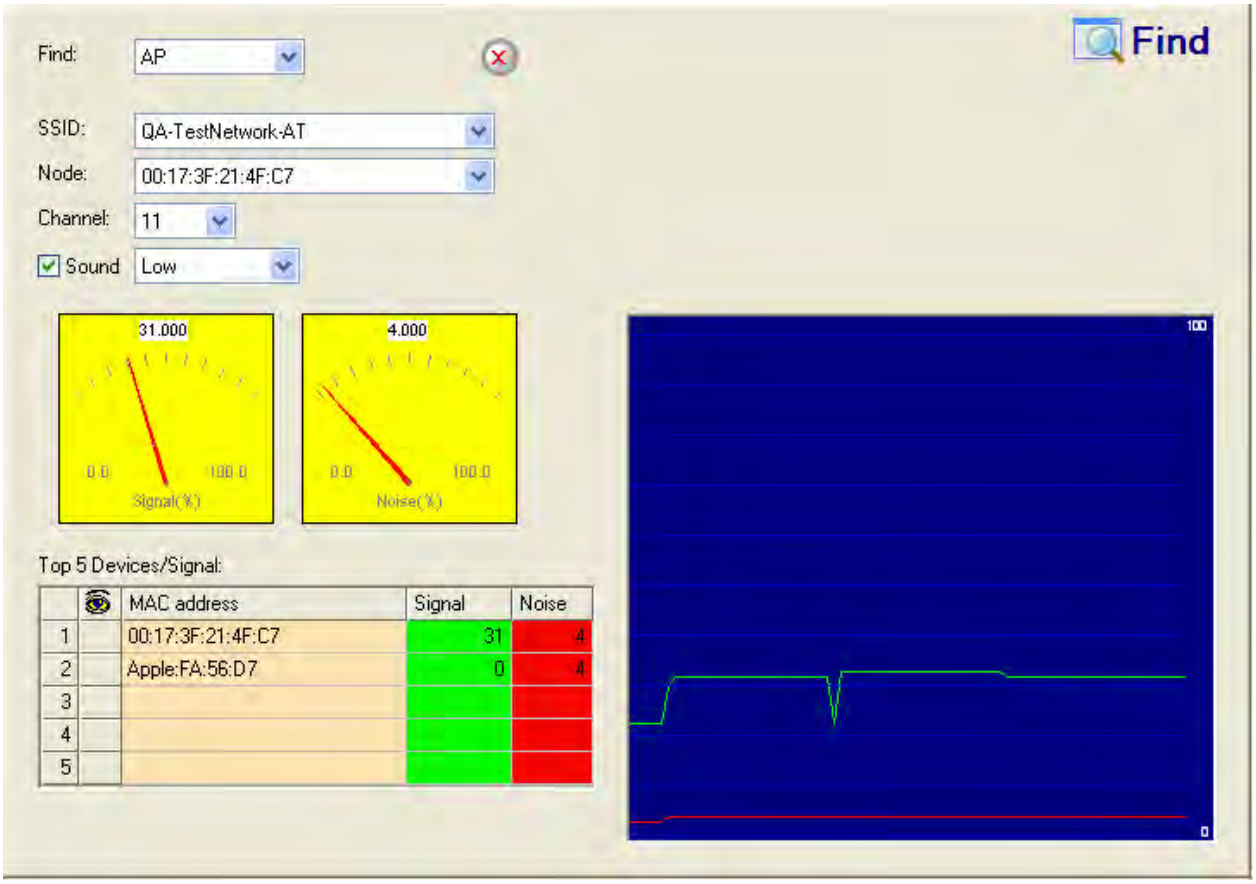
A form of Denial of Service attack which takes advantage of this process allows an attacker to prevent an 802.11n AP from receiving frames from a valid corporate client. To initiate a Block ACK exchange, the client sends an Add Block Acknowledgement (ADDBA) to the AP. The ADDBA frame contains sequence numbers to inform the AP of the size of the block being transmitted. The AP will then accept all frames that fall within the specified sequence (consequently dropping any frames that fall outside of the range) and transmit a BlockACK message back to the client when the transaction has been completed.

To exploit this process, an attacker can transmit an invalid ADDBA frame while spoofing a valid client's MAC address. Upon receipt of this message, the AP will remain closed to all traffic outside of the range specified by the (spoofed) ADDBA frame, thereby closing the AP

to communication from the actual valid client. This process will cause the AP to continuously ignore any traffic transmitted from the client until the invalid frame range has been satisfied, allowing the attacker to block the client for an indefinite period of time.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors ADDBA transactions for signs of spoofed client information. When an attacker is detected attempting to initiate a Block ACK attack, an alarm is triggered identifying the MAC addresses for both the attacker and victim devices. Use the Find tool to locate the attacking device and disable the attack or otherwise remove it from the wireless environment.



Although devices taking advantage of the ADDBA feature to initiate attacks can be eliminated on a case-by-case basis if necessary, the only sure way to truly eliminate the threat is to disable the ADDBA mechanism on the APs used in the wireless environment. Consult the AP vendor's documentation for the necessary configuration instructions.

AP PHY Data Rate Changed

Alarm Description & Possible Causes

An AP's data rate refers to the speed at which the device transmits data in the wireless environment. In most installations, the data rate in use is the maximum value available for the media type used by the majority of devices in the deployment (that is, 802.11a/g devices generally have a maximum rate of 54 Mbps; 802.11n devices have a maximum rate of 600 Mbps). This value is advertised in beacons and probe responses transmitted by each AP.

Some enterprise-grade AP vendors allow users to manually specify the data rates at which an AP can transmit. This configuration can be useful for ensuring that the rates in use do not drop below a specified threshold. By restricting the rates available to an AP, users can also prevent older "legacy" devices (such as those utilizing 802.11b technology) from associating with non-legacy corporate APs. As legacy connections can force APs to transmit at a lower rate for all devices, a single 802.11b connection can adversely affect every device associated to that same AP.

In deployments that make use of data rate specification, unauthorized changes to the supported rates can result in reduced throughput and reliability of the wireless network.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the list of rates supported by enterprise APs by comparing beacons and probe responses to ensure that no changes have been made. If alterations are detected, an AP Data Rate Changed alarm is triggered to notify IT personnel of the problem.

Unauthorized or unexpected changes to enterprise AP configurations may indicate a potential security breach. It is recommended that users identify the cause of the changes as soon as possible and restore the configuration on the AP to meet with corporate standards.

AP PHY Data Rate Anomaly

Alarm Description & Possible Causes

An AP's data rate refers to the speed at which the device transmits data in the wireless environment. In most installations, the data rate in use is the maximum value available for the media type used by the majority of devices in the deployment (that is, 802.11a/g devices generally have a maximum speed of 54 MBps). This speed value is advertised in beacons and probe responses transmitted by each AP.

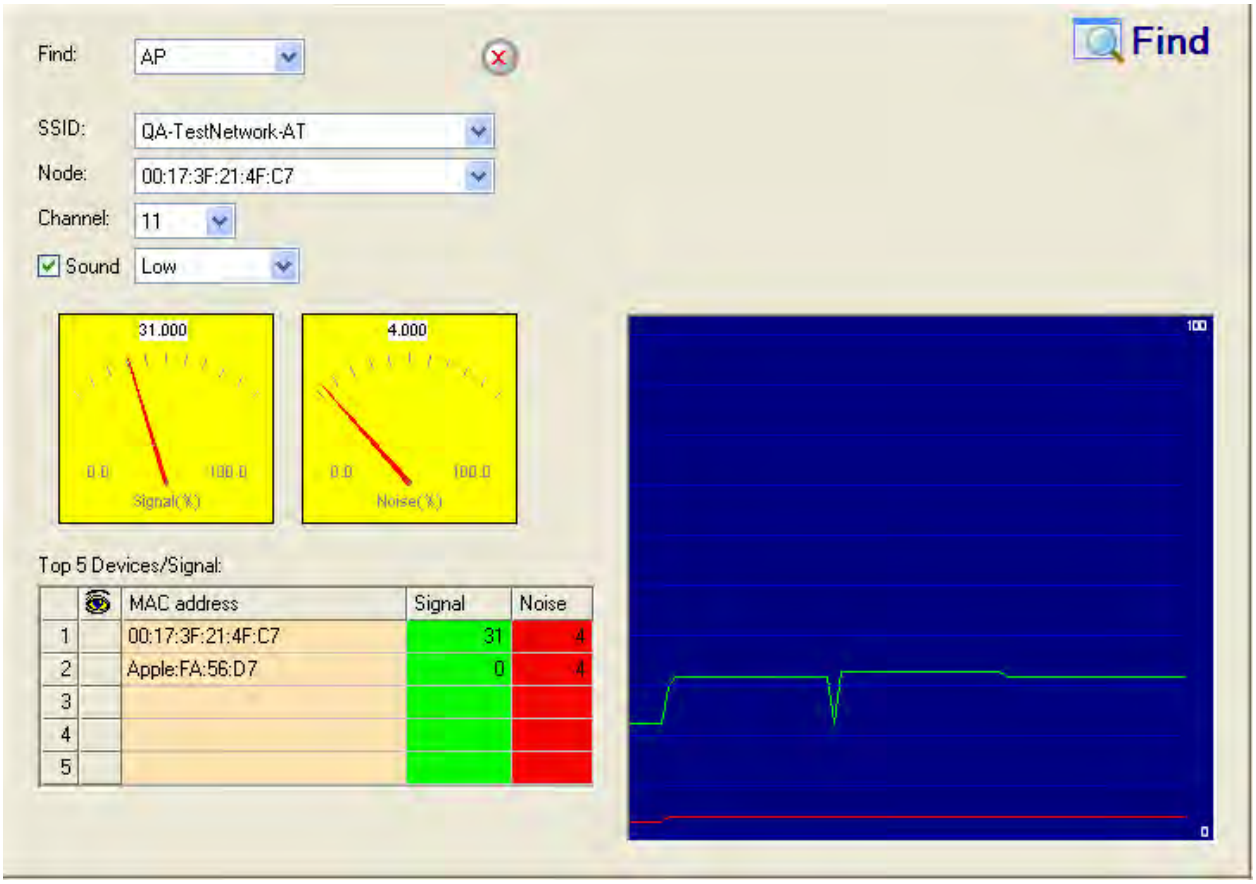
Some enterprise-grade AP vendors allow users to manually specify the data rates at which an AP can transmit. This configuration can be useful for ensuring that the rates in use do not drop below a specified threshold. By restricting the rates available to an AP, users can also prevent older "legacy" devices (such as those utilizing 802.11b technology) from associating with corporate APs. As legacy connections can force APs to transmit at a lower rate for all devices, a single 802.11b connection can adversely affect every device associated to that same AP.

In deployments that make use of data rate specification, unauthorized changes to the supported rates can result in reduced throughput and reliability of the wireless network.

Furthermore, in deployments that require the network to maintain adherence to a regulatory compliance standard (such as HIPAA, Sarbanes-Oxley, etc.), a single AP that does not comply with the specified regulation can result in the entire deployment violating corporate policy.

AirMagnet Solution

AirMagnet WiFi Analyzer allows the user to specify the supported data rates for all Known APs. If a device is detected transmitting at an unauthorized rate, an AP Data Rate Anomaly alarm is triggered. It is recommended that system administrators use the Find tool to locate the source device and eliminate it from the wireless network.



Additionally, users should determine whether any recognized corporate wireless clients had associated to the rogue AP, as these stations may have transmitted confidential data over the unsecured device.

Device Unprotected by EAP-TLS

Alarm Description & Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known Transport Layer Security (TLS), a certificate-based protocol. The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis. This means that every active connection to an AP utilizing EAP-TLS authentication creates a new shared key specific to that connection. This makes the protocol significantly stronger than standard shared-key mechanisms against wireless attackers.

Devices configured to use the EAP protocol but not the TLS authentication mechanism can represent potential insecure connections to the wireless network. There are a number of alternative mechanisms that may be used (such as EAP-TTLS or EAP-FAST) which generally provide greater convenience than EAP-TLS at the cost of reduced security for the network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data as a result. EAP exchanges that are not secured by TLS authentication can be easier for attackers to intercept and decode, potentially resulting in sensitive data sent from a valid user being leaked.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors EAP transactions to detect any devices that are not implementing the TLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the EAP-TLS mechanism.

Denial-of-Service Attack: Probe Request Flood

Alarm Description & Possible Causes

When attempting to associate to a wireless AP, a station must first transmit a probe request frame to determine the capabilities of any wireless devices in the environment. In a standard deployment, an AP that receives a probe request will transmit a probe response frame containing various data (such as data rates supported by the AP, authentication requirements, etc.), after which the station may proceed with an association request.

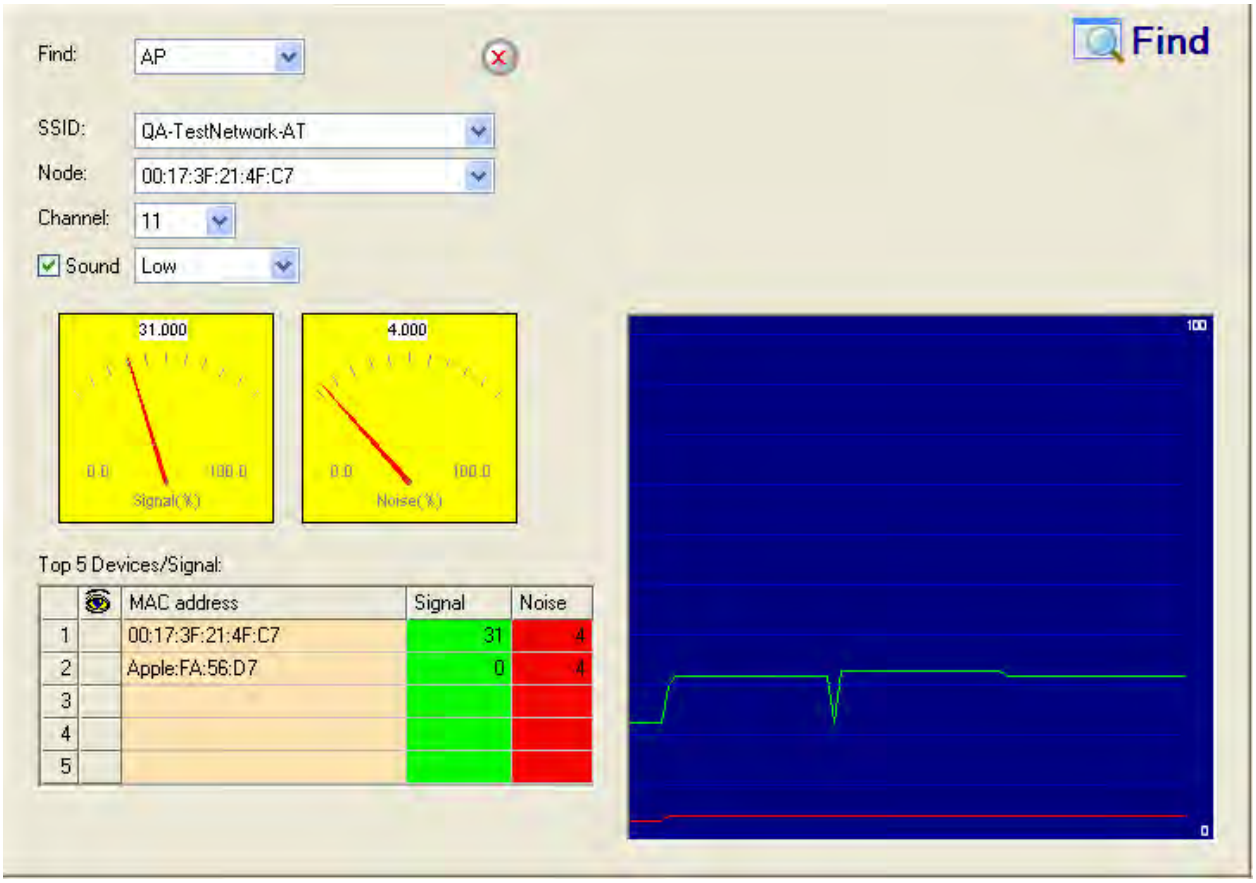
This procedure represents a potential vulnerability in 802.11 transactions that may be exploited in a wireless attack. In any deployment, if an AP receives a probe request frame, it automatically replies with a probe response frame. Consequently, if enough probe requests are transmitted to an AP, it can be blocked from servicing other clients due to the sheer volume of probe responses required.

A form of Denial of Service attack allows the attacker to force the target AP into a constant stream of probe responses intended to serve nonexistent clients. During a probe request flood, the attacker generates large quantities of probe requests sent from a series of "spoofed" MAC addresses targeted at a specific AP. As a result, the AP will be stuck

continuously responding to the false requests, thus resulting in a denial of service for all clients depending on that AP for wireless service.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the levels of probe request frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. The alarm description provided on the AirWISE screen will include either the MAC address of the station transmitting the probe requests or the address of the AP under attack. It is recommended that system administrators use the Infrastructure screen to observe the number of probe request frames detected and identify their source. Even in cases where the requests are from valid stations, the volume of management traffic active on the network can result in reduced throughput and speed for valid users. IT personnel should use the Find tool to locate the device running the attack and remove it from the deployment.



Note that attackers will often spoof the MAC address of a valid station already present in the deployment. In such a case, the valid station should be shut down so that its signal does not interfere with the detection of the attacker.

Denial-of-Service Attack: Probe Response Flood

Alarm Description & Possible Causes

When attempting to associate to a wireless AP, a station must first transmit a probe request frame to determine the capabilities of any wireless devices in the environment. In a standard deployment, an AP that receives a probe request will transmit a probe response frame containing various data (such as data rates supported by the AP, authentication requirements, etc.), after which the station may proceed with an association request.

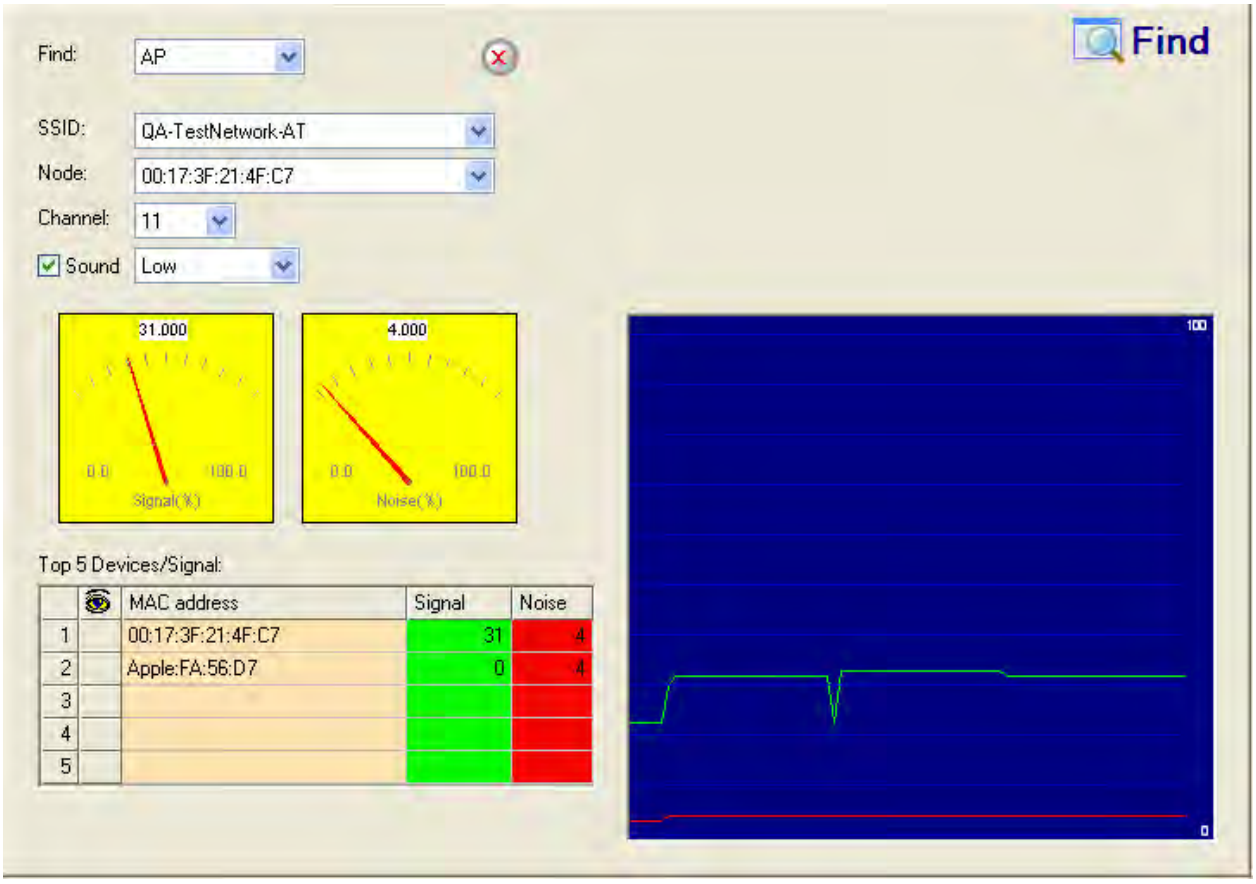
This procedure represents a potential vulnerability in 802.11 transactions that may be exploited in a wireless attack. A form of Denial of Service attack allows the attacker to prevent the target station from receiving any valid probe response frames from APs in the enterprise deployment. During a probe response flood, the attacker generates large quantities of probe responses sent from a series of "spoofed" MAC addresses targeted at a specific station. As a result, the station will be unable to identify valid probe responses sent from corporate APs while it processes the flood of spoofed frames. This initiates a denial of service in that the station experiences a delay or inability to associate to the corporate network.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the levels of probe response frames transmitted to stations in the wireless deployment and will trigger an alarm if two criteria are met:

- The number of probe response frames transmitted to a given station exceeds the specified threshold, and
- The target station has not transmitted a probe request frame signifying that it is seeking information about available APs.

Even in cases where the responses are valid, the volume of the frames could cause problems with wireless activity, including reduced throughput and missed frames due to heavy management traffic. Consequently, the attacking device should be located using the Find tool and removed from the enterprise environment.



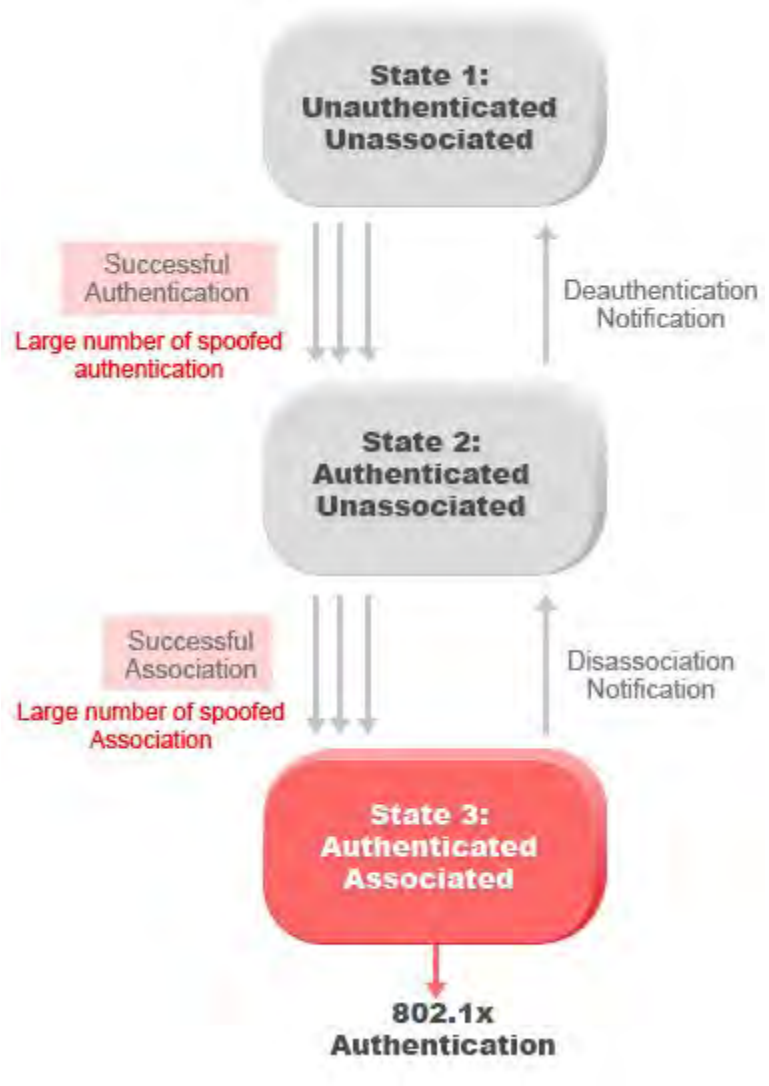
Denial-of-Service Attack: Re-Association Request Flood

Alarm Description & Possible Causes

In order to initiate a standard 802.11 connection, a station in the wireless deployment transmits an association request frame to its target AP. After the appropriate authentication protocols have been exchanged, the connection is established and the station can access the network. If the station roams outside of the initial AP's signal coverage, it will attempt to re-establish the connection with another AP on the same network. To do so, the station transmits a re-association request frame. This frame signals to the second AP that the station is ready to receive any frames that had been buffered during the roaming period.

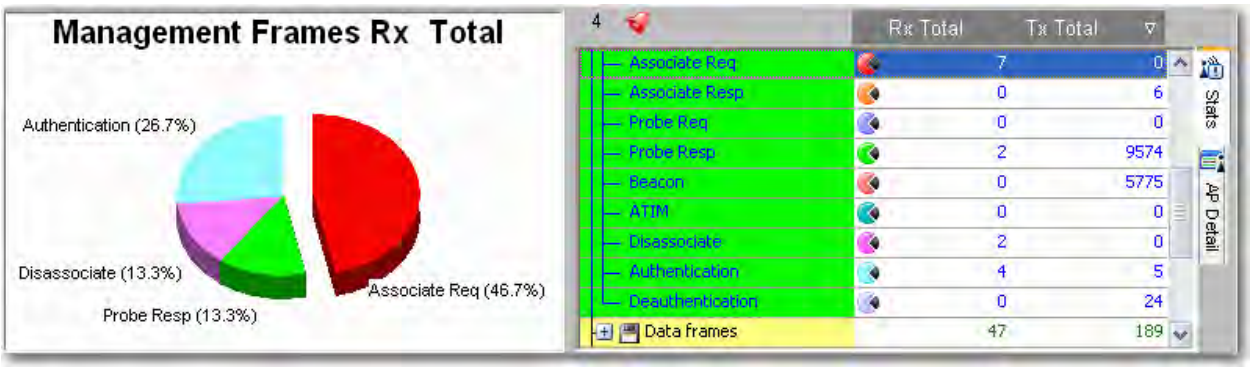
During the period of authentication (before the station has been cleared to associate), the AP stores the client's information in its client association table. This table is a buffer designed to allow the AP to process association (or re-association) requests in the order in which they are received. Although this process is effective in most deployments, it represents a potential vulnerability due to the fact that an AP's association table can be filled up with pending client association requests. In this case, the AP will be unable to service new users until the pending requests are cleared out.

A form of Denial-of-Service attack is to exhaust the AP's resources, particularly the client association table, by flooding the AP with a large number of spoofed client re-associations. An attacker can flood an AP's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients will not be able to associate, thus initiating an attack.

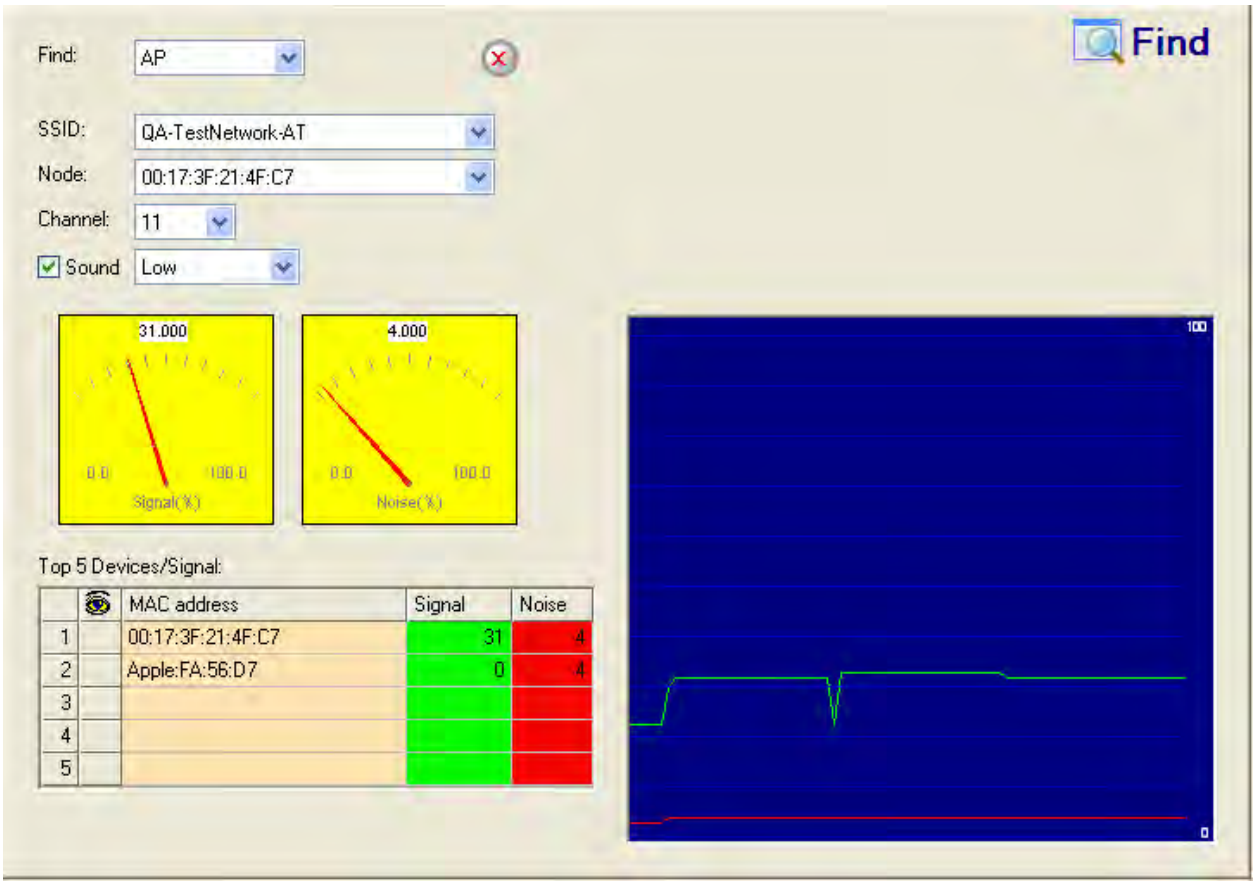


AirMagnet Solution

AirMagnet WiFi Analyzer monitors the levels of re-association request frames in the wireless environment and will trigger an alarm if the threshold for such frames is exceeded. You can view these frames by using the Infrastructure screen.



After identifying the source of the excessive frames, it is recommended that users track down the offending device using the Find tool and remove it from the enterprise deployment.



Rogue AP by MAC Address (ACL)

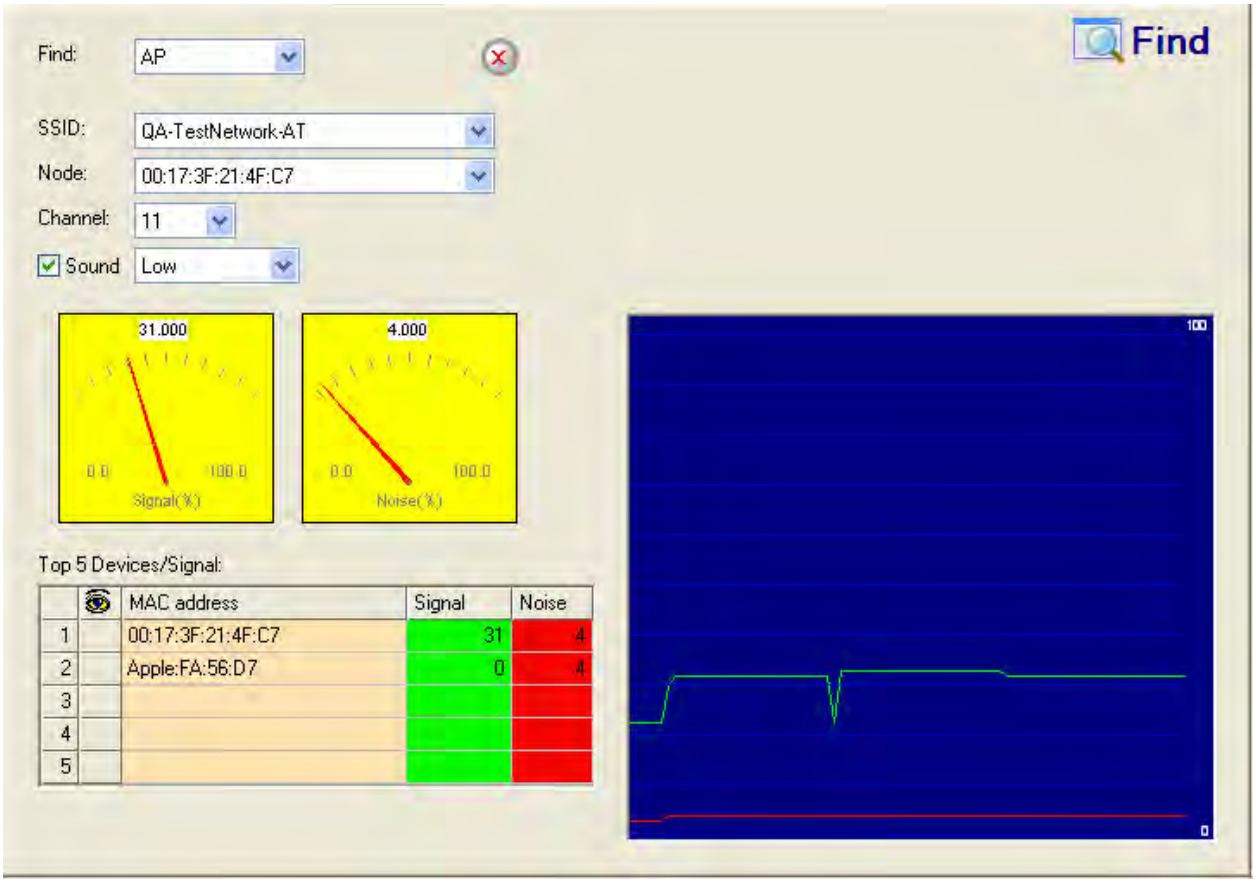
Alarm Description & Possible Causes

After configuring a list of MAC addresses of your authorized APs, AirMagnet Wi-Fi Analyzer can alert WLAN administrators on unauthorized (Rogue) APs whose MAC address falls out of the pre-configured address list. The authorized MAC address list can be imported to AirMagnet Enterprise from a file (*AccessControl.txt*). This file is common for APs, Infrastructure stations and Ad-hoc stations. It can also be auto-generated by requesting the AirMagnet Enterprise product to accept all or a specific subset of existing APs discovered by the AirMagnet SmartEdge Sensors.

Rogue APs installed by unauthorized employees usually do not follow enterprise standard deployment practices and may compromise security on both the wireless and the wired network. The Rogue AP alarm may also indicate malicious intruders attempting to hack into the enterprise wired network. AirMagnet Wi-Fi Analyzer discovered rogue devices should be investigated carefully.

AirMagnet Solution

Once a Rogue AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue AP Using Corporate SSID

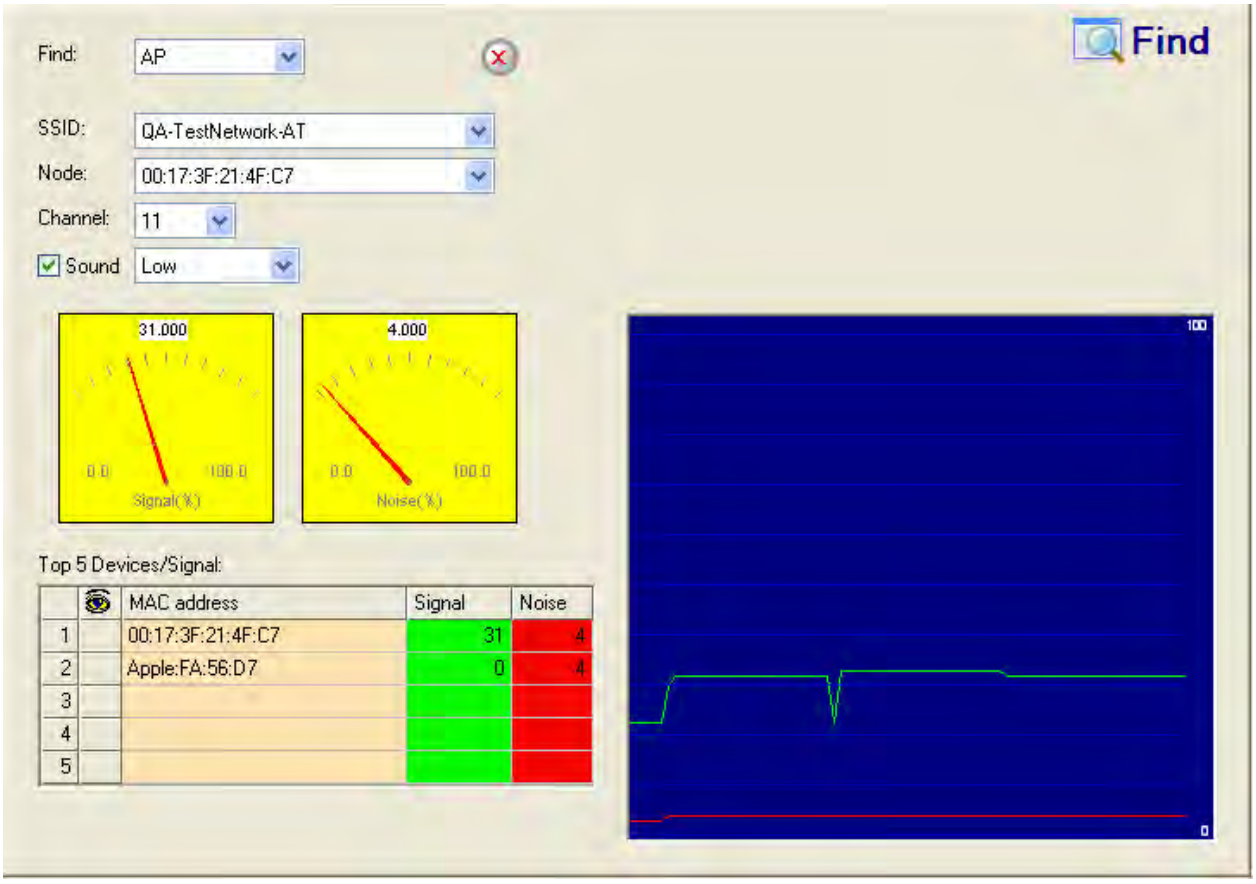
Alarm Description & Possible Causes

In most enterprise wireless deployments, multiple SSIDs may be used for various different groups of intended users of the network. For example, APs may be placed implementing one SSID for corporate users and another separate SSID for visitors or contract workers. Due to the variety of SSIDs that can be found in the deployments for corporate organizations, it is important that users be able to monitor the environment to ensure that any unidentified or unauthorized SSIDs are detected and removed before wireless security is breached.

In order to avoid detection, wireless attackers can configure a rogue AP to use an SSID that is known and valid in the corporate environment. This can present a security risk when the rogue AP does not implement the authentication mechanisms required by corporate policy. This poses a hazard in that since the AP is utilizing a valid corporate SSID, it may trick valid stations in the deployment into associating with it, allowing the attacker to monitor any traffic transmitted through the insecure connections.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors for the SSIDs defined in the MyWLAN SSID group and triggers an alarm when an unknown or rogue AP is discovered using a corporate SSID. Due to the potentially extreme nature of the security risk, users are advised to locate the rogue AP using the Find tool and ensure that it is a valid device.



Rogue AP Operating in Greenfield Mode

Alarm Description & Possible Causes

The 802.11n specification provides users with the ability to set 802.11n APs to utilize Greenfield mode, which ensures that only devices capable of supporting 802.11n speeds can associate to the wireless network. This mechanism can be used to prevent speed loss due to legacy (for example, 802.11a/b/g) devices in the wireless environment. Devices with Greenfield mode enabled use a new frame preamble, which cannot be decoded by legacy devices. By associating only with 802.11n-capable devices, APs operating in Greenfield mode can maintain transmit speeds of up to 300 Mbps. Conversely, if legacy devices associate, this speed drops to a maximum of 54 Mbps.

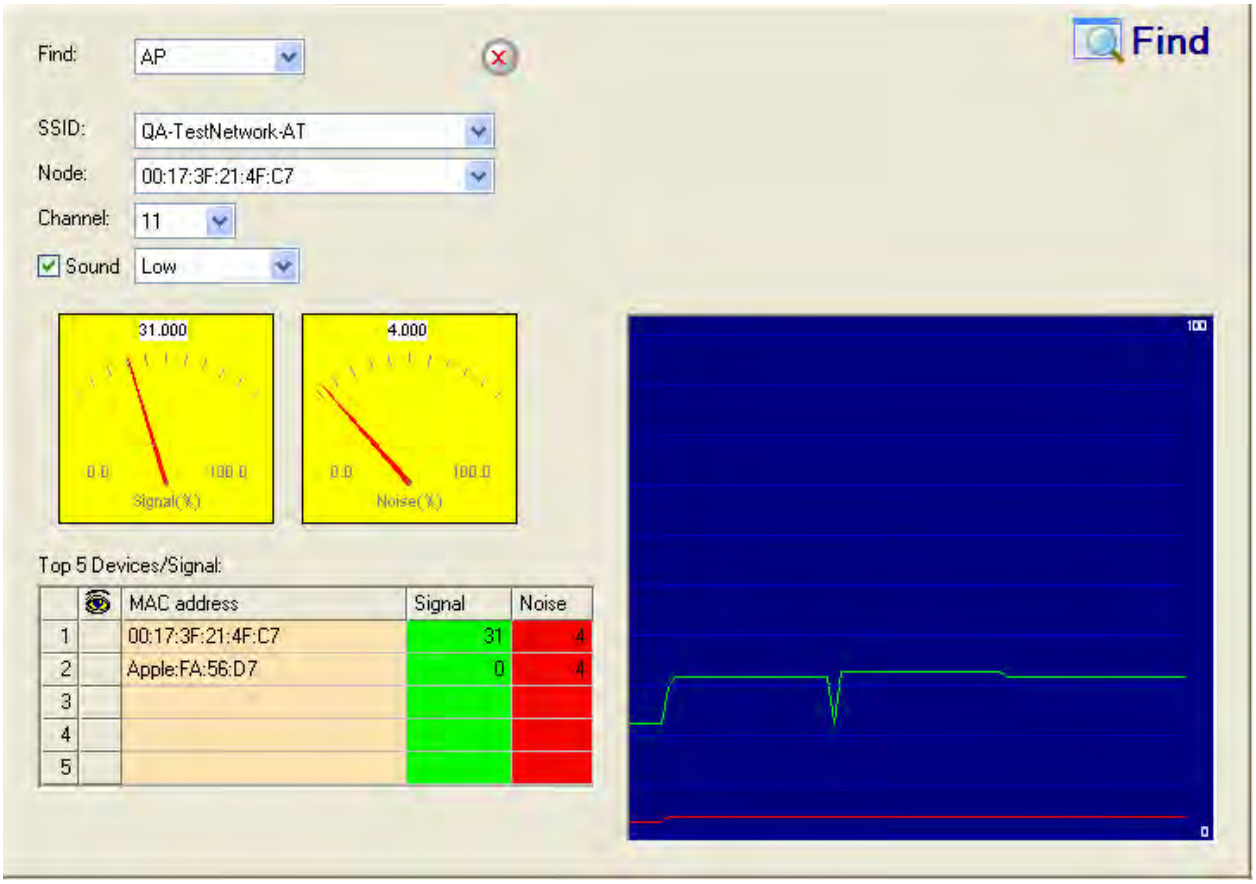
The preamble used by Greenfield devices presents a potential vulnerability in networks that do not use 802.11n-capable intrusion detection/prevention systems. Since legacy devices are unable to decode the new preamble, wireless deployments protected by systems monitoring for 802.11a/b/g traffic cannot detect devices operating in Greenfield mode.

To exploit this vulnerability, a wireless attacker can configure a rogue AP to utilize pure Greenfield mode and deploy it within a network that is protected by legacy intrusion detection devices. The rogue AP will be invisible to the protection system present, allowing

the attacker to lure valid 802.11n-capable clients into associating to the rogue AP. This may provide the attacker with access to any confidential information transmitted from the valid clients.

AirMagnet Solution

Wireless networks protected by legacy devices are unable to detect Greenfield devices. In order to protect against these attacks, users must upgrade the intrusion detection infrastructure present and deploy devices that are capable of monitoring 802.11n traffic. When a rogue AP is detected operating in Greenfield mode, use the Find tool to locate the rogue device and remove it from the network.

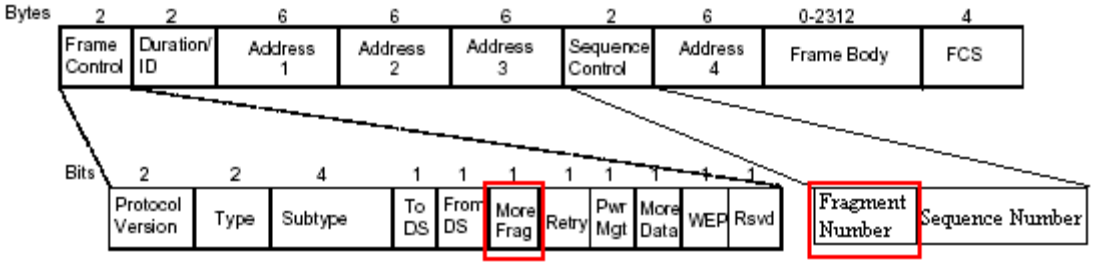


Small Fragmented Frames Detected

Alarm Description & Possible Causes

The 802.11 MAC layer supports frame fragmentation and defragmentation. The process of partitioning an 802.11 frame into smaller frames for transmission is called "fragmentation", which helps to increase reliability and reduce transmit errors. This is accomplished by increasing the probability of successful transmission of the smaller and fragmented frames in cases where channel characteristics limit reception reliability for longer frames.

Fragmentation is accomplished at each immediate transmitter before the actual start of transmission. The process of recombining fragmented frames into the original unfragmented longer frame is defined as "defragmentation". The IEEE 802.11 standard defines the packet format to identify fragmented frames for defragmentation (illustrated below).



While frame fragmentation can provide benefits, such as increased reliability and reduced error potential in network transmissions, these advantages can come at the cost of overall network throughput if not properly moderated. A network transmitting large numbers of small frame fragments could indicate that users have set the frame fragmentation threshold too low, resulting in small manageable frames being fragmented in addition to the larger ones. Since this process ultimately results in more packets being transmitted overall, the network's performance may suffer as a result.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks the fragmentation statistics and alerts on abused fragmentation usage that could lead to degraded WLAN performance. The fragmentation threshold needs to be carefully set to balance the benefit and overhead. Typically, equipment vendors set the default fragmentation threshold to 1536.

Out of Order Fragmented Frames

Alarm Description & Possible Causes

The 802.11 MAC layer supports frame fragmentation and defragmentation. The process of partitioning an 802.11 frame into smaller frames for transmission is called "fragmentation", which helps to increase reliability and reduce transmit errors. This is accomplished by increasing the probability of successful transmission of the smaller and fragmented frames in cases where channel characteristics limit reception reliability for longer frames. Fragmentation is accomplished at each immediate transmitter before the actual start of transmission. The process of recombining fragmented frames into the original unfragmented longer frame is defined as "defragmentation". The IEEE 802.11 standard defines the packet format to identify fragmented frames for defragmentation (illustrated below).

As shown in the figure above, every frame fragment is assigned a Sequence Number, which determines the order in which the fragments were transmitted. If the frames are received out of order, the recipient device must transmit a retry frame so that the source device will re-send the data. While most wireless environments will experience a certain level of retry traffic, large quantities of retry frames can cause reduced throughput and may inhibit overall network performance.

AirMagnet Solution

AirMagnet WiFi Analyzer detects these retry frames and tracks them on a per device and per channel basis. See the illustration below:

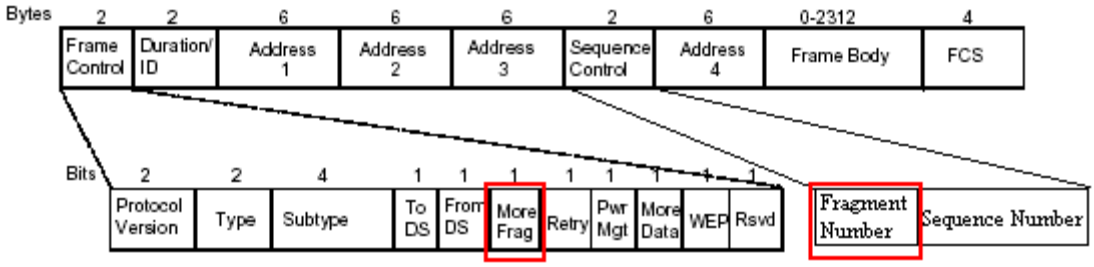
Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	46 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

High levels of retry frames can be caused by network interference, low wireless signal strength (due to insufficient infrastructure), or hidden nodes, among other causes. It is important that network administrators resolve the root cause of the retry frames in order to restore normal network functionality.

Incomplete or Invalid Fragmented Frames

Alarm Description & Possible Causes

The 802.11 MAC layer supports frame fragmentation and defragmentation. The process of partitioning an 802.11 frame into smaller frames for transmission is called "fragmentation", which helps to increase reliability and reduce transmit errors. This is accomplished by increasing the probability of successful transmission of the smaller and fragmented frames in cases where channel characteristics limit reception reliability for longer frames. Fragmentation is accomplished at each immediate transmitter before the actual start of transmission. The process of recombining fragmented frames into the original unfragmented longer frame is defined as "defragmentation". The IEEE 802.11 standard defines the packet format to identify fragmented frames for defragmentation (illustrated below).



If the frames received are incomplete or invalid, the recipient device must transmit a retry frame so that the source device will re-send the data. While most wireless environments will experience a certain level of retry traffic, large quantities of retry frames can cause reduced throughput and may inhibit overall network performance.

AirMagnet Solution

AirMagnet WiFi Analyzer detects these retry frames and tracks them on a per device and per channel basis. See the illustration below:

Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	46 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

High levels of retry frames can be caused by network interference, low wireless signal strength (due to insufficient infrastructure), or hidden nodes, among other causes. It is

important that network administrators resolve the root cause of the retry frames in order to restore normal network functionality.

Denial-of-Service Attack: Beacon Flood

Alarm Description & Possible Causes

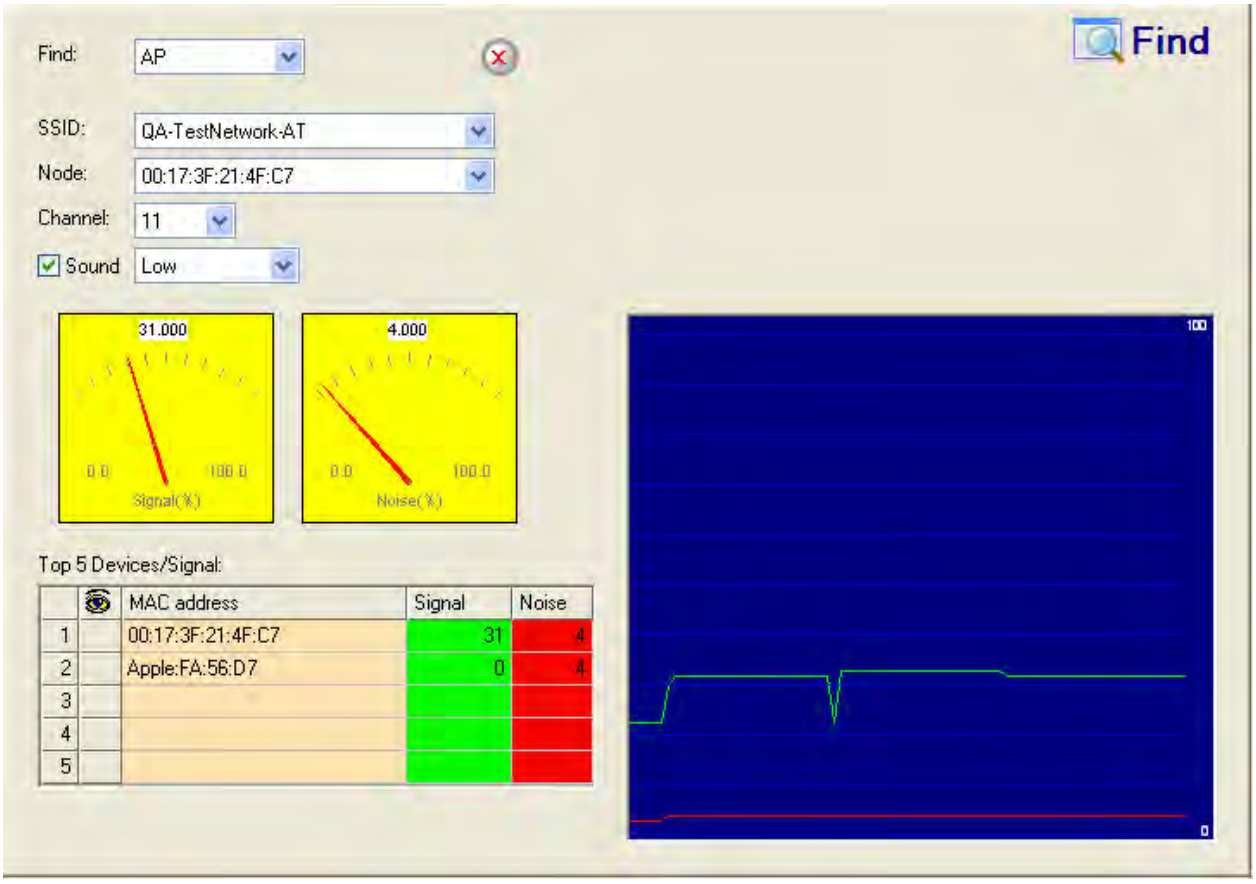
In a corporate wireless deployment, APs continually broadcast beacon frames in order to notify local devices of the configuration of the network. Beacons can contain a variety of data, including time stamp, SSID, authentication mechanism, and data rates supported by the AP. Upon receiving a beacon frame, stations can use the information provided to associate to the AP.

Before attempting to associate to the AP, wireless stations generally require a beacon frame in order to present the appropriate authentication credentials. This represents a potential vulnerability in that if a station cannot receive the desired beacon frame, it will be unable to connect. Due to the fact that all APs within a deployment will transmit beacon frames at regular intervals, stations may have difficulty collecting the appropriate beacon from within a particularly cluttered environment.

A wireless attacker can take advantage of this vulnerability to ensure that valid corporate stations cannot associate to the wireless network. To initiate a denial of service attack, the wireless intruder can flood the wireless airspace with random beacon frames that contain spoofed MAC address and SSID data. The volume of beacons in the air can prevent stations from receiving beacons from valid APs, thus denying stations wireless access.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the levels of beacon frames detected and will trigger a Beacon Flood alarm when the threshold is exceeded. Even in cases where the beacons are valid (due to a particularly dense AP deployment, for example), the volume of the frames could reduce overall network throughput. Consequently, the source(s) of the offending frames should be located using the Find tool, after which it can be removed from the enterprise environment.



Denial-of-Service Attack: MDK3 Destruction Attack

Alarm Description & Possible Causes

MDK3 is a suite of hacking tools that allows users to utilize a number of different security penetration methods against a target corporate AP. MDK3-Destruction mode is a specific implementation of the suite that uses an array of the tools to completely shut down the AP under attack. During an MDK3-Destruction attack, the tool simultaneously:

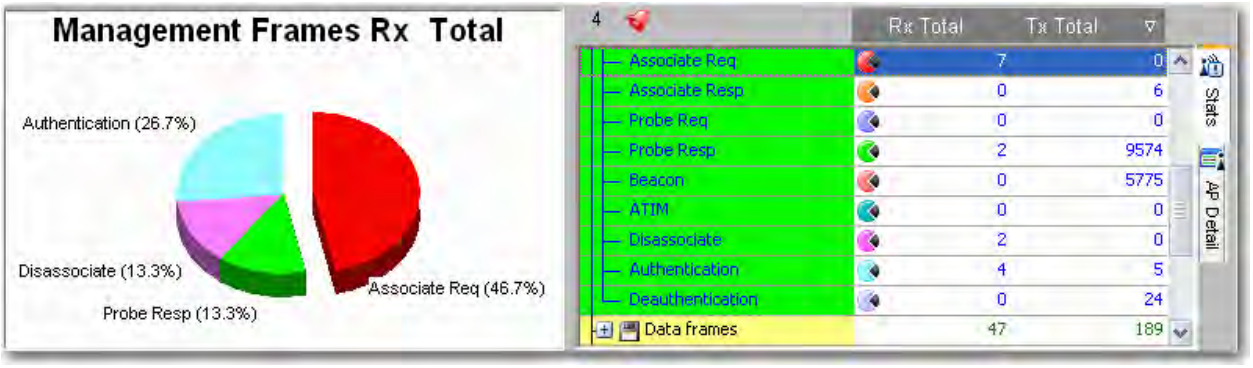
- Initiates a beacon flood attack, creating multiple fake APs within the environment,
- Triggers an authentication flood attack against the target AP, preventing it from servicing clients, and
- Starts a de-authentiation flood attack against the target AP, kicking all active connections from valid clients.

As long as the attack is in progress, users will be unable to access the target AP. Valid clients that have been disconnected due to the de-authentication flood portion of the attack may attempt to associate with the fake APs created, which could result in corporate data being sent to the attacker.

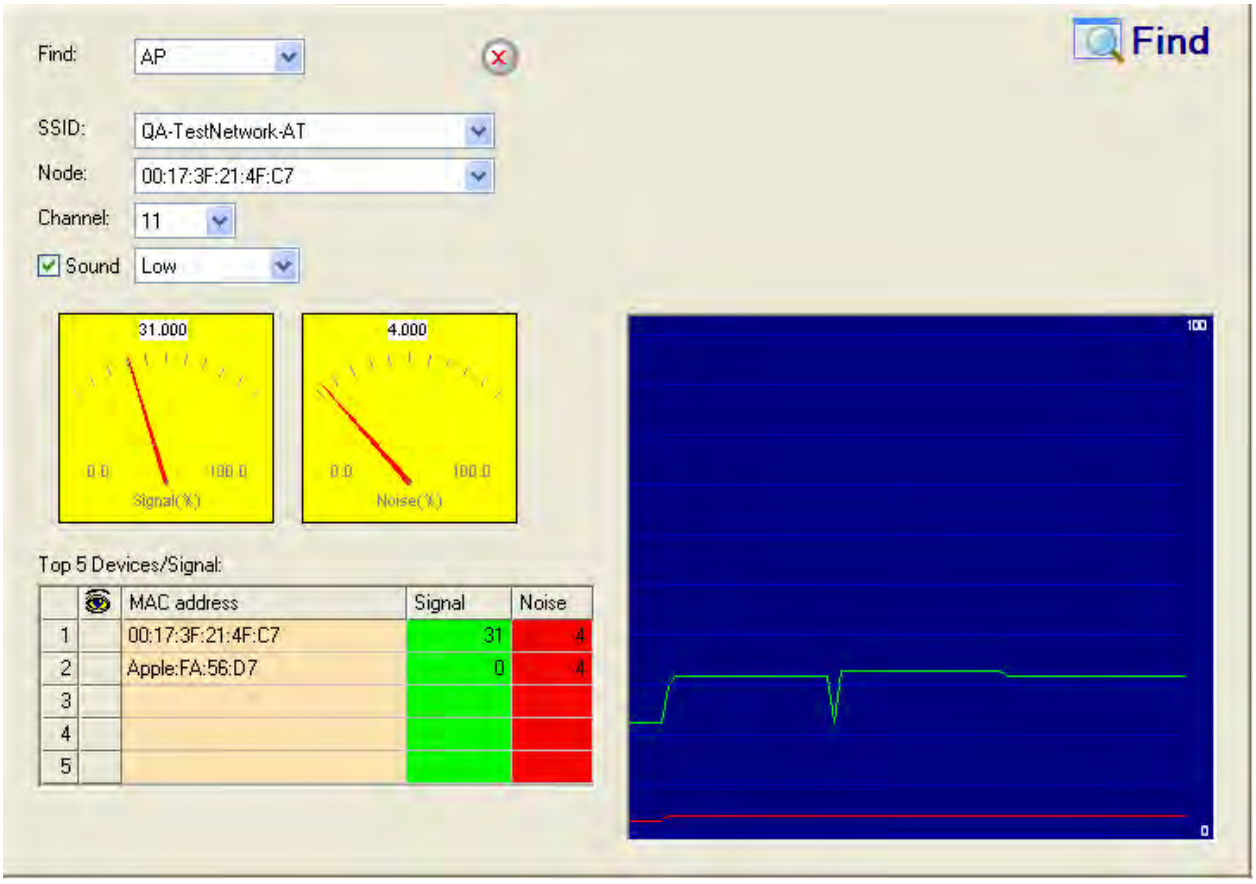
Due to the volume of traffic transmitted, the target AP may need to be rebooted after the attack has been stopped. For further details regarding the MDK3 tools, refer to http://homepages.tu-darmstadt.de/~p_larbig/wlan/.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors for the symptoms of an MDK3-Destruction attack and triggers an alarm when they are detected. Due to the dramatic impact that this attack can have on a wireless deployment, it is strongly recommended that the source of the attack be identified using the Infrastructure screen as soon as possible.



After the device has been identified, the Find tool can be used to locate the device. IT personnel should remove the device immediately before additional damage can be done. Additionally, in some deployments, the corporate APs affected may need to be rebooted in order to clear out their association tables before wireless activity can resume.



KARMA Tool Detected

Alarm Description & Possible Causes

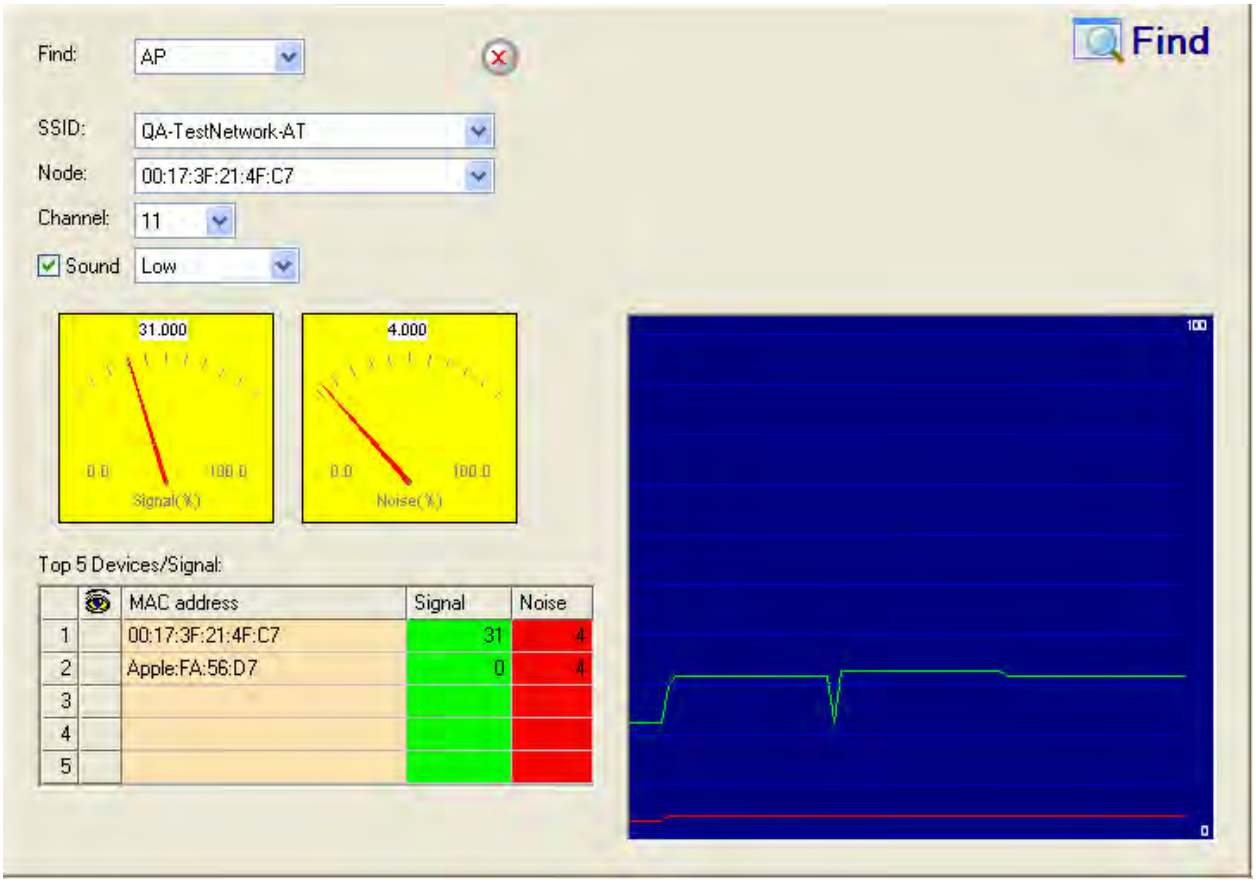
KARMA is a set of wireless tools designed to test the security of a wireless network. The basic implementation of the tool set allows the attacker to monitor for probe request frames transmitted by stations seeking known wireless SSIDs. The attacker can then generate a rogue AP using one of the SSIDs captured, which could result in a corporate station joining the AP automatically. More advanced attackers may take advantage of this connection to obtain corporate authentication credentials or attack the client station itself.

Updates to the KARMA tool suite streamline the attack process, allowing the user to configure a rogue AP that responds to any probe request frames detected. For example, if two clients are seeking two different SSIDs (for example, "home" for the first and "corporate" for the second), the rogue AP will respond as "home" and "corporate" to each, in turn. In this manner, the attacker can exploit connections from multiple clients in the deployment, rather than requiring that they associate one at a time. After the connection has been established, both users are at risk of transmitting confidential information through the attacking AP.

For additional information on KARMA, refer to http://blog.trailofbits.com/karma/.

AirMagnet Solution

In some deployments, IT personnel make use of the KARMA tools to ensure that corporate clients comply with the corporate wireless policies in place. If an unknown or rogue device is detected using the KARMA tools, users should locate the source of the frames using the Find tool and remove it from the wireless environment.



In order to ensure that the company's wireless clients are protected from such attacks, it is recommended that users configure their stations to connect to networks only upon request, rather than automatically. This will prevent the KARMA tools from capturing probe requests and easily emulating corporate APs.

Wi-FiTap Tool Detected

Alarm Description & Possible Causes

Wi-FiTap is a tool that allows an attacking station to communicate directly with a target client, without associating to the corporate wireless network. In avoiding the need to connect to an enterprise AP, the attacker effectively bypasses any security measures configured to protect the corporate network (such as Cisco PSPF). Upon successfully establishing a connection with a valid client, the Wi-FiTap utility can be modified to allow the

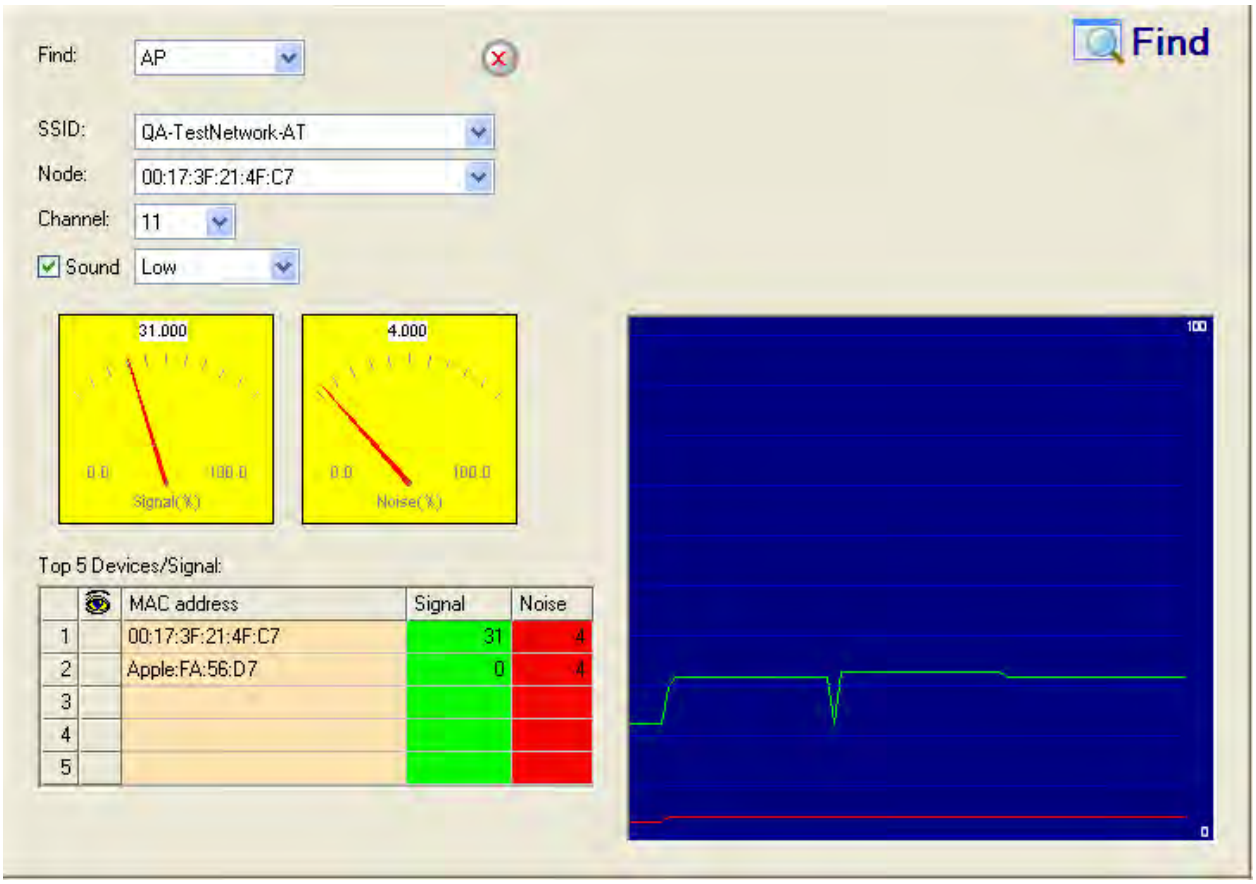
attacker to subsequently emulate a corporate AP, sending spoofed responses to transmissions captured from the target station. In this manner, the attacker can monitor traffic for critical or secure data, representing a security risk.

During a Wi-FiTap attack, the rogue station initially monitors the wireless airspace to determine the channel(s) on which corporate APs are transmitting. Upon identifying the AP and channel to be targeted, the attacker configures the Wi-FiTap tool to emulate the AP's BSSID (for example, MAC address) and sets the attacking machine's wireless card to emulate an AP. After obtaining a list of the valid AP's network clients (by using a utility such as Tcpdump or Ethereal), the attacker can then communicate directly with any of those clients while appearing to be the valid AP to which they are associated.

For additional information on the Wi-FiTap tool, refer to http://sid.rstack.org/index.php/Wi-Fitap_EN.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors wireless traffic for potential instances of the Wi-FiTap utility and notifies users if an attack is detected. It is recommended that security personnel identify the device and locate it using the Find tool. The attacking station should be removed from the wireless environment as soon as possible in order to prevent it from intercepting any confidential transmissions.

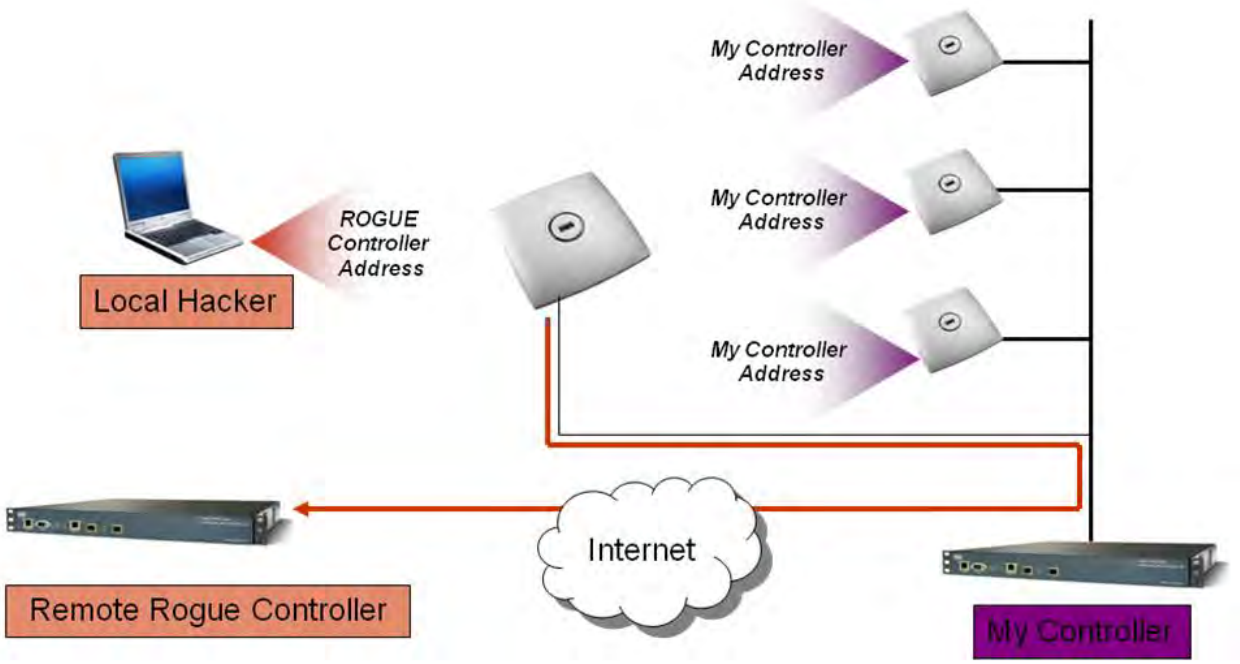


SkyJack Attack Detected

Alarm Description & Possible Causes

As the popularity of light-weight access points managed by centralized control systems grows, so does the demand for simple plug-and-play deployment and redundant failover of these access points and control systems. The corporate wireless network is becoming less of a luxury and more of a critical element of the network infrastructure, with its ease of deployment and redundancy configuration contributing to its growth in usage by IT teams wanting to provide employees network access quickly. Many wireless infrastructure vendors have met these industry demands allowing the light-weight access point to discover the control systems automatically. This helps the newly deployed access points find a control system for the first time and it helps the currently deployed access points fail over to backup control systems if their primary control system goes offline. The methods by which the access points find a control system include received information in a DHCP response, factory configured DNS entries, broadcasted discovery messages on their wired interfaces, and listening for specific frames from fellow, already configured infrastructure access points on their wireless interfaces. Unfortunately, it is this last method that has introduced a major security risk for companies using these light-weight access point centralized control system deployments.

The frames used to assist newly deployed or failing over access points are often unencrypted data frames sent from currently deployed access points, regardless of the encryption and authentication used by those currently deployed access points. This is necessary because the newly deployed or failing over access points may not have the correct encryption keys to decrypt the frames required for seamless deployment or failover. However, infrastructure access points that listen to, and act on the data in unencrypted wireless frames poses a major security threat. These frames can include IP addresses and MAC addresses of control systems, as well as other information for proper access point management. By spoofing these unencrypted frames and transmitting them into the uncontrolled wireless medium, an attacker could trick a newly deployed or failing over access point to connect to a control system of their choosing, including a system in an external location under their control. Once the infrastructure access point is connected to the attackers control system, the access point is in effect SkyJacked and the attacker could force the access point to operate in any manner they choose. The attacker could exploit the open wireless connection to gain access to the corporate wired network or attempt to obtain user login information from corporate clients attempting to attach to the SkyJacked access point.



AirMagnet Solution

AirMagnet WiFi Analyzer alerts the user on wireless traffic patterns that match signatures for potential SkyJack attack attempts. If the alert is raised, users should closely monitor their infrastructure access points and control systems to verify their operation state is expected. Further protection against SkyJack attacks includes disabling deployment and failover assistance over the wireless medium.

Rogue Station by MAC Address (ACL)

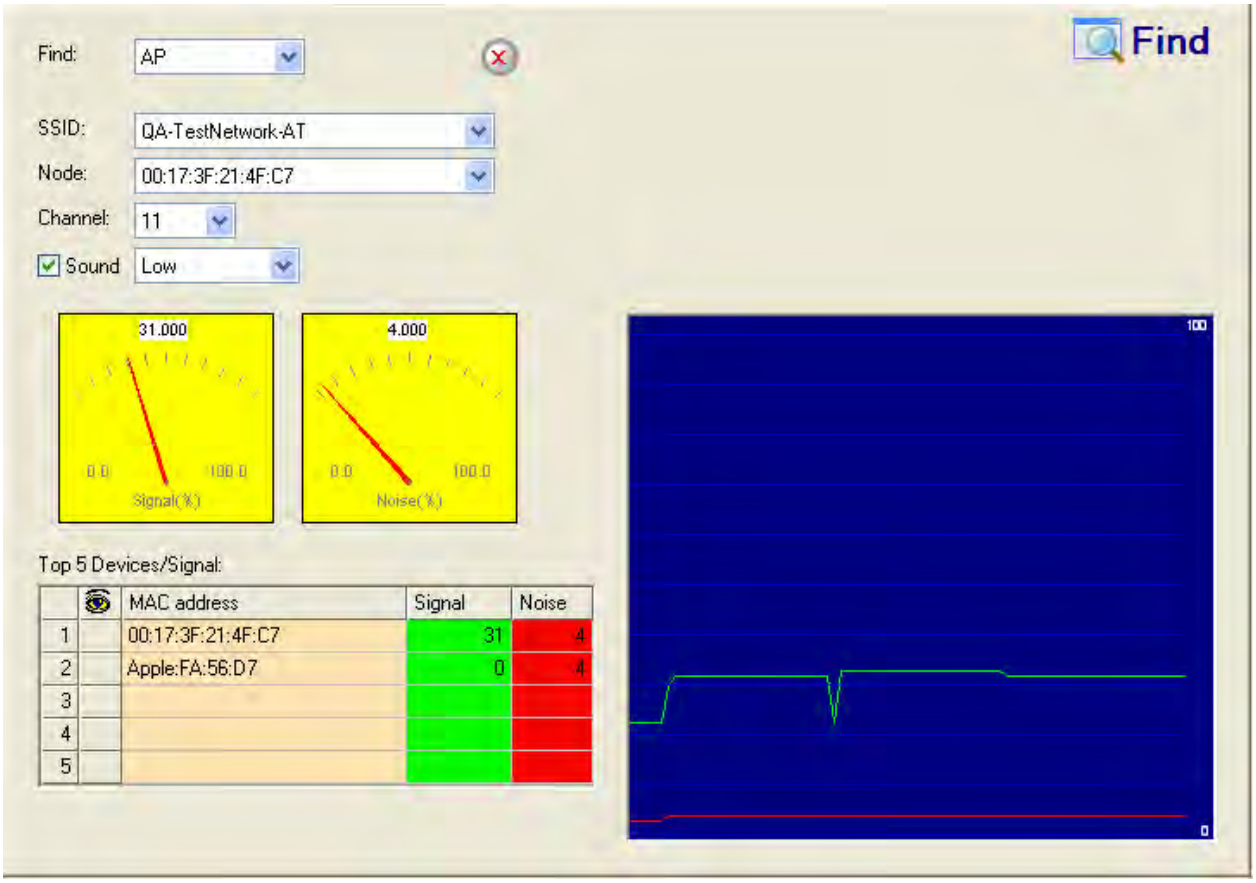
Alarm Description & Possible Causes

After configuring a list of MAC addresses of your enterprise authorized client stations, AirMagnet Wi-Fi Analyzer can alert WLAN administrators on unauthorized stations (rogue stations) whose MAC address falls out of the pre-configured address list. The authorized MAC address list can be imported to AirMagnet Enterprise from a file (AccessControl.txt). This file is common for APs, Infrastructure stations and Ad-hoc stations. It can also be auto-generated by requesting the AirMagnet Enterprise product to accept all or a specific subset of existing APs discovered by the AirMagnet SmartEdge sensors.

Rogue stations installed by unauthorized employees usually do not follow enterprise standard deployment practices and may compromise security on both the wireless and the wired network. The Rogue station alarm may also indicate malicious intruders attempting to hack into the enterprise wired network. AirMagnet Wi-Fi Analyzer discovered rogue devices should be investigated carefully.

AirMagnet Solution

Once a Rogue station is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.

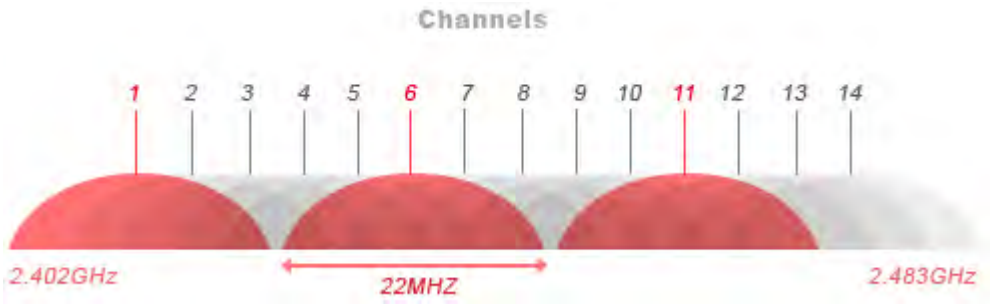


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Interfering APs Detected

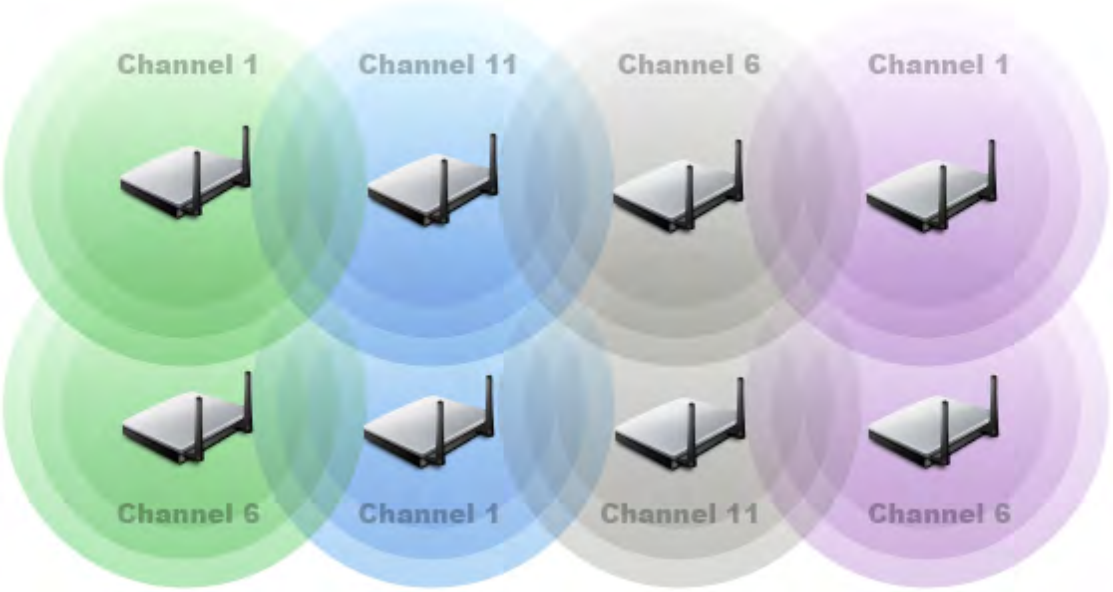
Alarm Description & Possible Causes

802.11b and 11g devices operate in the RF frequency range of 2.4GHz. A total of 14 channels are defined by the IEEE standard in this frequency range with each channel occupying 22 MHz. Adjacent channels overlap with each other in RF frequency usage (see illustration below).



802.11b and 11g Channel Allocation and Frequency Overlaps

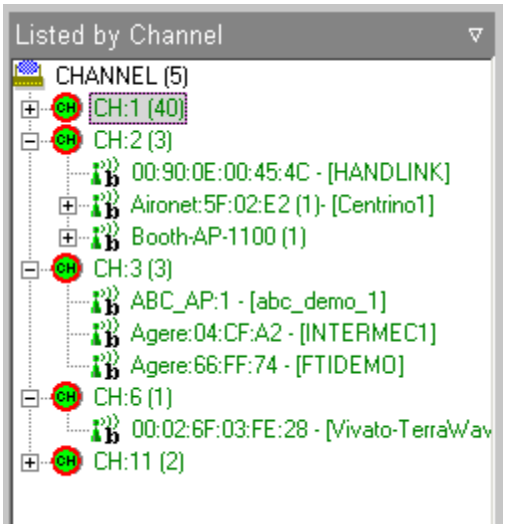
Wireless devices operating in adjacent channels (channel numbers less than 5 apart) have their RF frequencies overlapped and will interfere with one another. Ideally, APs should be 5 channels apart to avoid such a problem. See the sample channel allocation and AP deployment below.



Site Survey Allocates Non-overlapping Channels to Physically Adjacent APs

AirMagnet Solution

AirMagnet WiFi Analyzer analyzes channel allocation and usage to detect their mutual interference and the alarm is generated when a channel frequency is overlapped by more than the tolerable number (the user configurable alarm threshold) of APs. For example, if AirMagnet WiFi Analyzer detects 5 APs operating in channel 1, 2, 3, 4, 5, and 6 individually, it would generate this alarm to indicate these APs all interfere with each other and exceeded the default threshold of 3 APs with overlapping frequency usage. Most experts advise the use of channels 1, 6 and 11, while some recommend the use of only channels 1 and 11. The user can use the AirMagnet Infrastructure view to further investigate current channel usage and take counter measures.



Infrastructure View (List by Channel) showing channel allocation

Policy - Mismatched SSID

A certain client is configured with a SSID which doesn't match any of the available SSID in this wireless LAN

Policy - Client with match-all SSID

A certain client is configured with a match-all SSID (null string or ANY) which not be accepted by any AP in this wireless LAN since they only accept specific SSIDs

Policy - Mismatched RF channel

A certain RF channel does not have any clients, instead has APs with matching SSID , which could be caused by mis-configuration of the clients

Policy - Mismatched privacy setting

A certain clients and APs cannot get associated because of the mismatched WEP encryption configuration

Conflicting AP Configuration

Alarm Description & Possible Causes

One of the ways for AirMagnet WiFi Analyzer to validate a configuration policy is to check the configuration consistency from APs supporting the same SSID. Large corporations will have huge wireless implementations with more than one AP providing the wireless service. In order to provide effective roaming capabilities for clients it is important that the APs with similar SSIDs have similar configurations. Configuration parameters such as the following should have the same settings across APs under the same SSID:

- Authentication and encryption (static WEP, TKIP, and so on)
- Performance options (short/long preamble)
- SSID broadcasting

Inconsistent settings among APs may result in inconsistent security enforcement or inconsistent client connectivity experience.

AirMagnet Solution

AirMagnet WiFi Analyzer identifies APs with a nonconforming configuration for the WLAN administrator to correct. Take appropriate steps to ensure consistent configurations throughout the wireless environment. This will include ensuring the same encryption setting and preamble options.

Policy - Authentication failure

Authentication failure

Policy - (Re)Association failure

(Re)Association failure

Policy - Possible equipment failure

Possible equipment failure

AP Using Non-Standard SSID

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator on in-ACL Access Points that are not using Standard SSID's. For example, if your deployed WLAN is configured only with MyOfficeWlan and MyVoIPWlan, you would then include these two SSIDs in the authorized SSID Group list. After this list is imported, AirMagnet WiFi Analyzer raises an "AP Using Non-standard SSID" alarm when an AP marked in-ACL and operating with a different SSID is discovered. Sudden changes in the SSID for the APs could indicate that an unauthorized person has gained access to the APs and has made those changes. Any changes in the SSID may cause network interruption for your clients as they no longer detect the original SSID that is configured within their client utility or Windows zero-config.

AirMagnet Solution

AirMagnet WiFi Analyzer also alerts the user to any sudden changes in the SSID of in-ACL access points. This may indicate that an intruder has control over the access point and has modified the SSID configuration. This can cause all valid clients to get disconnected from the AP as they now are not talking on the same network or may be compromising the security of the network. Please connect to the AP that has the configuration change and assign a stronger password for the access point login and change the SSID back to the original one to continue providing service to the clients.

Policy - AP signal out of range

AP signal out of range.

Policy - Mismatched capability settings

Mismatched capability settings.

Policy - Device with bad WEP key

Device with bad WEP key.

Channel With High Noise Level

Alarm Description & Possible Causes

The emergence of wireless technologies means that multiple, diverse wireless devices will be operating in close proximity. In the 2.4GHz unlicensed frequency range, 802.11b and 11g devices are not the only wireless equipment in operation. Other technologies including Bluetooth, 2.4 GHz cordless phones, wireless surveillance cameras, microwave ovens, baby monitors used in hospitals, and so on, can all interfere with the WLAN, resulting in an increased **BER** (bit error rate), leading to reduced coverage and degraded performance. At the 5GHz frequency range where 802.11a operates, regulatory rules have been more restrictive in favor of WLAN data communication networks; the existence of noise is present, but not as prevalent as the 2.4GHz spectrum, and thus it experiences less interference problems.

Noise Level	Impact to Indoor Operating Range	Impact to Outdoor Operating Range
0 dB	*0%*	*0%*
3 dB	*19%*	*30%*
5 dB	*30%*	*44%*
10 dB	*50%*	*68%*

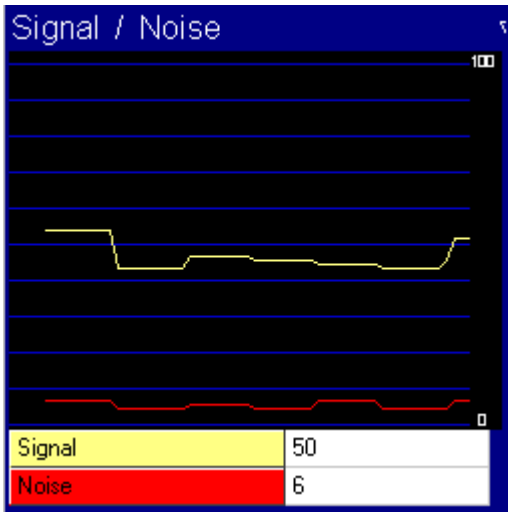
RF Noise Impact to Wireless Device Operating Range

AirMagnet Solution

AirMagnet WiFi Analyzer cannot differentiate the sources of interference (without additional assistance; see below) as Bluetooth, microwave, phones, and so on and their presence appear in the form of RF channel noise to AirMagnet WiFi Analyzer. By tracking the noise level for each channel, AirMagnet WiFi Analyzer raises this alarm against the channel that has a sustained high noise level. To further identify the source of channel noise, a directional antenna can be used to track down and approach the source by following the noise level. Once the source is located, it is should be dealt with immediately.

If you purchase AirMagnet Spectrum Analyzer and integrate it with AirMagnet WiFi Analyzer, you now have a more powerful tool that can identify these additional sources of interference. By enabling the Spectrum Analyzer integration function, you can use the RF Interference page to identify which channels are experiencing interference from non-802.11 sources. You may then use the Find tool to track these devices down and remedy the problem.

If the equipment causing problems is owned by the company, this can be an easy fix, but if it belongs to a neighboring company, remedying the situation can be more difficult. This stresses the importance of an effective site survey to study the environment before the deployment process to achieve the best results for the corporate WLAN.



Channel Noise Level available on the Remote Analyzer

Excessive Multicast/Broadcast on Channel

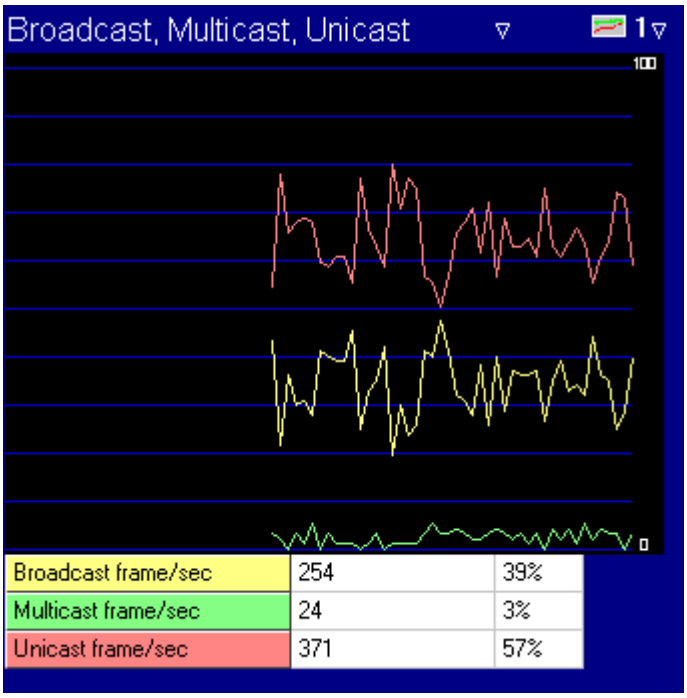
Alarm Description & Possible Causes

Just like in a wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices connected. What makes the WLAN more sensitive to these frames is the fact that all multicast and broadcast frames are transmitted at low speed (for example, 1 or 2 Mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth.

Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process, thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 Mbps, which is a considerable delay for a voice application.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel. To further investigate this multicast and broadcast situation, the Channel or Infrastructure views can be used to display the corresponding statistics, as illustrated below.



Multicast and Broadcast Frames To Raise Alarms on Abused Usage

Spoofed MAC Address Detected

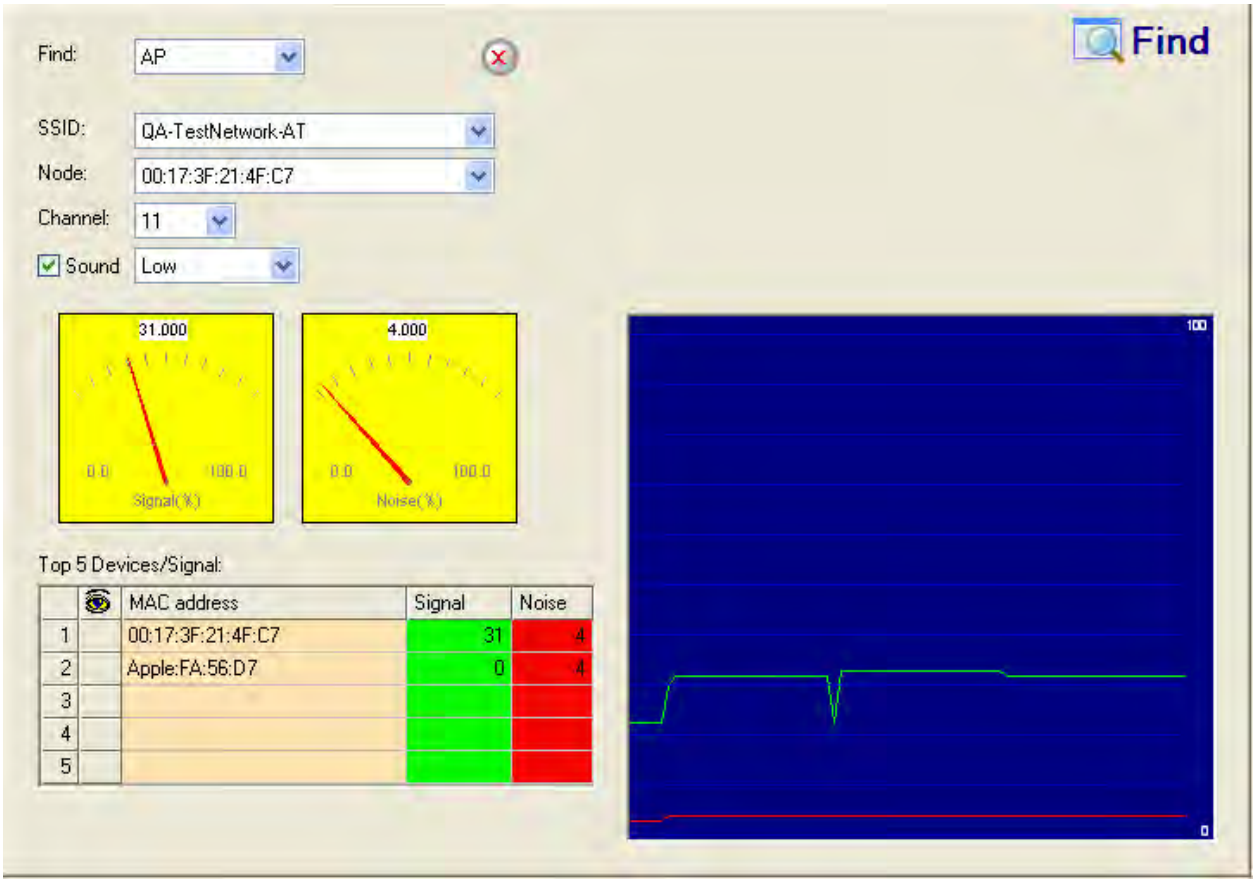
Spoofing tools: SMAC, macchanger, SirMACsAlot, Gentle MAC Pro

Alarm Description & Possible Causes

A wireless intruder wishing to disrupt the wireless network has a wide range of attack tools to choose from. Most of these tools (which are available free for download on the Internet) rely on a spoofed MAC address, causing the intruder's device to masquerade as an authorized wireless Access Point or client. Using these tools, an attacker can launch various denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

AirMagnet Solution

AirMagnet WiFi Analyzer detects a spoofed MAC address by following the IEEE authorized OUI (vendor ID) and 802.11 frame sequence number signature. An administrator or the wireless security analyst can use AirMagnet WiFi Analyzer's Find tool to track down the intruding device by following the signal strength displayed on the screen, as illustrated below.



AirMagnet WiFi Analyzer's Find Tool used for locating an intruding device

Policy - Higher layer protocol problem

Higher layer protocol problem.

Denial-of-Service Attack: Association Table Overflow

Alarm Description & Possible Causes

Wireless intruders can exhaust AP resources, most importantly the client association table, by emulating a large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients would attempt association and authentication with the target AP. The 802.11 authentication would typically complete because most deployments use 802.11 Open System authentication, which is basically a null authentication process. Association with these emulated clients would then follow the authentication process. These emulated clients, however, would not follow up with higher level authentication such as 802.1x or VPN, thus leaving the protocol transaction half-finished. At this point, the Access Point under attack has maintained a state in the client association table for each emulated client. Once the AP's resources and client association table are filled up with these emulated clients and their state information, legitimate clients can no longer be serviced by the attacked AP - thus emulating a denial of service attack.

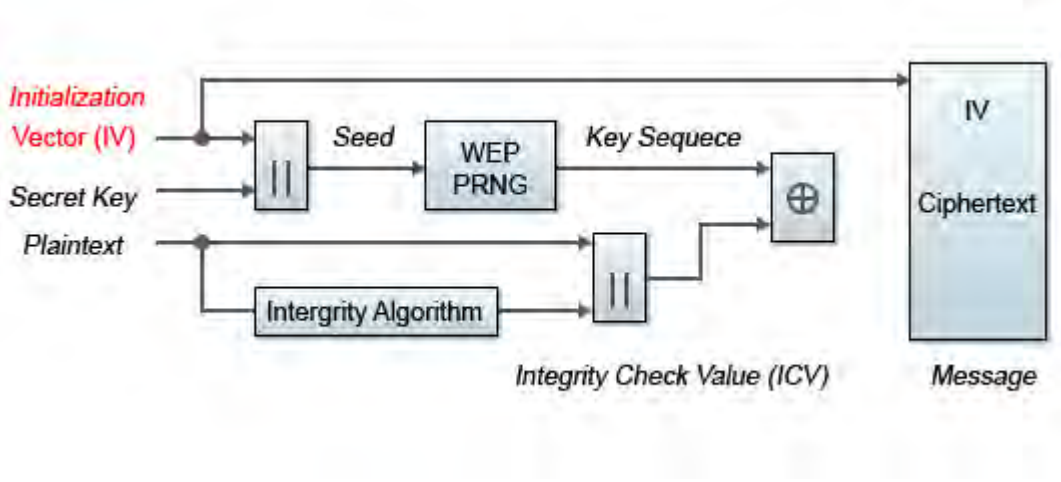
AirMagnet Solution

AirMagnet WiFi Analyzer tracks the client authentication process and identifies a DoS attack signature against an AP. Incomplete authentication and association transactions trigger the AirMagnet WiFi Analyzer attack detection and statistical signature matching process.

Crackable WEP IV Key Used

Alarm Description & Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir)*.



WEP Encipherment Block Diagram

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key, which is specified by the user, concatenated with the 24-bit IV (Initialization Vector), which is determined by the transmitting station. The IV can be reused frequently in consecutive frames, thus increasing the chance of the secret key being recovered by wireless intruders. By excluding certain IV values that would create so-called “weak keys,” the weakness of WEP as described in the above paper is avoided.

AirMagnet Solution

AirMagnet WiFi Analyzer alerts on weak WEP implementations and recommends a device firmware upgrade (if available) from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the **TKIP** (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise-level wireless equipment. **TKIP-**enabled devices are not subject to any such WEP key attacks.

Policy - 802.1x authentication failure

The 802.1x authentication has failed. Either certain steps are missed or the client has been misconfigure.d

Device Unprotected by VPN

Alarm Description & Possible Causes

If your WLAN security deployment requires the use of VPN, AirMagnet WiFi Analyzer can alert you on devices that participate in wireless communication without VPN protection. Using VPN protection in your WLAN network can help provide system and user authentication, create dynamic keys for encryption, and provide access control and (most importantly) Quality of Service (QoS). Using VPN in addition to WEP in the network also provides encryption all the way to the VPN gateway. This can be very effective for travelling employees who use hotspot networks.

AirMagnet Solution

AirMagnet WiFi Analyzer recognizes VPN implementations using **IPSec**, **PPTP**, **L2TP**, and **SSH** as the tunneling protocols. Alarms are triggered when devices communicate with each other without any VPN protection.

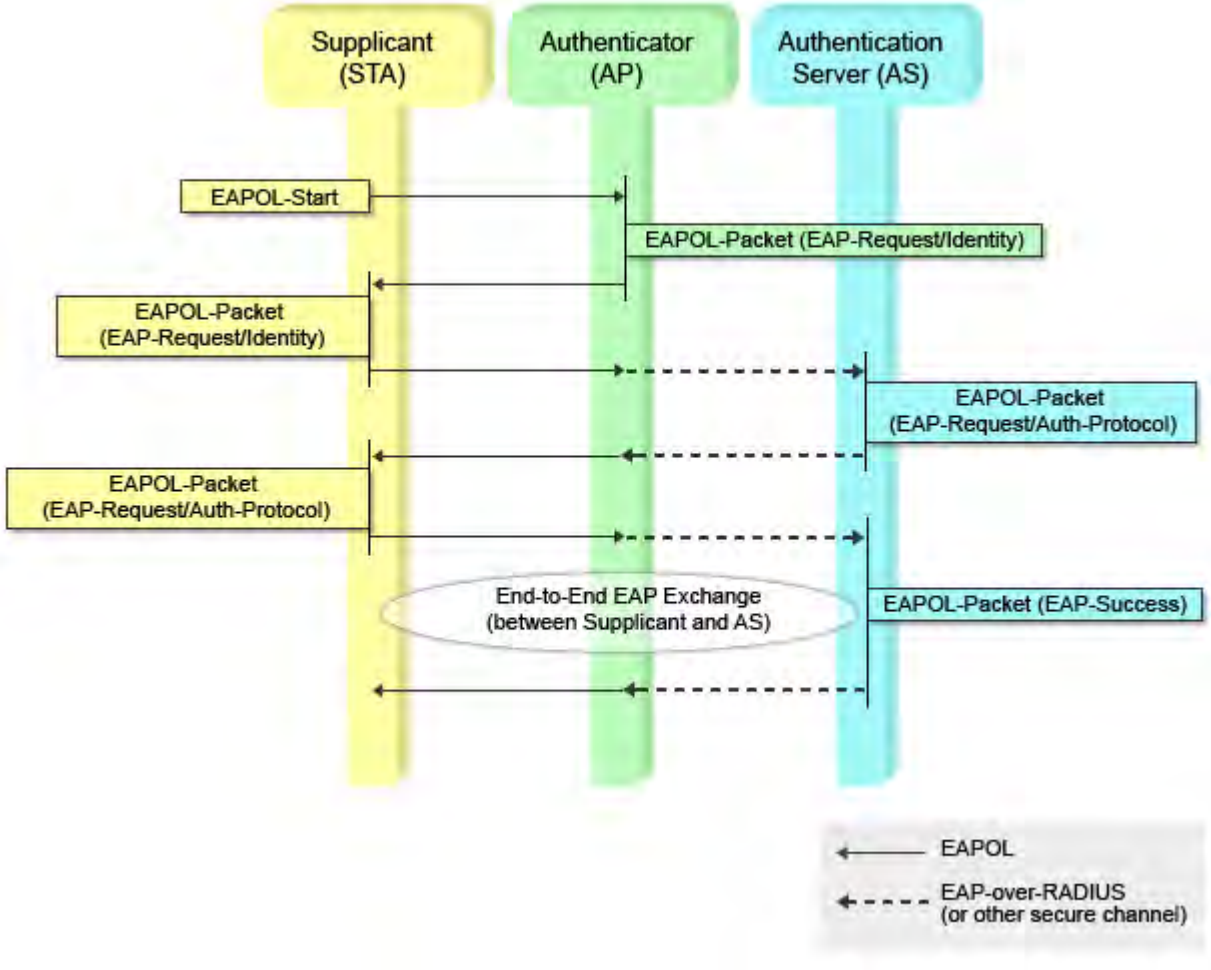
Note: *AirMagnet WiFi Analyzer will not be able to trigger this alarm if 802.11 encryption such as 802.1x or TKIP is also deployed on your WLAN.*

You can disable this AirMagnet WiFi Analyzer alarm if you do not deploy VPN as part of your WLAN security infrastructure.

Device Unprotected by 802.1x

Alarm Description & Possible Causes

If your WLAN security deployment requires the use of 802.1x for authentication and encryption, AirMagnet WiFi Analyzer can alert you on devices that are not configured to use 802.1x protection. **WPA** (Wireless Protected Access) specified 802.1x as one of the requirements. The 802.1x framework provides centralized user authentication and encryption key management.



802.1x framework provides centralized user authentication and encryption key management

802.1x is used with a variety of **EAP** (Extensible Authentication Protocol) types such as **LEAP**, **TLS**, **TTLS**, **EAP-FAST** and **PEAP** to implement an authentication and encryption mechanism. If your WLAN security relies on WPA or 802.1x, APs not configured for 802.1x weaken your WLAN security by allowing non-compliant users to falsely authenticate and enter your wired network. Mis-configured client stations without 802.1x protection also introduce security risks. For example, it would not have the mutual authentication mechanism provided by 802.1x framework and therefore be vulnerable to accidentally associate with an intruder's fake AP.

AirMagnet Solution

AirMagnet WiFi Analyzer recognizes all 802.1x **EAP** types including **PEAP**, **TLS**, **TTLS**, **LEAP**, **EAP-FAST,** and so on. AirMagnet WiFi Analyzer detects APs and client stations unprotected by 802.1x by observing rejected 802.1x authentication challenges.

Ad-hoc Node Using AP's SSID

Alarm Description & Possible Causes

The IEEE 802.11 standard defines two modes of WLAN operation:

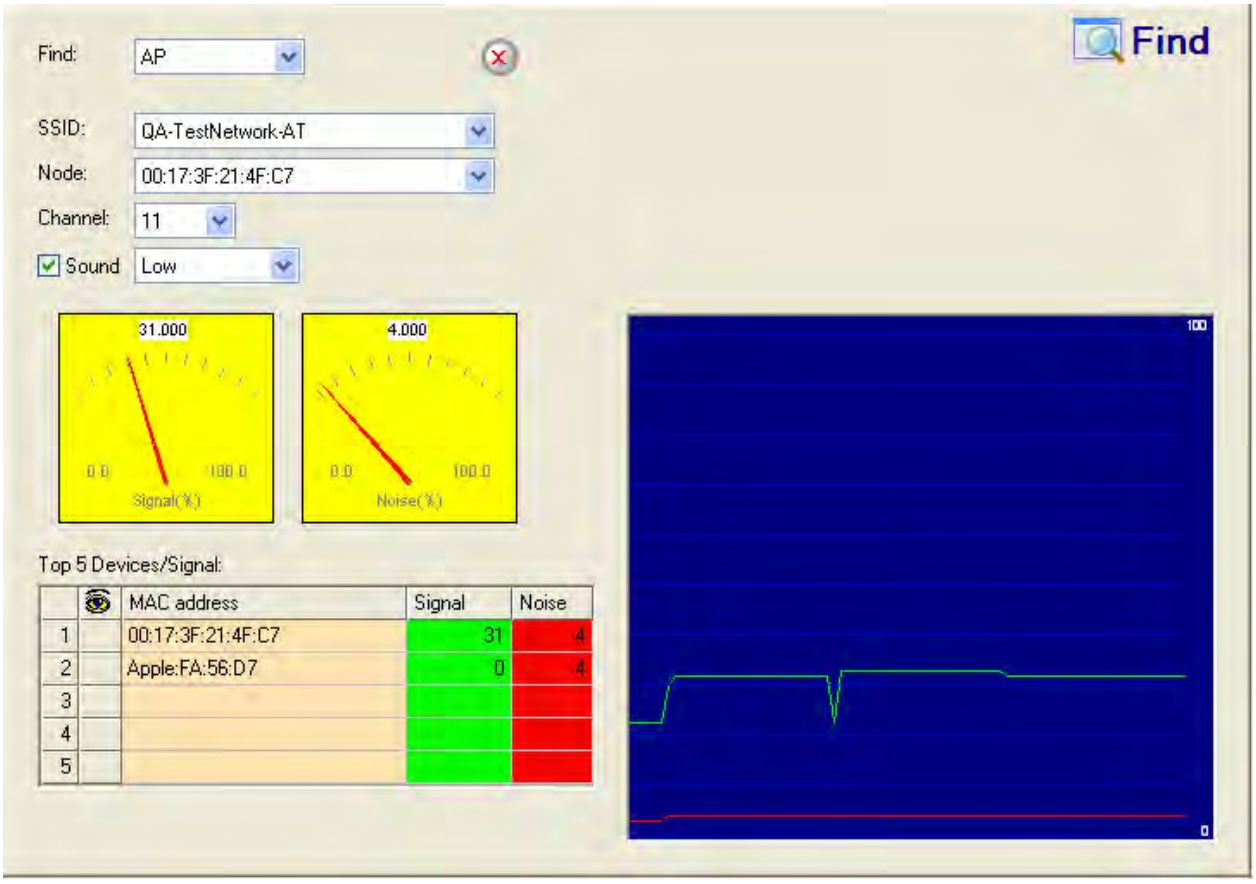
- **Infrastructure** mode for AP and client station networking, and
- **Ad-hoc** mode for peer-to-peer networking between wireless clients.

Both modes may have their own SSIDs and can co-exist in the same RF environment. However, when infrastructure mode and ad-hoc mode devices share the same SSID, client connections may become unreliable and inconsistent. Separate SSIDs should be used for infrastructure and ad-hoc mode WLANs.

Oftentimes, when an SSID is used by both infrastructure mode and ad-hoc mode devices, it is caused by a mis-configuration. Such a mis-configuration may cause connection problems not only for the mis-configured device but also for all clients in the area.

AirMagnet Solution

AirMagnet WiFi Analyzer detects SSID sharing between infrastructure and ad-hoc mode devices and raises an alarm for early warning. Locate the ad-hoc device and force the user to use a different SSID for communicating with other ad-hoc devices. Once the ad-hoc device is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate it.

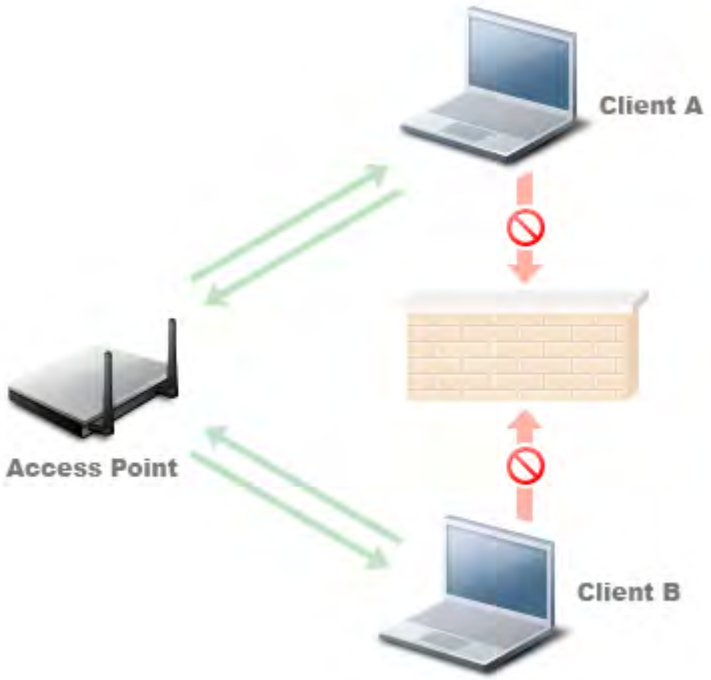


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Hidden Station Detected

Alarm Description & Possible Causes

A hidden station problem occurs when a wireless node cannot hear one or more of the other nodes, and thus the media access protocol (**CSMA/CA** - Carrier Sense Multiple Access/Collision Avoidance) cannot function properly. When this happens, multiple nodes will attempt to transmit their data over the shared medium simultaneously, causing signal interference with one another. For example, imagine there are two 802.11 end-users (Station A and Station B) and one access point. Station A and Station B can't hear each other because of high attenuation (for example, substantial range), but they can both communicate with the same access point. Because of this situation, Station A may begin sending a frame without noticing that Station B is currently transmitting (or vice versa). This will very likely cause a collision between Station A and Station B to occur at the access point. As a result, both Station A and Station B would need to re-transmit their respective packets, which results in higher overhead and lower throughput.

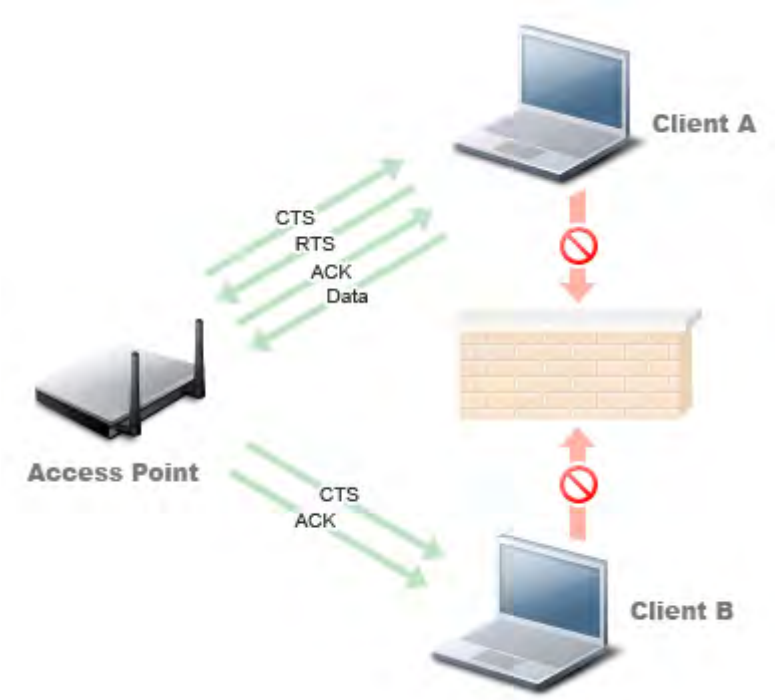


Hidden Node Problem - Traffic from Station A and Station B Collide at AP

AirMagnet Solution

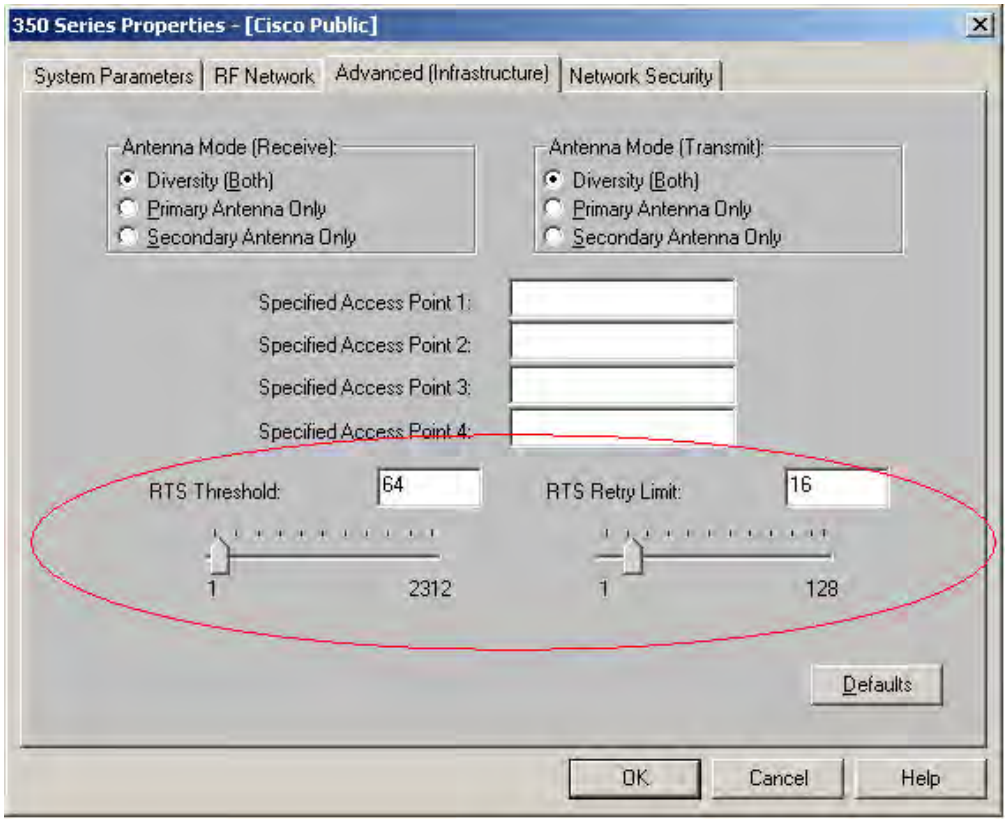
AirMagnet WiFi Analyzer detects a hidden node problem by identifying a hidden station from the location. For example, if you placed an AirMagnet WiFi Analyzer at the location of **Station A** above, it would passively listen and analyze the traffic received at that location and identify all stations hidden from the location (where the AirMagnet Analyzer is located). Once hidden stations are detected, AirMagnet WiFi Analyzer would suggest countermeasures, typically turning on the **RTS**/**CTS** (Request-to-send/Clear-to-send) mechanism to coordinate media access. In the above example, one would re-configure Station A and Station B to have a very low threshold (packet size) to trigger the use of **RTS** and **CTS**.

RTS/CTS Mechanism is Designed to Synchronize Wireless Medium Access Before Data Transmission



RTS/CTS Mechanism Resolves Hidden Node Problem

In order to configure a device to use RTS/CTS, please see the sample Cisco configuration below:



Sample RTS/CTS Configuration for a Cisco Aironet Client Adapter to Resolve the Hidden Node Problem

Unassociated Station Detected

Alarm Description & Possible Causes

In the event where a wireless client station failed to authenticate or associate with an Access Point, it would continue trying periodically until it is successfully associated for normal communication. AirMagnet WiFi Analyzer detects client stations stuck in the constant retry mode to alert the WLAN administrator for two reasons:

- A user is out of wireless service and is in need of help.
- If multiple users are reported by AirMagnet Wi-Fi Analyzer to be in the unassociated mode, then the wireless infrastructure (AP or back-end authentication server) may be down.

AirMagnet Solution

AirMagnet Wi-Fi Analyzer reports this alarm along with the SSID of the unassociated client station. The WLAN administrator can use the AirMagnet Diagnostic Tool to proactively find the association or authentication problem with the reported unassociated station. Alternatively, the WLAN administrator can also use AirMagnet WiFi Analyzer's active end-to-

end test tools to further investigate the problem by emulating a client station in the action of association, DHCP, Ping, and Trace route.

AP System or Firmware Reset

Alarm Description & Possible Causes

The wireless access point goes through a system or firmware reset in the event of reconfiguration, power failure, or software defects. When a system reset occurs, all previously associated client stations lose their connections until the access point has completed its startup sequence of actions. All client stations have to go through the authentication and association procedure to regain wireless connectivity. The period of lost connectivity may range from tens of seconds to a few minutes.

Since the AP reset is transient and wireless service eventually recovers, there is usually very little trace to link it to the lost client connectivity.

AirMagnet Solution

AirMagnet WiFi Analyzer can accurately detect an AP system reset regardless of the cause. With this AirMagnet WiFi Analyzer alarm, linkage can be drawn between interrupted service and its root cause in such a scenario.

AP Broadcasting SSID

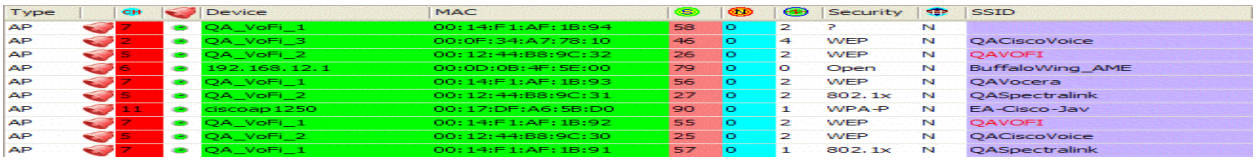
Alarm Description & Possible Causes

WLAN SSIDs are typically announced in the broadcast beacon frames sent by Access Points. It is meant for client stations to easily identify available WLANs and the APs providing the service. War-drivers equipped with tools such as Netstumbler sometimes scan for the SSIDs sent by Access Points to discover potential targets. If the WLAN SSID is uncovered, your network may be susceptible to two specific threats:

- Intruders can set the SSID on their client to attempt to join that WLAN. According to most war-driving web sites, many Access Points implemented these days are operating without any security. Even though knowing the SSID name does not necessarily mean that rogue clients will be able to join the network, it is necessary to carry out other forms of security attacks (such as Denial-of-service).
- Your WLAN and APs with GPS information on your geographical location may be collected in a global database and published on the Internet.

AirMagnet Solution

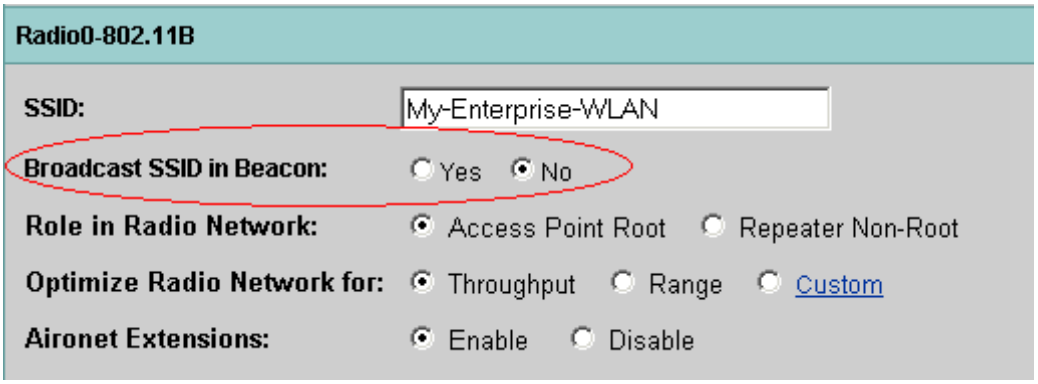
AirMagnet WiFi Analyzer detects an AP broadcasting its SSID and triggers alarms (it is also able to discover SSIDs that are not broadcast). In the **Start** page, APs are listed with their SSIDs in red to indicate a non-broadcast SSID. See sample AirMagnet screenshots below:



Type		Device	MAC				Security		SSID
AP	7	QA_VoFi_1	00:14:F1:AF:1B:94	58	0	2	?	N	
AP	2	QA_VoFi_3	00:0F:34:A7:78:10	46	0	4	WEP	N	QACiscoVoice
AP	5	QA_VoFi_2	00:12:44:B8:9C:32	26	0	2	WEP	N	QAVOFI
AP	6	192.168.12.1	00:0D:0B:4F:5E:00	79	0	0	Open	N	BuffaloWing_AME
AP	7	QA_VoFi_1	00:14:F1:AF:1B:93	56	0	2	WEP	N	QAVocera
AP	5	QA_VoFi_2	00:12:44:B8:9C:31	27	0	2	802.1x	N	QASpectralink
AP	11	ciscoap1250	00:17:DF:A6:5B:D0	90	0	1	WPA-P	N	EA-Cisco-Jav
AP	7	QA_VoFi_1	00:14:F1:AF:1B:92	55	0	2	WEP	N	QAVOFI
AP	5	QA_VoFi_2	00:12:44:B8:9C:30	25	0	2	WEP	N	QACiscoVoice
AP	7	QA_VoFi_1	00:14:F1:AF:1B:91	57	0	1	802.1x	N	QASpectralink

START page shows non-broadcast SSID in red

Most AP vendors support the configuration for SSID broadcast. A Cisco Aironet AP can be configured from the Internet browser (see illustration below).



Turning off SSID broadcast for Cisco Aironet Access Point through the browser interface

Ad-hoc Station Detected

Alarm Description & Possible Causes

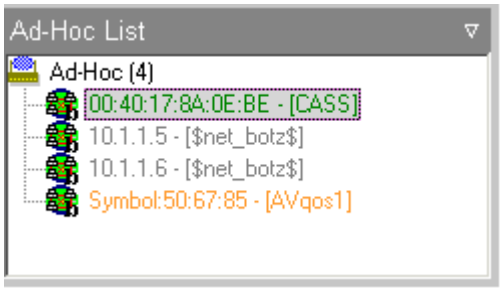
A Wireless client station operating in ad-hoc mode (peer-to-peer networking) is usually not protected by the same rigorous security rules as enterprise-deployed APs in the infrastructure mode.

Ad-hoc Mode Networking (Station Peer-to-Peer) Bypasses Enterprise Security Infrastructure

Peer-to-peer networking is usually not supported by the enterprise WLAN, and thus lacks the necessary security measures such as 802.1x user authentication and the dynamic key encryption. As a result, ad-hoc mode stations risk exposing data in the air through weak (if any) encryption. In addition, weak authentication may allow unauthorized devices to associate. If the ad-hoc mode client station is also connected to the wired network, the entire enterprise wired network is at risk. An Ad-hoc mode client station should be investigated as a rogue AP because of the high risk imposed.

AirMagnet Solution

AirMagnet WiFi Analyzer detects ad-hoc mode usage and triggers alarms. To get a list of all ad-hoc mode stations, you can use the **Infrastructure** view. See the illustration below:



Infrastructure page identifies all Ad-hoc mode stations for security sweep

Once this alarm is triggered, you can locate the ad-hoc device using the Find tool and remove it from the enterprise network.

High Management Traffic Overhead

Alarm Description & Possible Causes

The IEEE 802.11 standard defines three basic frame types: Management, Control, and Data frames. Management frames (such as beacon, probe-request/response, association request/response, authentication, and so on) do not carry user data but are needed to facilitate connection setup. They are considered to be the necessary overhead of WLAN operation.

Frame Type (Bits 2,3)	Subfield (Bits 7,6,5,4)	Frame Function
Management Type 00	*0000*	*Association Request*
	0001	*Association Response*
	0010	*Association Request*
	0011	*Reassociation Response*
	0100	*Probe Response*
	0101	*Probe Response*
	1000	*Beacon*
	1001	*Announcement Traffic Indication (ATIM)*
	1010	*Dissassociation*
	1011	*Authentication*
	1100	*Deauthentication*
Control Type 01	*1010*	*Power-Save (PS) Poll*
	1011	*Request to Send (RTS)*
	1100	*Acknowledgement (ACK)*
	1110	*Contention Free (CF) End*
	1111	*CF End + CF ACK*
Data Type 10	*0000*	*Data*
	0001	*Data + CF ACK*
	0010	*Data + CF Poll*
	0011	*Data + CF ACK + CF Poll*
	0100	*Null (no data)*
	0101	*CF ACK*
	0110	*CF Poll*
	0111	*CF ACK + CF Poll*
Reserved Type 11		

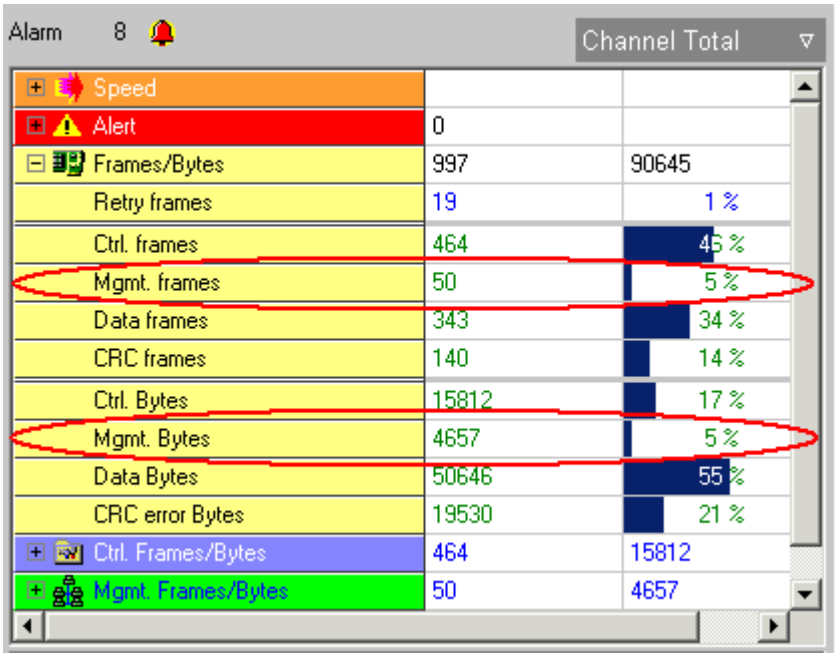
802.11 Frame Types for Management, Control, and Data Frames

Management frames are sent in low speed (1mbps or 2mbps for 802.11b), and therefore consume more WLAN bandwidth than data frames. In an efficient WLAN, channel bandwidth utilization by management frame traffic should be rather low (less than 1%). A high percentage of management traffic is a problem by itself in terms of bandwidth consumption, but it may also be an indication of more severe problems. For example, if many client

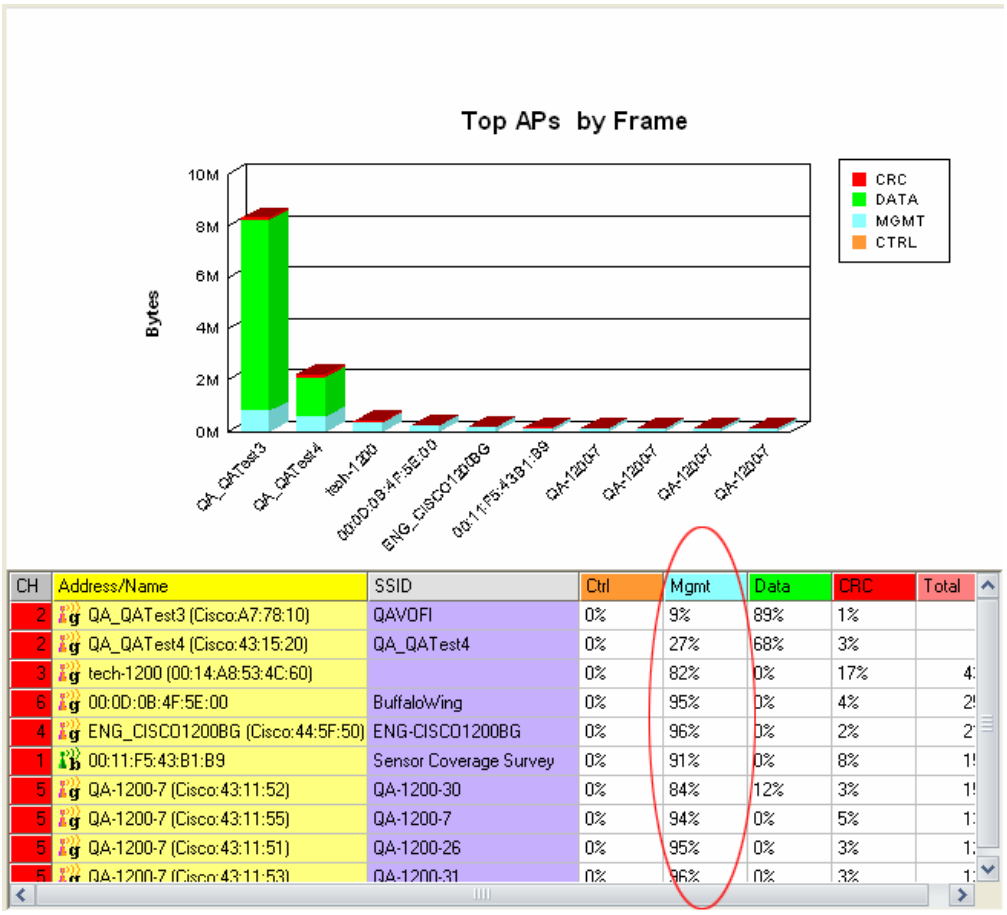
stations fail to associate with AP, they constantly retry associating to the AP, resulting in large amount of management traffic.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks management traffic and its corresponding bandwidth utilization status on a per channel and per device basis. When the user-defined utilization threshold is exceeded, alarms are triggered. To further pin down the cause of the high management overhead problem, the WLAN administrator may investigate the problem by using the AirMagnet **Channel** or **Charts** view. Refer to the sample screen shots below:



Channel page displays the management frame statistics



CH	Address/Name	SSID	Ctrl	Mgmt	Data	CRC	Total
2	QA_QATest3 (Cisco:A7:78:10)	QAVOFI	0%	9%	89%	1%	
2	QA_QATest4 (Cisco:43:15:20)	QA_QATest4	0%	27%	68%	3%	
3	tech-1200 (00:14:A8:53:4C:60)		0%	82%	0%	17%	4
6	00:0D:0B:4F:5E:00	BuffaloWing	0%	95%	0%	4%	2
4	ENG_CISCO1200BG (Cisco:44:5F:50)	ENG-CISCO1200BG	0%	96%	0%	2%	2
1	00:11:F5:43:B1:B9	Sensor Coverage Survey	0%	91%	0%	8%	1
5	QA-1200-7 (Cisco:43:11:52)	QA-1200-30	0%	84%	12%	3%	1
5	QA-1200-7 (Cisco:43:11:55)	QA-1200-7	0%	94%	0%	5%	1
5	QA-1200-7 (Cisco:43:11:51)	QA-1200-26	0%	95%	0%	3%	1
5	QA-1200-7 (Cisco:43:11:53)	QA-1200-31	0%	96%	0%	3%	1

Channel page displays the traffic distribution among management/data/control frames by channel or by device

AP Overloaded by Stations

Alarm Description & Possible Causes

A WLAN Access Point has only limited resources, and therefore it can only service a limited number of clients. When the limit is reached, additional clients may have service requests rejected or existing clients may experience degraded performance. When designing a WLAN equipment deployment and provisioning for service, this limitation should be considered. After deployment, the limitation may be challenged by the growing number of users, and it therefore requires constant monitoring for under-provisioned deployment.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors on the AP work load by tracking its active client stations. You can configure the system to generate alarms of different severity levels by the work load threshold (active client session count), for example, warning alarms for 64 active client sessions and urgent alarms for 128 active client sessions. To investigate the AP current

client sessions, you can use the **Infrastructure** view. If multiple APs are becoming overloaded frequently, it is recommended that you either reduce the number of clients connecting to the network or increase the number of APs implemented.

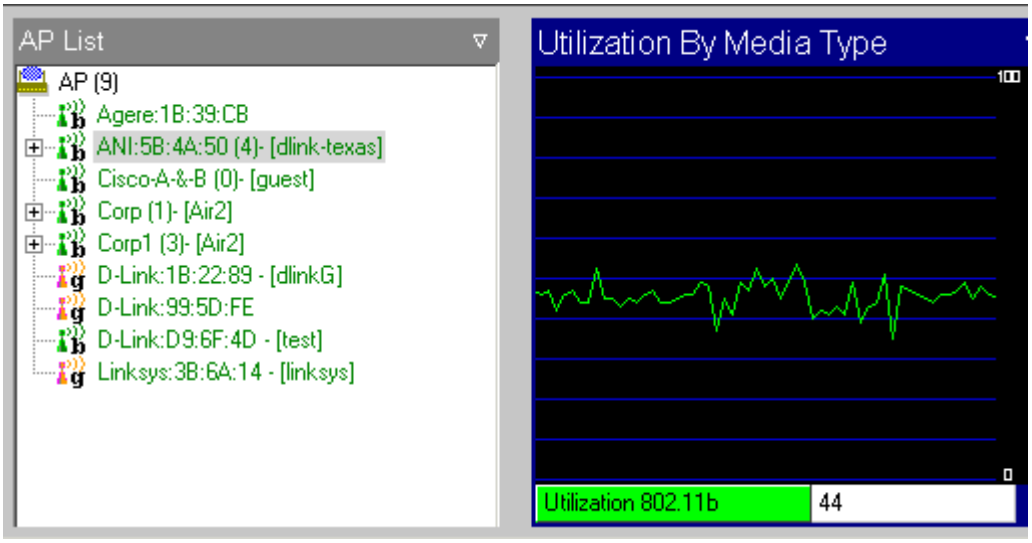
AP Overloaded by Utilization

Alarm Description & Possible Causes

A WLAN design for deployment generally includes an expectation for the maximum number of clients an AP can support. Similarly, there is an expectation for the maximum bandwidth utilization supported by an AP. Such expectations can be used to monitor on sufficient WLAN provisioning and effective load-balancing.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks AP bandwidth utilization (the sum of outgoing and incoming traffic combined) and raises an alarm when the sustained utilization exceeds the user-configured threshold. To further investigate AP bandwidth utilization, you may use the **Infrastructure** screen to identify stations associated with this AP and their individual bandwidth consumption from and to the AP. You may also use the **Charts** screen to identify the top talkers on your WLAN and their respective traffic type/speed distribution. If multiple APs are becoming overloaded frequently, it is recommended that you either reduce the number of clients connecting to the network or increase the number of APs implemented.



Infrastructure page displays AP bandwidth utilization

802.1x Rekey Timeout Too Long

Alarm Description & Possible Causes

It is well publicized that WLAN devices using a static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir*). A cracked WEP secret key results in no encryption protection thus compromises data privacy. Dynamic encryption key or key rotation mechanisms such as **TKIP** resolve such vulnerabilities by periodically changing the encryption key, even within a single session. Managing key rotation for multicast and broadcast traffic is usually more challenging because multiple devices have to update to the new key synchronously. Vendors' implementations of multicast/broadcast key rotation can vary from null to complete. When the multicast and broadcast key is not rotated or rotated infrequently, it is as weak as static WEP, which is subject to key recovery attacks.

By continuously monitoring on WLAN 802.1x authentication and encryption transactions, AirMagnet Wi-Fi Analyzer can detect an AP configured without encryption key rotation or configured with a long key rotation timeout. It is important for WLAN 802.1x configurations to include a reasonable encryption rekey timeout as explained above, as a stale encryption key makes your encryption static and as vulnerable as static WEP key encryption. A rekey mechanism should be applied to unicast, multicast, and broadcast data streams. **TKIP** (Temporal Key Integrity Protocol) enabled devices implement a WEP key hashing algorithm and typically rotate keys on their unicast data streams, but not always on the multicast or broadcast data streams.

AirMagnet Solution

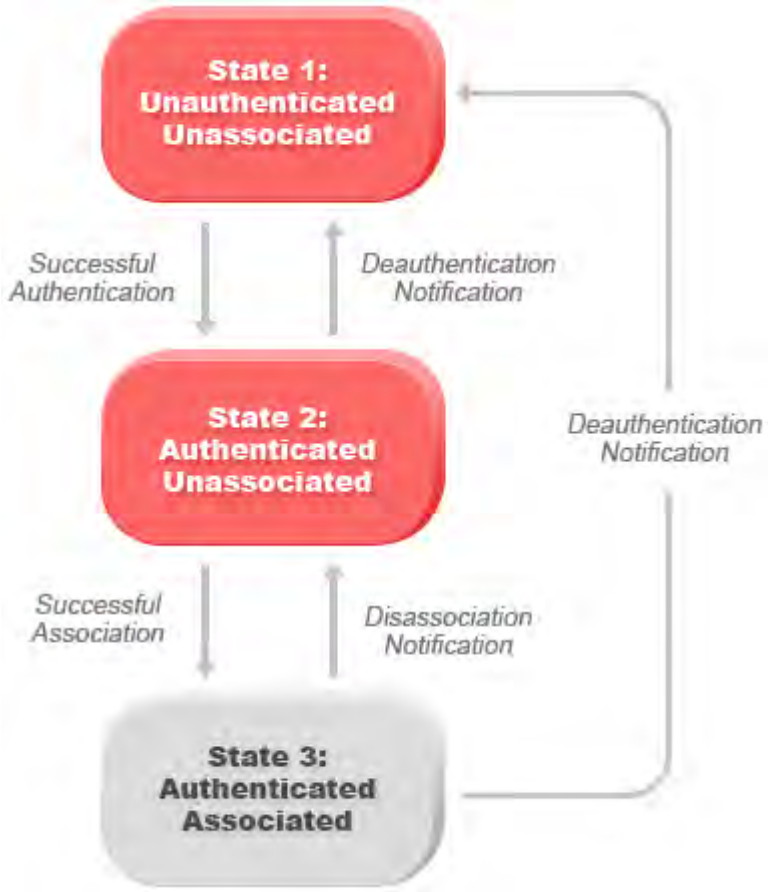
This AirMagnet WiFi Analyzer alarm assists you in enforcing the rekey mechanism for all data streams. Take appropriate steps (such as checking the AP configuration for this setting) to resolve this issue.

Denial-of-Service Attack: Authentication Flood

Potential Attack tool: Void11

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and APs implement such a state machine (illustrated below) according to the IEEE standard. On the AP, each client station has a state recorded in AP's client table (association table), which always has a size limit that can be either a hard coded number or based on the physical memory constraint.



Attacker spoofs many 802.11 authentication requests to flood AP association table with clients stuck in state 1 and state 2

A form of denial-of-service attack aims to flood the AP's client state table (association table) by emulating many client stations (MAC address spoofing) sending authentication requests to the AP. Upon reception of each individual authentication request, the target AP would create a client entry in **state 1** in the association table. If **Open System** authentication is used on the AP, the AP would send back an **authentication success** frame and move the client to **state 2**. If Shared-key authentication is used on the AP, the AP would send an **authentication challenge** to the attacker's emulated client, which would not respond. In this case, the AP keeps the client in **state 1**. In either case, the AP ends up with many clients dangling in either **state 1** or **state 2,** filling up the AP association table. When the table reaches its limit, legitimate clients will not be able to authenticate and associate with this AP, thus denial-of-service attack is committed.

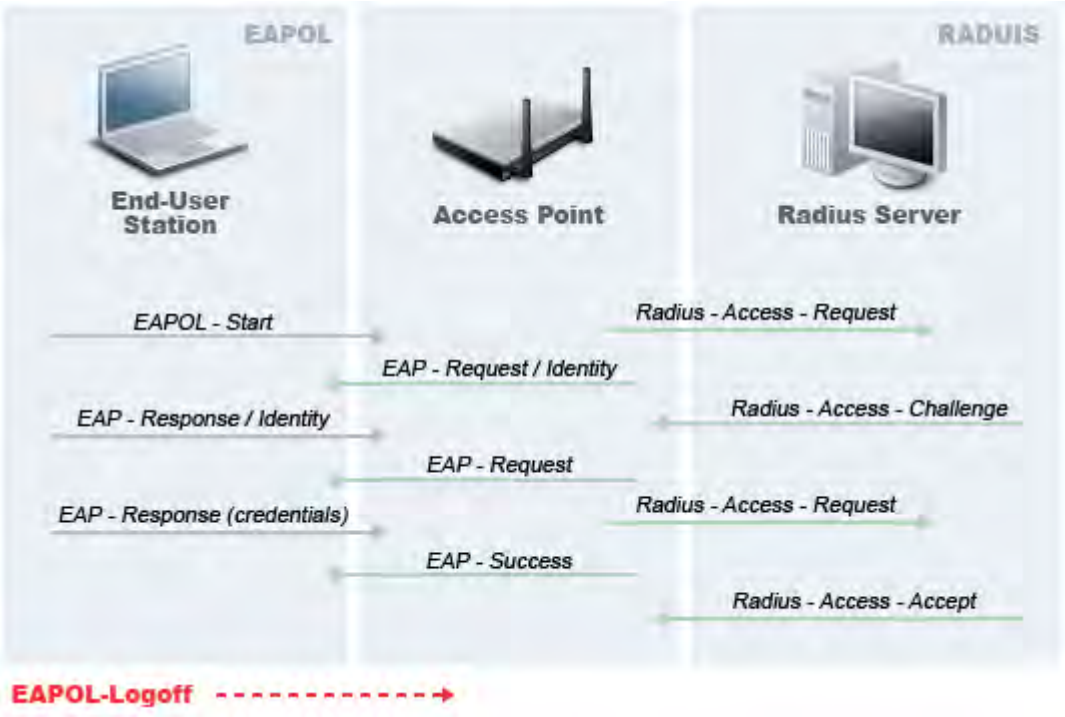
AirMagnet Solution

AirMagnet WiFi Analyzer detects this form a DoS attack by tracking client authentication and association states. When the alarm is triggered, the AP under attack will be identified. The WLAN security analyst can log on to the AP to check the current association table status or use the AirMagnet active tool (DHCP, ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: EAPOL-Logoff Attack

Alarm Description & Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame to begin the authentication transaction. At the end of an authenticated session when a client station wishes to log off, the client station sends an 802.1x EAPOL-Logoff frame to terminate the session with the AP.



Attacker spoofs a 802.1x EAPOL-Logoff frame from the legitimate client station to fool the AP in logging off the client

Since the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame, logging the user off the AP, thus committing a Denial-of-Service attack. While this client station is logged off from the AP using the attacker's spoofed EAPOL-logoff frame, the client station is actually unaware of it until it tries to communicate through the WLAN later. Typically, the client station will discover the disrupted connection status and re-associate and authenticate automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-Logoff frames to be effective on this attack.

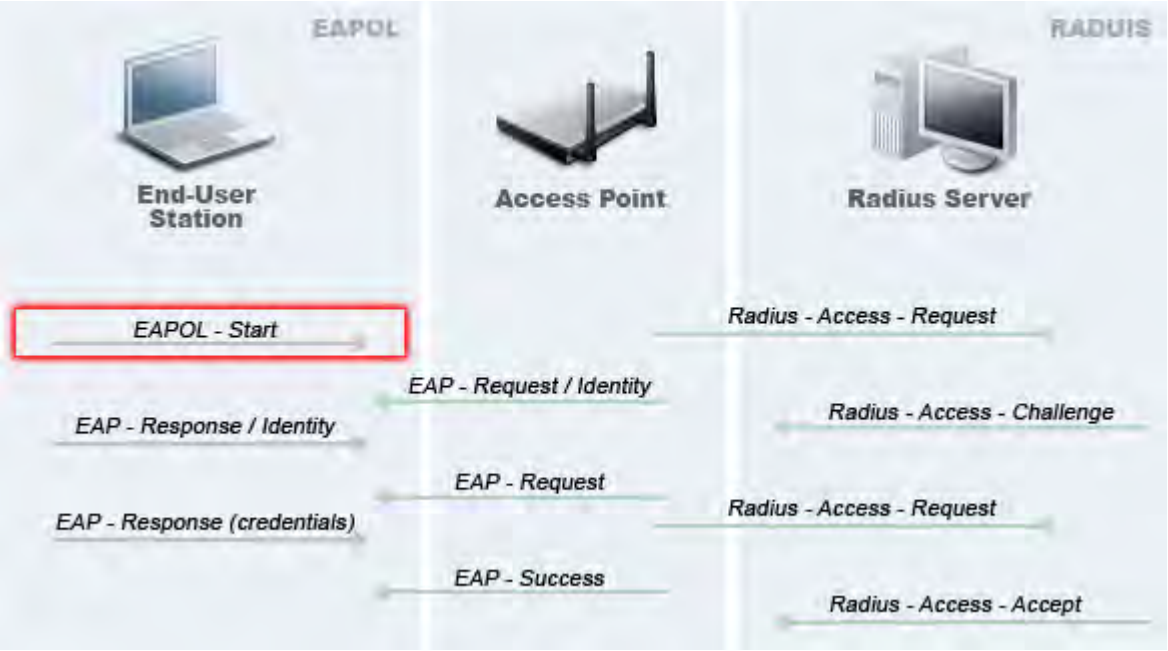
AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and AP under attack will be identified. The WLAN security officer can log on to the AP to check the current association table status or use AirMagnet active tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: EAPOL-Start Attack

Alarm Description & Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame sent by the client station to begin the authentication transaction. The AP responds to an EAPOL-Start frame with an EAP-Identity-Request and some internal resource allocation.



Attacker floods 802.1x EAPOL-Start frames to exhaust AP resources

An attacker can attempt to bring down an Access Point by flooding it with EAPOL-Start frames to exhaust the AP internal resources. When the AP has no more internal resources to allocate, users will be unable to associate to it, thus initiating a Denial-of-Service.

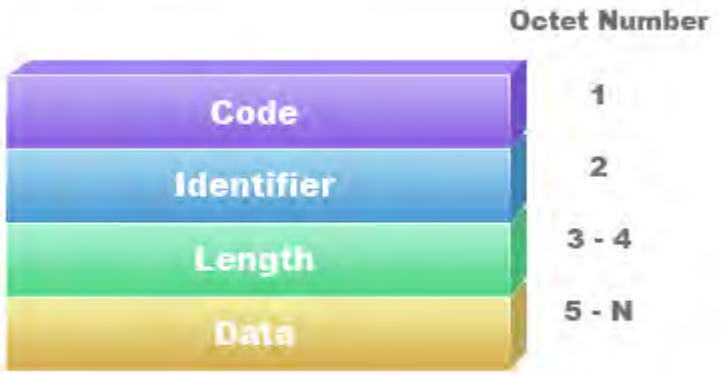
AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of Denial-of-Service attack by tracking the 802.1x authentication state transition and particular attack signature. When the alarm is triggered, the client and AP under attack will be identified. The WLAN security officer can log on to the AP to check the current association table status or use AirMagnet active tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: EAP ID Flood Attack

Alarm Description & Possible Causes

IEEE 802.1x and IETF RFC 2284 defines the EAP packet header format as follows:



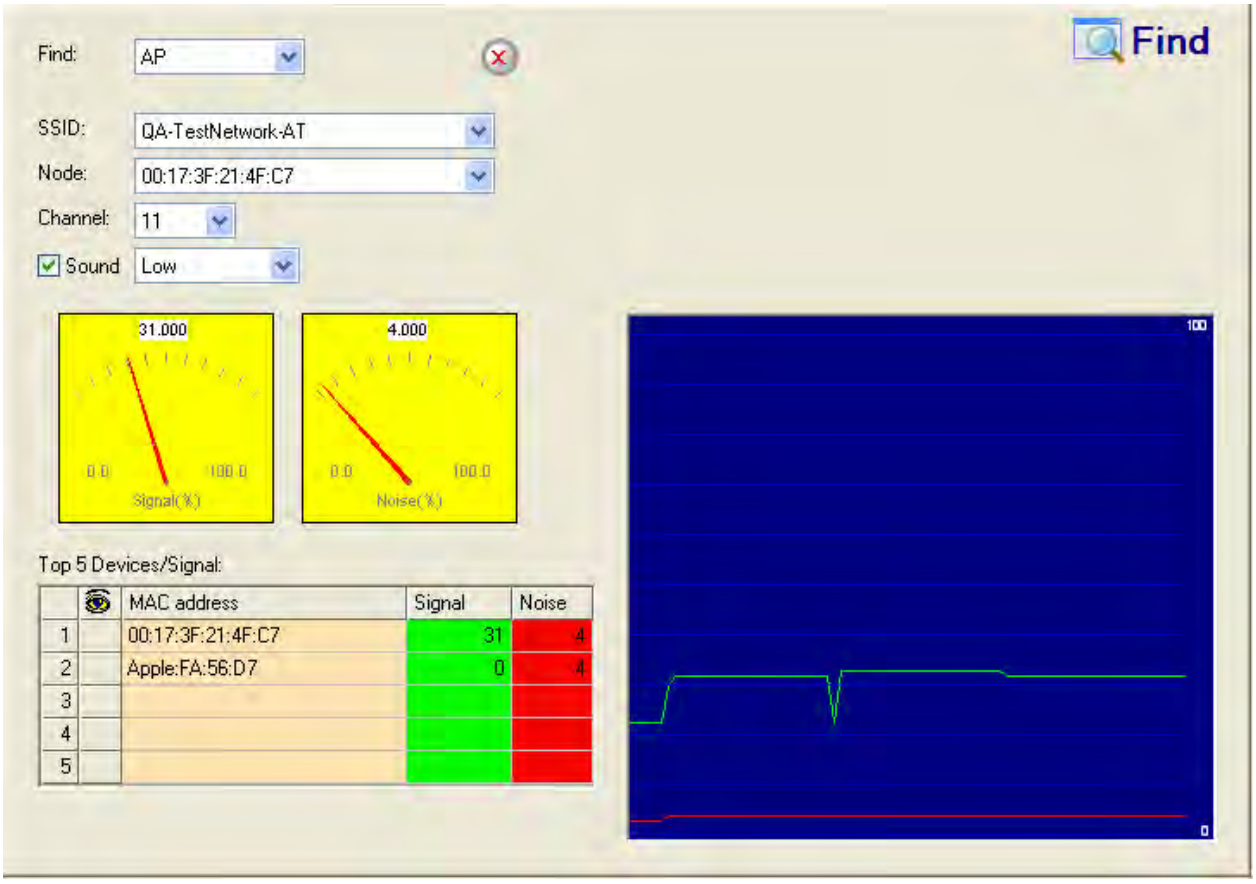
802.1x EAP packet header format - the identifier field is 1 byte long

The Identifier field is one octet in length and allows the matching of responses with the requests. The Identifier field and System Port (that is, 802.11 association) together uniquely identify an authentication exchange. Thus, the use of a single octet identifier field results in a restriction of 256 authentications per System Port.

An attacker could attempt to bring down the 802.1x authentication capability on an access point by consuming the EAP Identifier space (0-255). Since the EAP Identifier is only required to be unique within an 802.11 association, there is no need for an access point to lock out further connections once the Identifier space has been exhausted. This attack is only effective on APs that implement the EAP Identifier as a system wide parameter (as opposed to per 802.11 association parameter).

AirMagnet Solution

Use AirMagnet WiFi Analyzer's FIND tool to locate the device and take appropriate steps to remove it from the wireless environment. Refer to the illustration below.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Denial-of-Service Attack: Premature EAP-Success Attack

Alarm Description & Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or **EAPOL**. The **802.1x** protocol starts with a **EAPOL-Start** frame to begin the authentication transaction. When the 802.1x authentication packet exchange completes with the back-end **RADIUS** server, the AP sends an **EAP-Success** frame to the client to indicate a successful authentication. See the protocol exchange highlighted below:

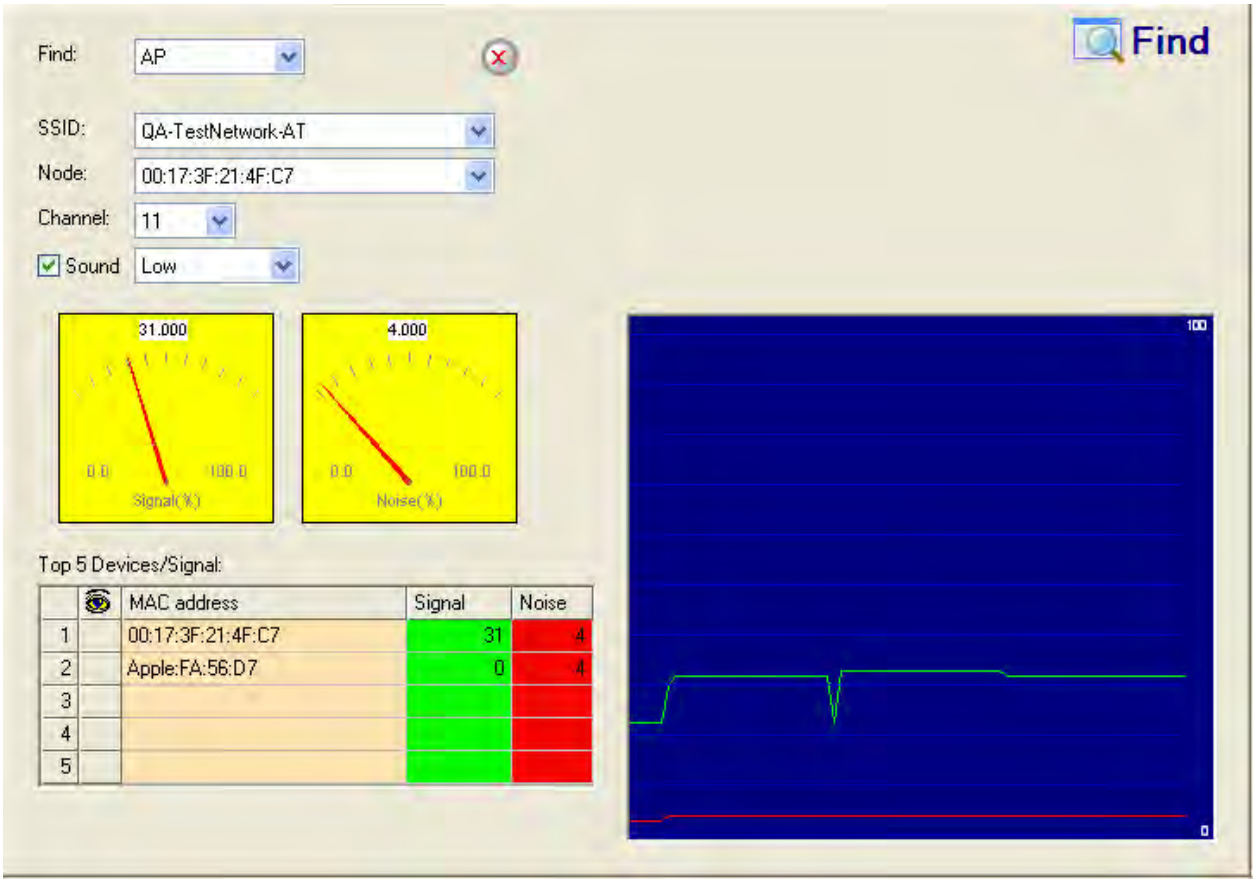
Attacker spoofs pre-mature EAP-Success frames from an AP before the authentication is completed

The IEEE 802.1X specification prohibits a client from bringing up its interface when the required mutual authentication has not been completed. This enables a well-implemented 802.1x client station to avoid being fooled by a fake AP sending premature **EAP-Success** packets to bypass the mutual authentication process.

An attacker could keep the client interface from coming up (therefore Denial-of-Service) by continuously spoofing pre-mature **EAP-Success** frames from the AP to the client to disrupt the authentication state on the client as explained in the previous paragraph.

AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of DoS attack by tracking spoofed pre-mature **EAP-Success** frames and the 802.1x authentication states for each client station and AP. The user can use AirMagnet Wi-Fi Analyzer's Find tool to locate the device and take appropriate steps to remove it from the wireless environment.

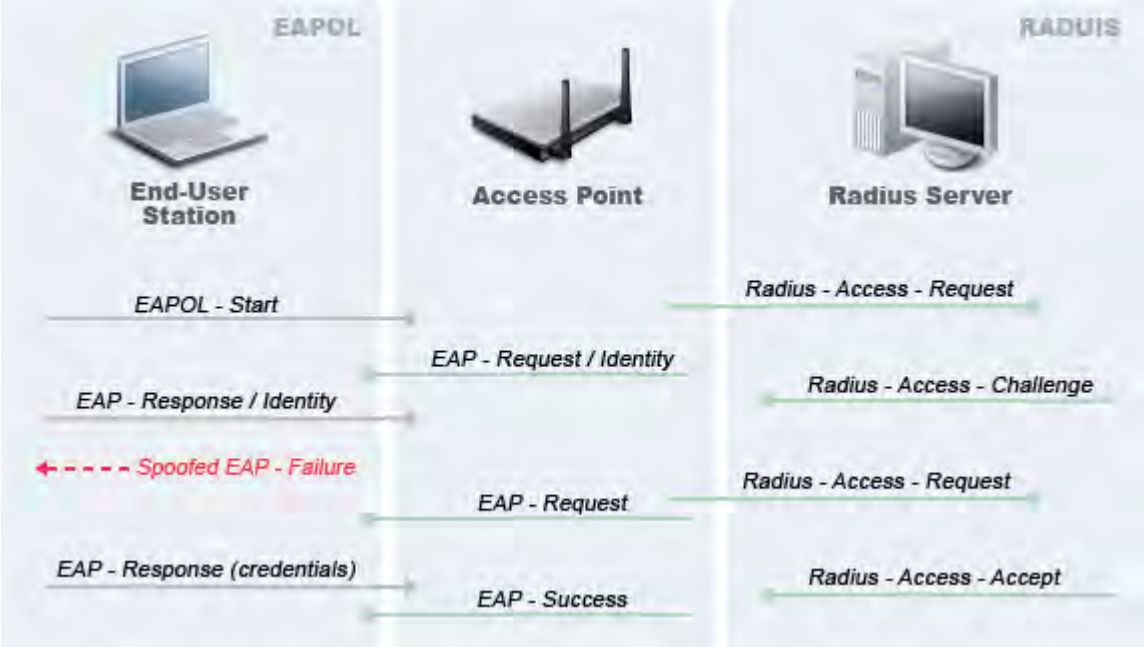


AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Denial-of-Service Attack: Premature EAP-Failure Attack

Alarm Description & Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or **EAPOL**. The **802.1x** protocol starts with a **EAPOL-Start** frame to begin the authentication transaction. When the 802.1x authentication packet exchange completes with the back-end **RADIUS** server, the AP sends an **EAP-Success** or **EAP-Failure** frame to the client to indicate a successful or failed authentication. See the protocol exchange highlighted below:



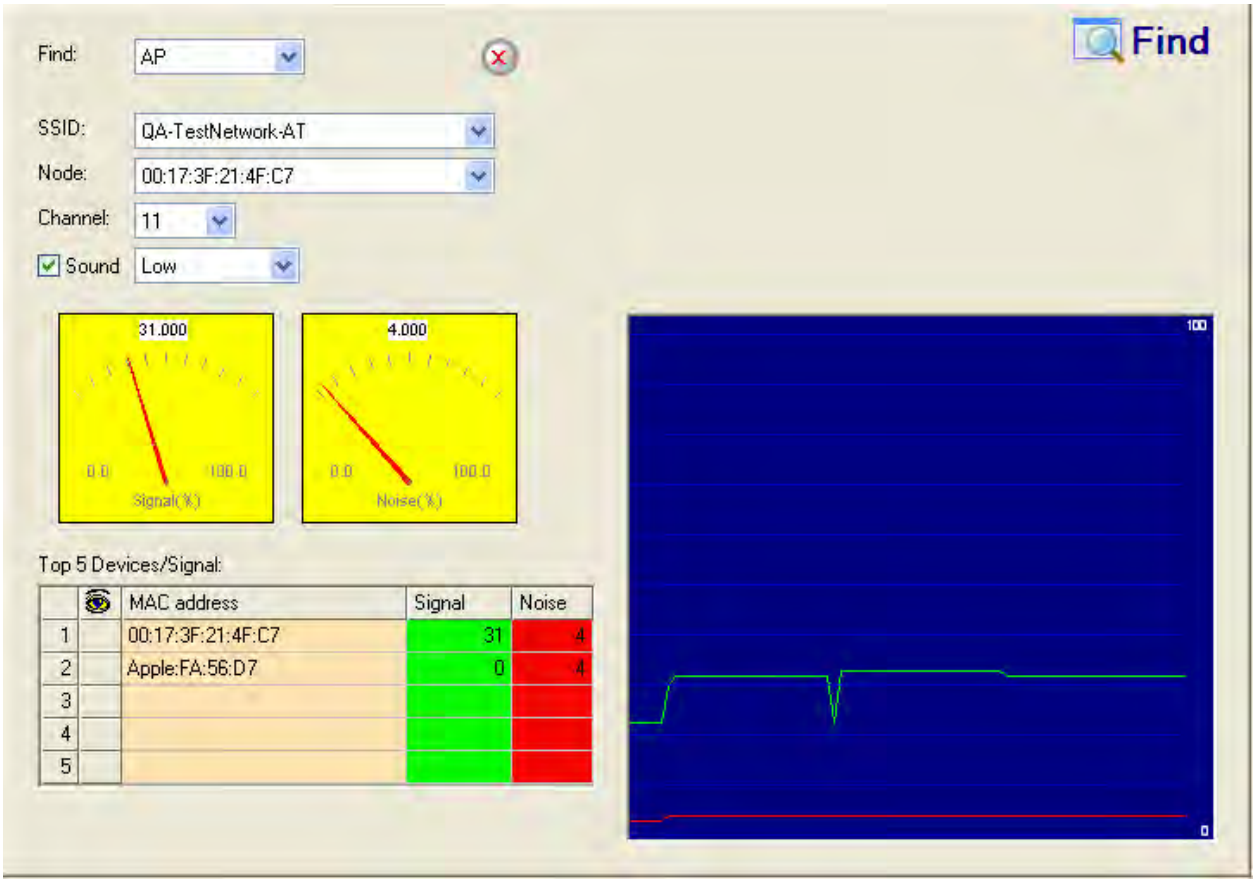
Attacker spoofs pre-mature EAP-Failure frames from an AP before the authentication is completed

The IEEE 802.1X specification prohibits a client to bring up its interface when the required mutual authentication has not been completed. This enables a well implemented 802.1x client station to avoid being fooled by a fake AP sending premature **EAP-Success** packets to bypass mutual authentication.

An attacker could keep the client interface from coming up (therefore Denial-of-Service) by continuously spoofing pre-mature **EAP-Failure** frames from the AP to the client to disrupt the authentication state on the client as explained in the previous paragraph.

AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of DoS attack by tracking the spoofed pre-mature **EAP-Failure** frames and the 802.1x authentication states for each client station and AP. You can use AirMagnet WiFi Analyzer's Find tool to locate the device and take appropriate steps to remove it from the wireless environment.



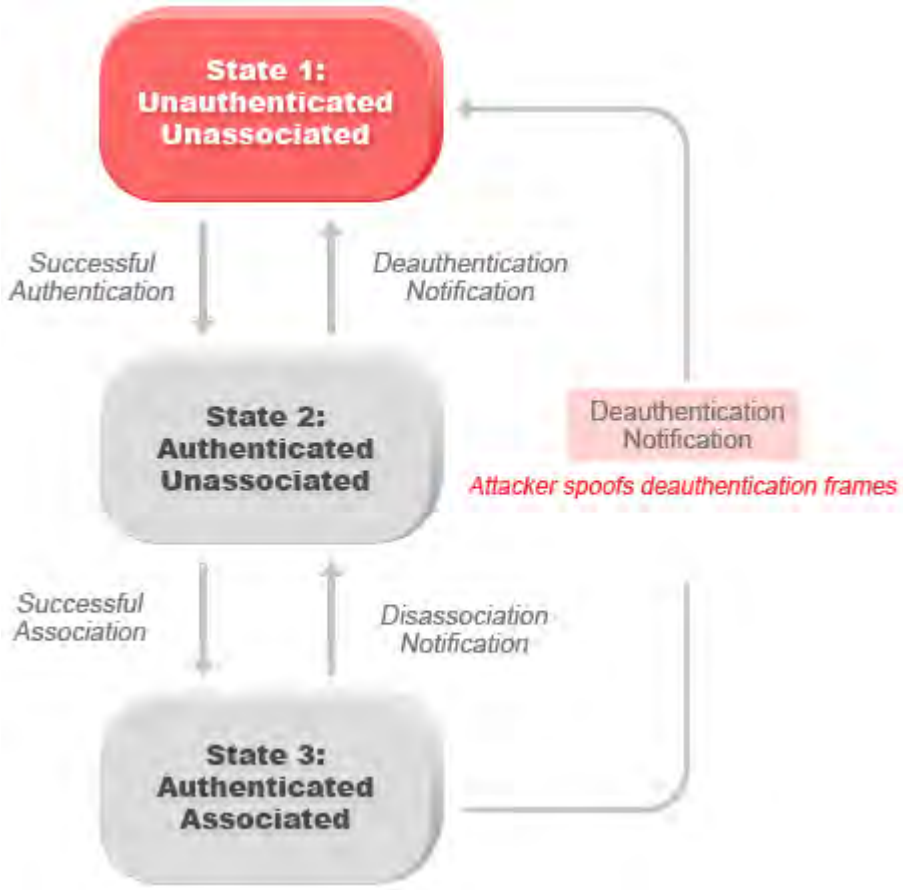
AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Denial-of-Service Attack: De-Authentication Broadcast

Potential Attack tools: WLAN Jack, Void11, Hunter Killer, AirForge

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and APs implement such a state machine (illustrated below) according to the IEEE standard. A successfully associated client station stays in **State 3** in order to continue the wireless communication. Client station in **State 1** and **State 2** can not participate in WLAN data communication until it is authenticated and associated to **State 3**.



Attacker spoofs 802.11 de-authentication frames from AP to client station to bring client to state 1

A form of denial-of-service attack aims to send all clients of an AP to the unassociated/unauthenticated **State 1** by spoofing de-authentication frames from the AP to the broadcast address. With today's client adapter implementation, this form of attack is very effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations would re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame.

AirMagnet Solution

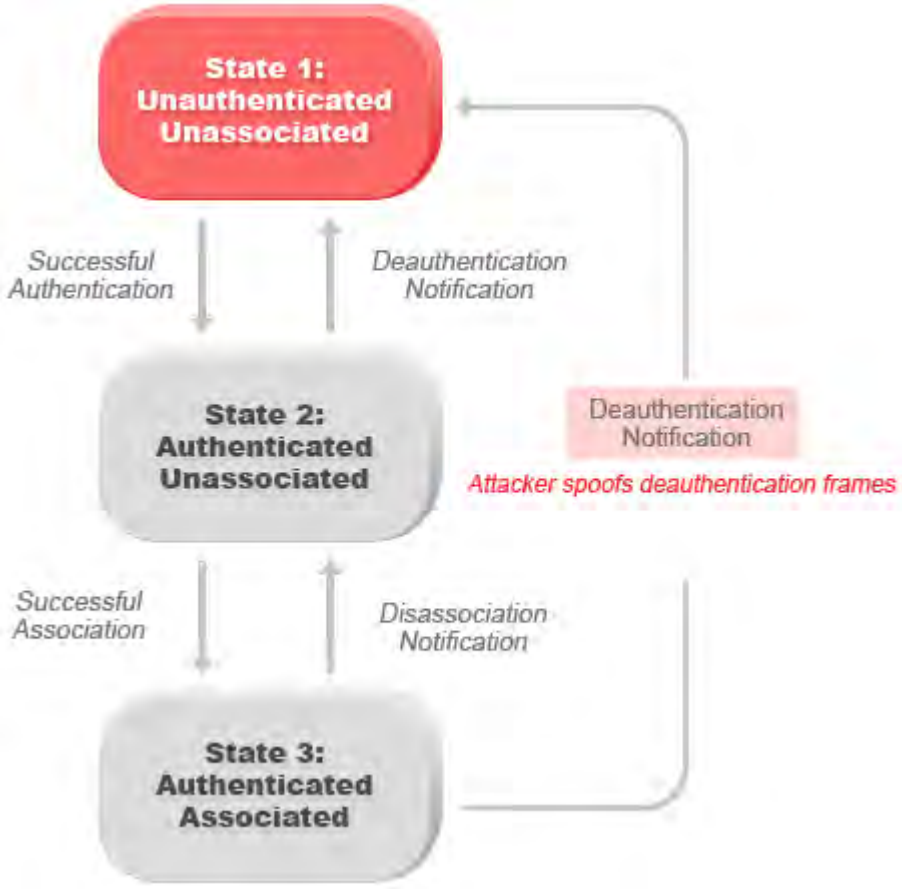
AirMagnet WiFi Analyzer detects this form of DoS attack by detecting spoofed de-authentication frames and tracking client authentication and association states. When the alarm is triggered, the AP under attack will be identified. The WLAN security analyst can log on to the AP to check the current association table status or use AirMagnet Wi-Fi Analyzer active tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: De-Authentication Flood

Potential Attack tools: WLAN Jack, Void11, AirForge

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and APs implement such a state machine (illustrated below) according to the IEEE standard. A successfully associated client station stays in **State 3** in order to continue wireless communication. Client station in **State 1** and **State 2** can not participate in WLAN data communication until it is authenticated and associated to **State 3**.



Attacker spoofs 802.11 de-authentication frames from AP to client station to bring client to state 1

A form of denial-of-service attack aims to send a client of an AP to the unassociated/unauthenticated **State 1** by spoofing de-authentication frames from the AP to the client unicast address. With today's client adapter implementations, this form of attack is very effective and immediate in terms of disrupting wireless services against the client. Typically, client stations would re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame. An attacker would repeatedly spoof the de-authentication frames to keep all clients out of service.

AirMagnet Solution

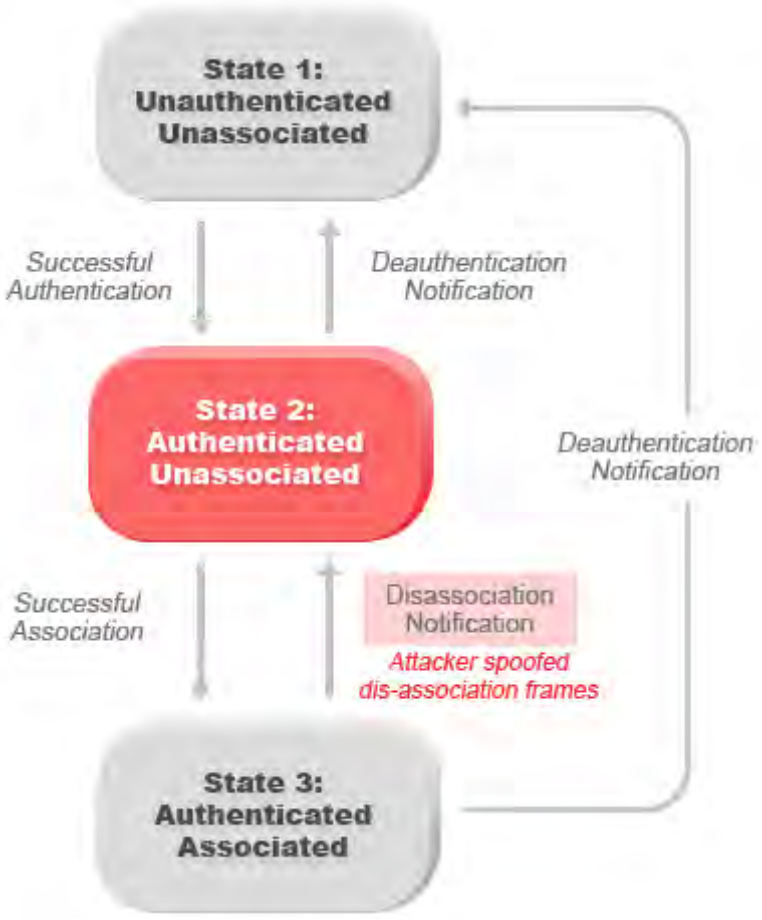
AirMagnet WiFi Analyzer detects this form of DoS attack by detecting spoofed de-authentication frames and tracking client authentication and association states. When the alarm is triggered, the AP and client under attack will be identified. The WLAN security officer can log on to the AP to check the current association table status or use the AirMagnet Wi-Fi Analyzer active tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: Disassociation Broadcast

Potential Attack tools: ESSID Jack, WLAN Jack

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and APs implement such a state machine (illustrated below) according to the IEEE standard. A successfully associated client station stays in **State 3** in order to continue wireless communication. Client station in **State 1** and **State 2** can not participate in WLAN data communication until it is authenticated and associated to **State 3**.



Attacker spoofs 802.11 disassociation frames from AP to broadcast address to force all clients to state 2

A form of denial-of-service attack aims to send a client of an AP to the unassociated/authenticated **State 2** by spoofing disassociation frames from the AP to the broadcast address (all clients). With today's client adapter implementations, this form of attack is very effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations would re-associate to regain service until the attacker sends another disassociation frame. An attacker would repeatedly spoof the disassociation frames to keep all clients out of service.

AirMagnet Solution

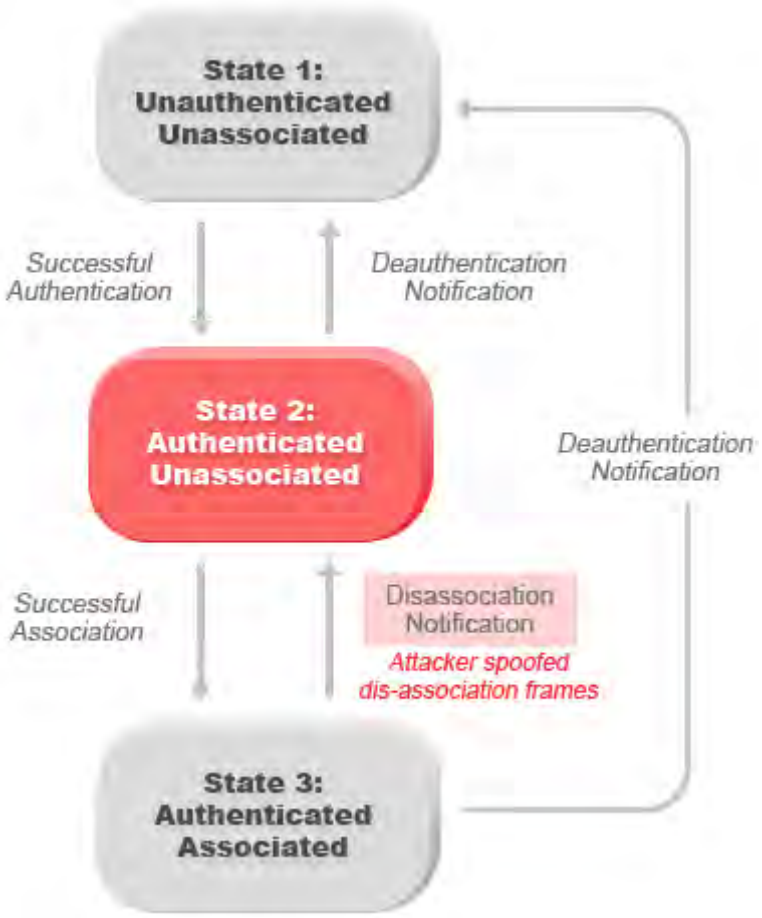
AirMagnet WiFi Analyzer detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the AP under attack will be identified. The WLAN security officer can log on to the AP to check the current association table status or use the AirMagnet Wi-Fi Analyzer active Tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: Disassociation Flood

Potential Attack tools: ESSID Jack, WLAN Jack

Alarm Description & Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and APs implement such a state machine (illustrated below) according to the IEEE standard. A successfully associated client station stays in **State 3** in order to continue wireless communication. Client station in **State 1** and **State 2** can not participate in WLAN data communication until it is authenticated and associated to **State 3**.



Attacker spoofs 802.11 disassociation frames from AP to client station to bring client to state 2

A form of denial-of-service attack aims to send a client of an AP to the unassociated/authenticated **State 2** by spoofing disassociation frames from the AP to a client. With today's client adapter implementations, this form of attack is very effective and immediate in terms of disrupting wireless services against this client. Typically, client stations would re-associate to regain service until the attacker sends another disassociation frame. An attacker would repeatedly spoof the disassociation frames to keep the client out of service.

AirMagnet Solution

AirMagnet WiFi Analyzer detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the AP under attack will be identified. The WLAN security officer can log on to the AP to check the current association table status or use the AirMagnet WiFi Analyzer active Tools (Diagnostics, DHCP, Ping) to test the wireless service provided by this AP.

Denial-of-Service Attack: RF Jamming Attack

Alarm Description & Possible Causes

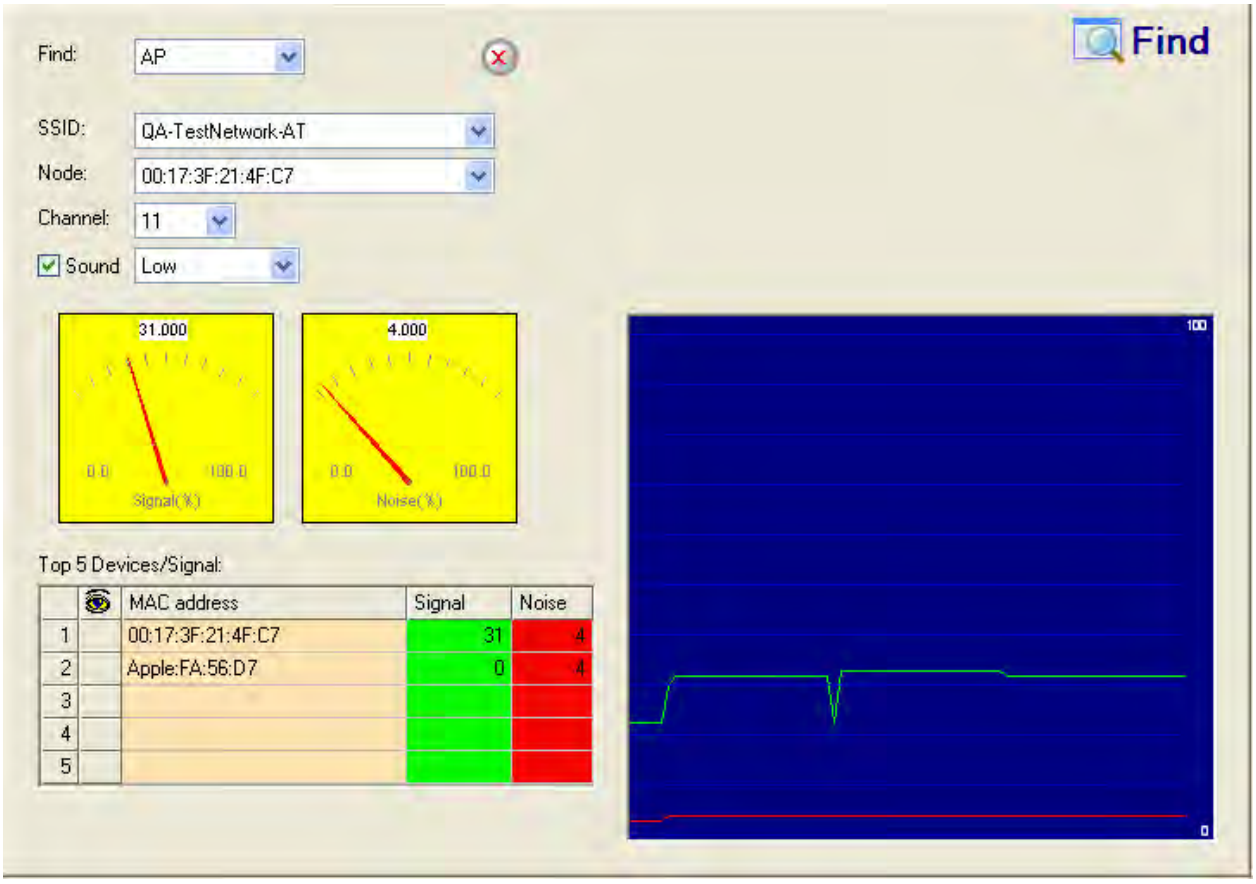
WLAN reliability and efficiency depend on the quality of the RF media. Be it 802.11b/g at 2.4GHz or 802.11a at the 5GHz RF spectrum, they are all susceptible to RF noise impact. An attacker leveraging this WLAN vulnerability can perform two types of Denial-of-Service attacks:

- **Disrupt WLAN service:** At the 2.4GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4GHz or 5GHz spectrum with a high gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a one kilo-watt jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same one kilo-watt jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.
- **Physically damage AP hardware:** An attacker using a high output transmitter with directional high gain antenna 30 yards away from an AP can pulse enough high energy RF power to damage electronics in the AP resulting in it being permanently out of service. Such **HERF** (high energy RF) guns have been demonstrated to work and cost very little to build.

AirMagnet Solution

AirMagnet WiFi Analyzer detects continuous RF noise over a certain threshold for a potential RF jamming attack. A reported RF jamming attack can be further investigated by tracking down the noise source using the AirMagnet **Find** tool with an external directional antenna.

Tracking down noise source of RF jamming attack using the AirMagnet Handheld Analyzer on a Pocket PC



AirMagnet Wi-Fi Analyzer's Find tool locates devices by tracking their signal level

Dictionary Attack on EAP Methods

Alarm Description & Possible Causes

IEEE **802.1x** provides an **EAP** (Extensible Authentication Protocol) framework for wired or wireless LAN authentication. An **EAP** framework allows flexible authentication protocol implementation. Wireless vendors supporting 802.1x or WPA implement authentication protocols such as **LEAP**, **MD5**, **OTP** (one-time-password), **TLS**, **TTLS**, and so on Some of these authentication protocols are based upon the user name and password mechanism, where the user name is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker would gain the user name from the unencrypted **802.1x** identifier protocol exchange. The attacker then tries to guess a user's password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or concatenation of words or names with a minor modification such as a trailing digit or two.

A dictionary attack can take place online actively, where an attacker repeatedly tries all the possible password combinations. **Online** dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (**RADIUS** servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place **off-line**, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations off-line. Unlike online attacks, off-line attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an off-line attack tool's success.

AirMagnet Solution

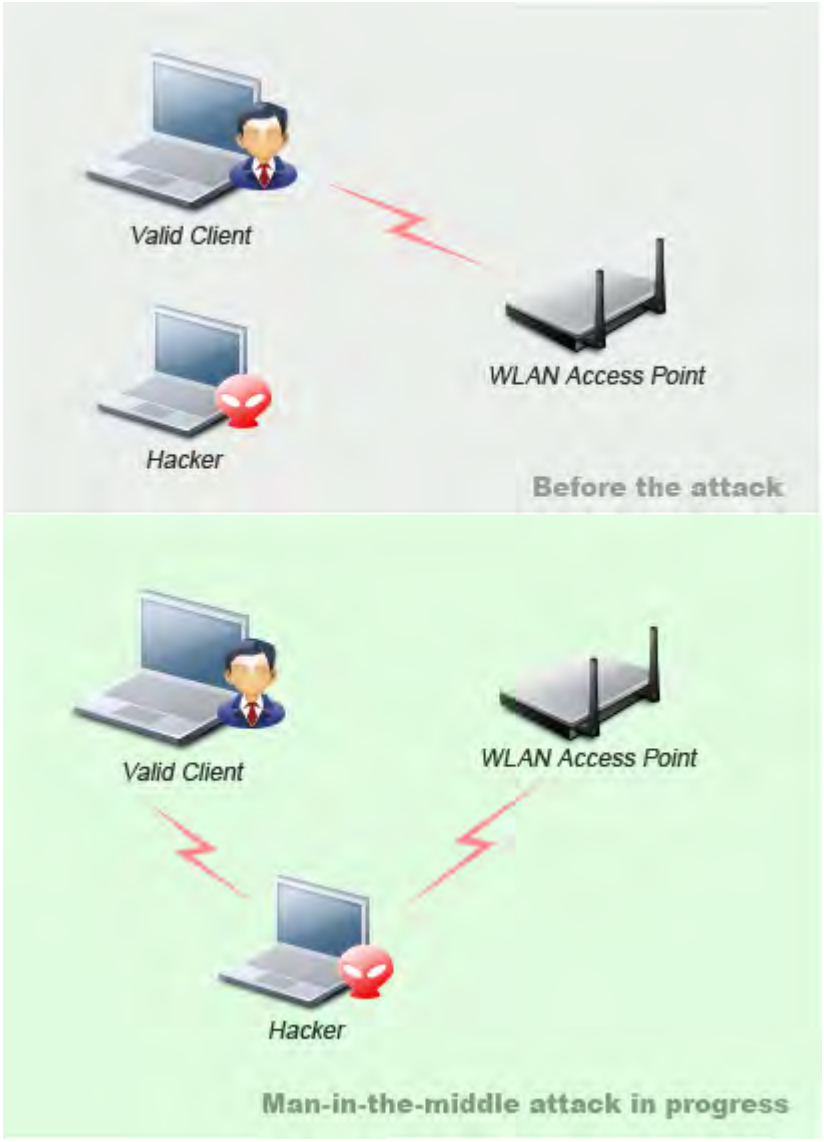
AirMagnet WiFi Analyzer detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. Upon detection of a dictionary attack, the AirMagnet WiFi Analyzer alarm message identifies the user name and attacking station's MAC address. AirMagnet advises switching user name and password-based authentication methods to encrypted tunnel-based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors, including Cisco.

Man-in-the-Middle Attack Detected

Potential Attack tool: Monkey Jack

Alarm Description & Possible Causes

Man-in-the-Middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use an 802.11 wireless analyzer and monitor 802.11 frames sent over the wireless LAN. By capturing the wireless frames during the association phase, the hacker can get the IP and MAC address information about the wireless client card and access point, the association ID for the client, and the SSID of the wireless network.



Commonly used Man-in-the-Middle attack

The most commonly used method at this time for performing the Man in the Middle attack involves the hacker sending spoofed disassociation or de-authentication frames. After that, the hacker station will spoof the MAC address of the client in order to continue being associated to the AP. At the same time, the hacker will set up a spoofed AP in another channel to keep the client associated. Now, all traffic between the valid client and AP will pass through the hacker's station. One of the most commonly used Man-in-the-Middle attack tools is Monkey-Jack.

AirMagnet Solution

AirMagnet WiFi Analyzer recommends the use of strong encryption and authentication mechanisms to thwart any Man-in-the-middle attacks by hackers. One way to avoid such an attack is to prevent MAC spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Device Using Shared Key Authentication

Alarm Description & Possible Causes

The IEEE 802.11 standard designed the Shared Key Authentication protocol to work with static **WEP** key encryption to lock out unauthorized WLAN devices from associating with an AP or ad-hoc station. It is a simple 4-packet exchange challenge/response protocol as illustrated below:

Shared key authentication 4-packet protocol exchange

Shared key authentication uses a standard challenge and response approach for authentication between the 802.11 client and the access point. The challenge text is unencrypted and in clear text. The algorithm (not the shared secret key) for the challenge response is standard and public knowledge. It has been proven that shared key authentication can be easily exploited through a passive attack by eavesdropping. An attacker can use brute force to compute the challenge response off-line after capturing challenge text, which is in clear text. Once the match is found, the attacker has acquired the shared secret key. See the paper "***Your 802.11 Wireless Network has No Clothes"*** published by University of Maryland, which highlights some of the security problems including the shared key vulnerability in wireless LANs.

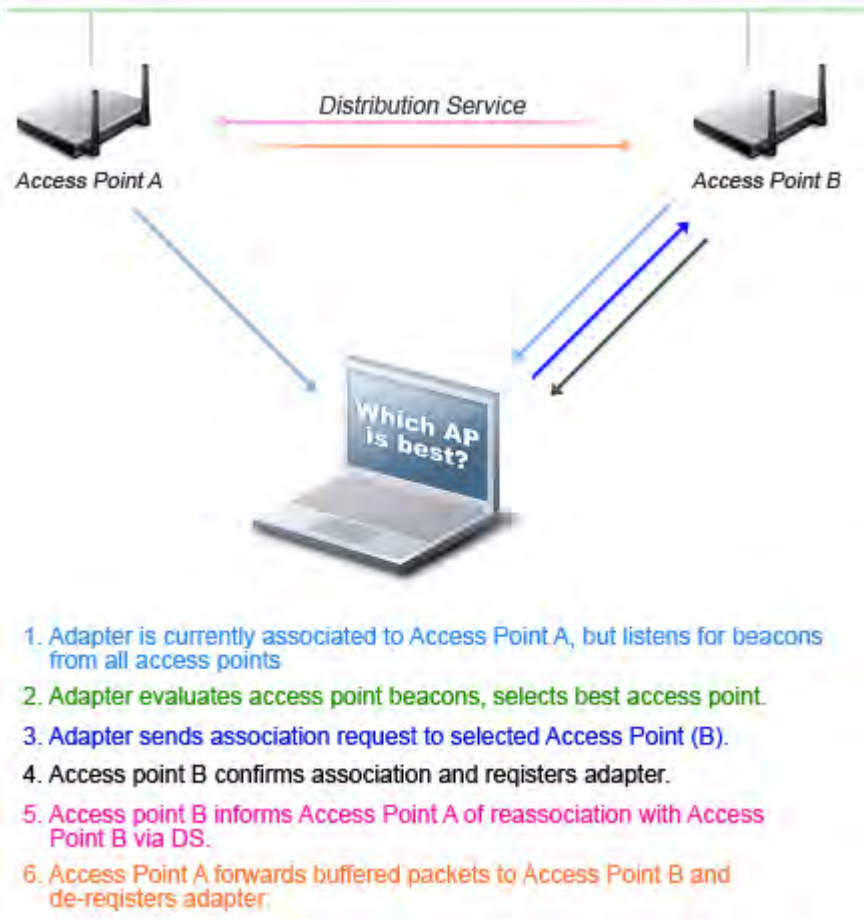
AirMagnet Solution

AirMagnet WiFi Analyzer detects the use of Shared Key Authentication and advises alternatives. Many enterprises today deploy 802.11 WLANs using **Open Authentication** instead of **Shared Key Authentication** with a higher level authentication mechanism provided by **802.1x** and **EAP** methods such as **LEAP**, **PEAP**, **TLS**, and so on.

Excessive Roaming or Re-Associations

Alarm Description & Possible Causes

After successfully associating with an AP, WLAN client devices start using the wireless connection for communication but continue to search for better wireless services (such as another AP with stronger signal strength, less channel noise, or higher supported speed).



A Wireless Client Roams to the Best AP for Quality Communication

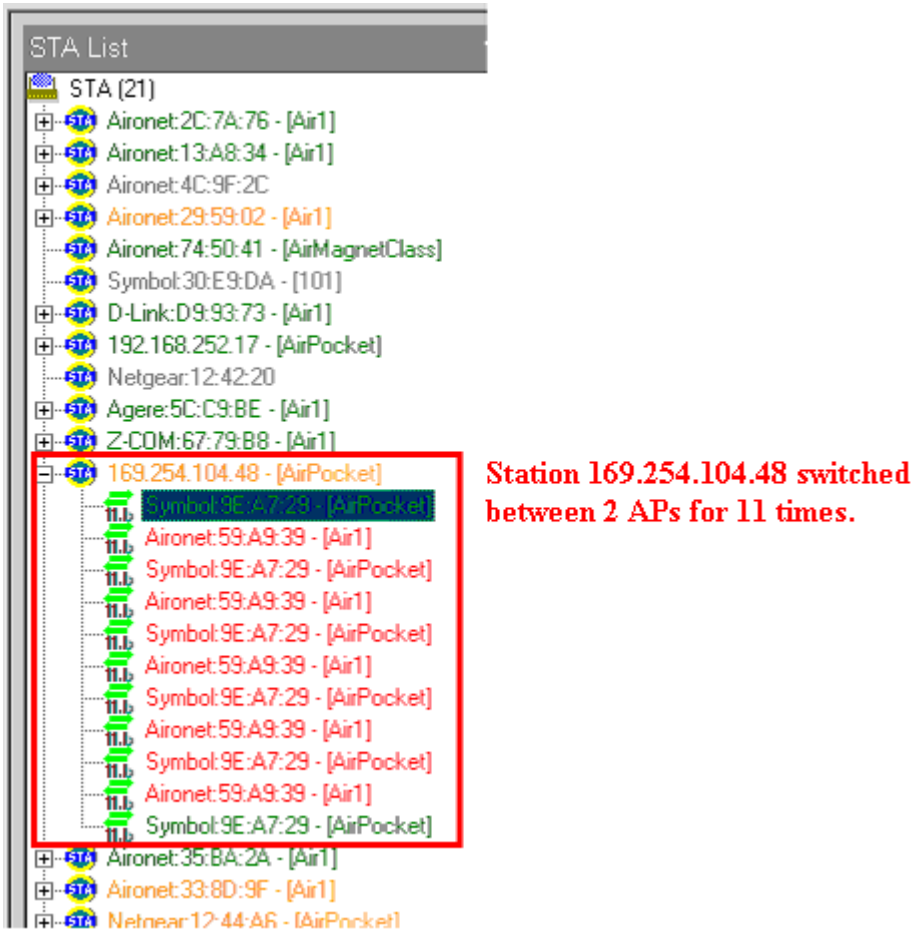
Once an AP with better service is identified, the client station will associate with the new AP and break the association with the original AP. Mobile roaming devices such as VoIP phones and bar code scanners on a WLAN frequently perform such a re-association act. With more advanced WLAN management technologies (such as the ones listed below), client stations are increasingly likely to change association to adjust to the dynamic RF environment:

- AP load balancing and bandwidth allocation
- Dynamic channel selection to avoid RF interference and dedicated channel bandwidth
- Automatic AP output power adjustment for optimized coverage and capacity

All these technologies are designed to improve WLAN efficiency; however, vendor implementations and fine-tuning are not on par with each other. Immature new products may cause confused client stations to frequently re-associate, thus resulting in disrupted service.

AirMagnet Solution

Stationary devices such as wireless printers and wireless desktops are not expected to have repeated re-associations. AirMagnet Wi-Fi Analyzer watches out for the anomaly of excessive client re-associations by tracking association counts and APs. Once detected and reported by AirMagnet WiFi Analyzer, this problem can be further investigated by using the station list on the Infrastructure page to display APs and session characteristics involved (refer to the illustration below).



Using the Infrastructure Page *station List* to investigate excessive roaming problem

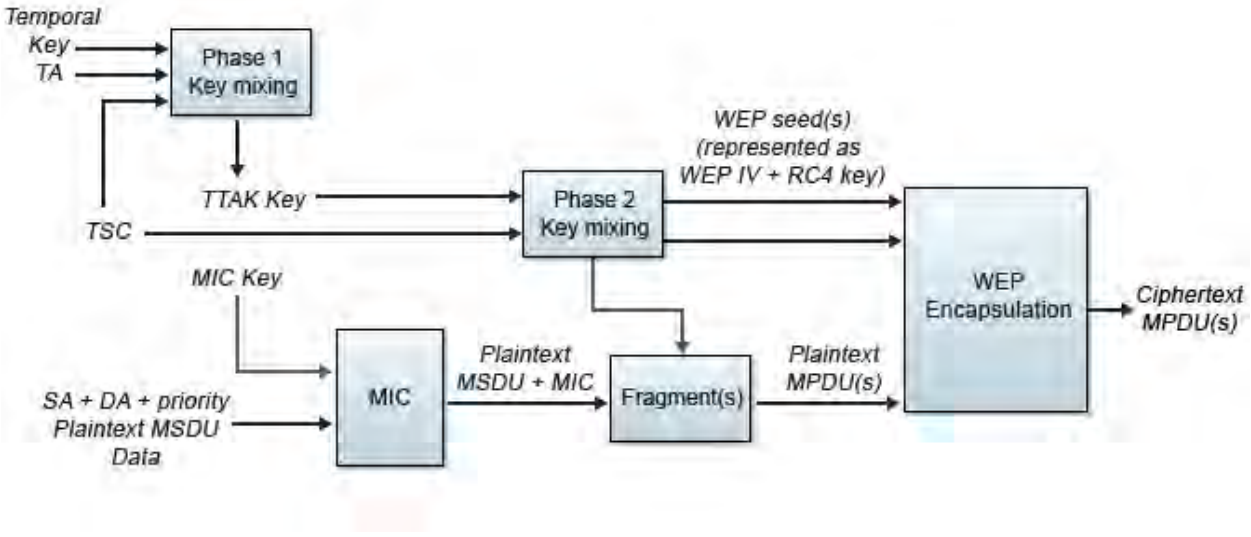
Policy - RTS frames not responded to by CTS

RTS (Request-To-Send) is usually responded to by a CTS (Clear-To-Send) and then followed by the actual data transmission. Without receiving the CTS frame, the station is unable to transmit data therefore breaking wireless communication.

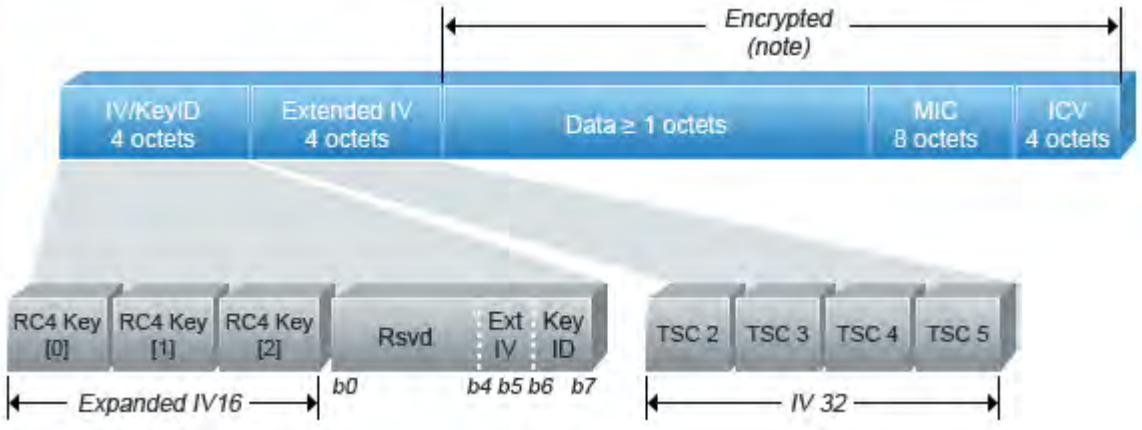
Device Unprotected by TKIP

Alarm Description & Possible Causes

The latest **IEEE 802.11i** standard includes **TKIP** (Temporal Key Integrity Protocol) and **MIC** (Message Integrity Checksum) as recommended data privacy protocols. The **Wi-Fi Alliance** also recommends **TKIP** and **MIC** in its **WPA** (Wireless Protected Access) specification. WLAN traffic encrypted with TKIP and MIC defeats packet forgery and replay attacks. Most importantly, TKIP is immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with **MIC, TKIP** also provides per-packet key mixing, which helps prevent many keystream attacks.



TKIP and MIC encryption algorithm addresses the weakness of static WEP as well as defeating packet forgery and replay attack



TKIP and MIC encrypted frames expands the original data by 20 bytes for stronger encryption and integrity check

Unlike **AES-**based **CCMP** encryption, TKIP typically does not require a hardware upgrade. Many WLAN equipment vendors (including Cisco) have added TKIP and MIC support in their latest firmware and drivers.

AirMagnet Solution

AirMagnet WiFi Analyzer detects WLAN traffic that is not protected by TKIP encryption and raises an alarm for attention. AirMagnet WiFi Analyzer advises updating these devices to their latest firmware and re-configuring them to include TKIP encryption.

Access Point Down

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer monitors the radio emissions of all APs in order to help maintain WLAN health. Wireless service is often disrupted due to a failure in APs for reasons such as power failure, damaged antenna, blocked radio transmission, and so on This alarm will trigger whenever an AP goes down for any reason.

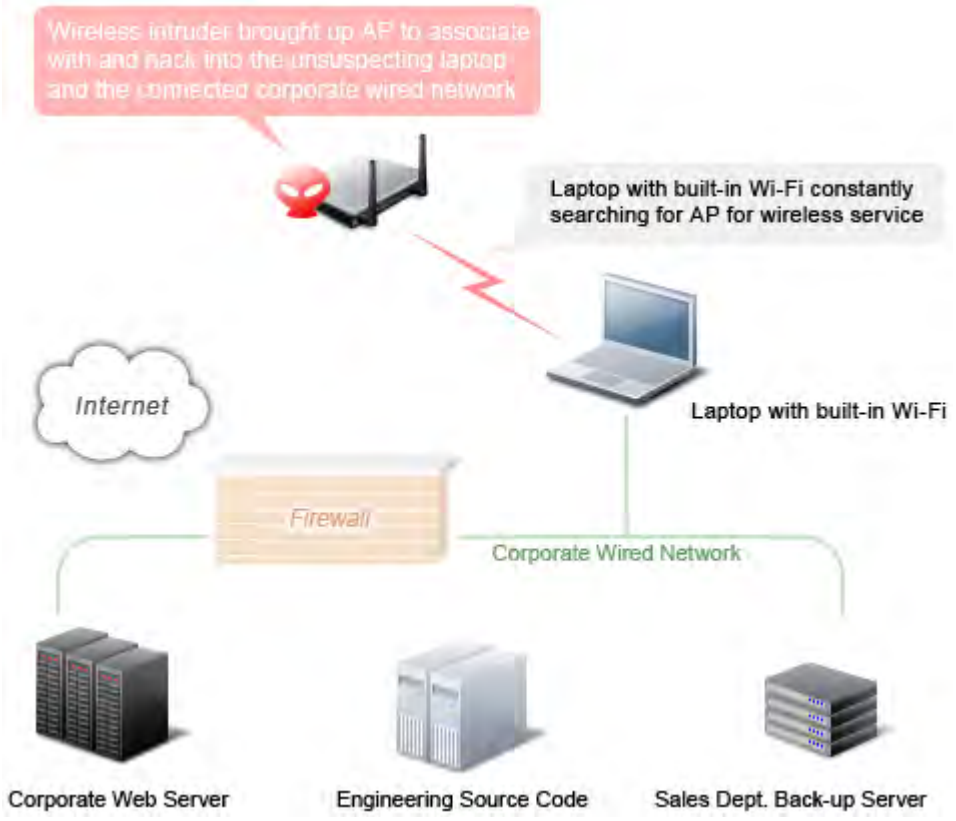
AirMagnet Solution

If AirMagnet WiFi Analyzer is given the AP list, which is the same list used for rogue AP detection, it can generate alarms when any one of the listed APs is not heard by any of the AirMagnet SmartEdge sensors. This alarm is of utmost importance to the wireless administrator's ability to provide uninterrupted coverage to the wireless clients in the enterprise.

Exposed Wireless Station Detected

Alarm Description & Possible Causes

The popularity of WLANs results in user laptops with multiple WLAN configuration profiles to be used in various environments, such as an enterprise office, home, or a wireless hotspot. Typically, all these different configuration profiles are with set up with different levels of security settings. For example, an enterprise office may use the strongest authentication and encryption while home or hotspot configurations may likely use virtually no authentication or encryption. Choosing among these configuration profiles with different security settings may be automatic or manual depending upon the vendor implementation. This can create a potential security vulnerability if an attacker learns these profile settings while the client is searching for service. After learning the user profiles, an attacker can bring up an AP advertising for the desired service (SSID) to lure the client for association. Once the unsuspecting user station has associated, the attacker gains network access to the client station.



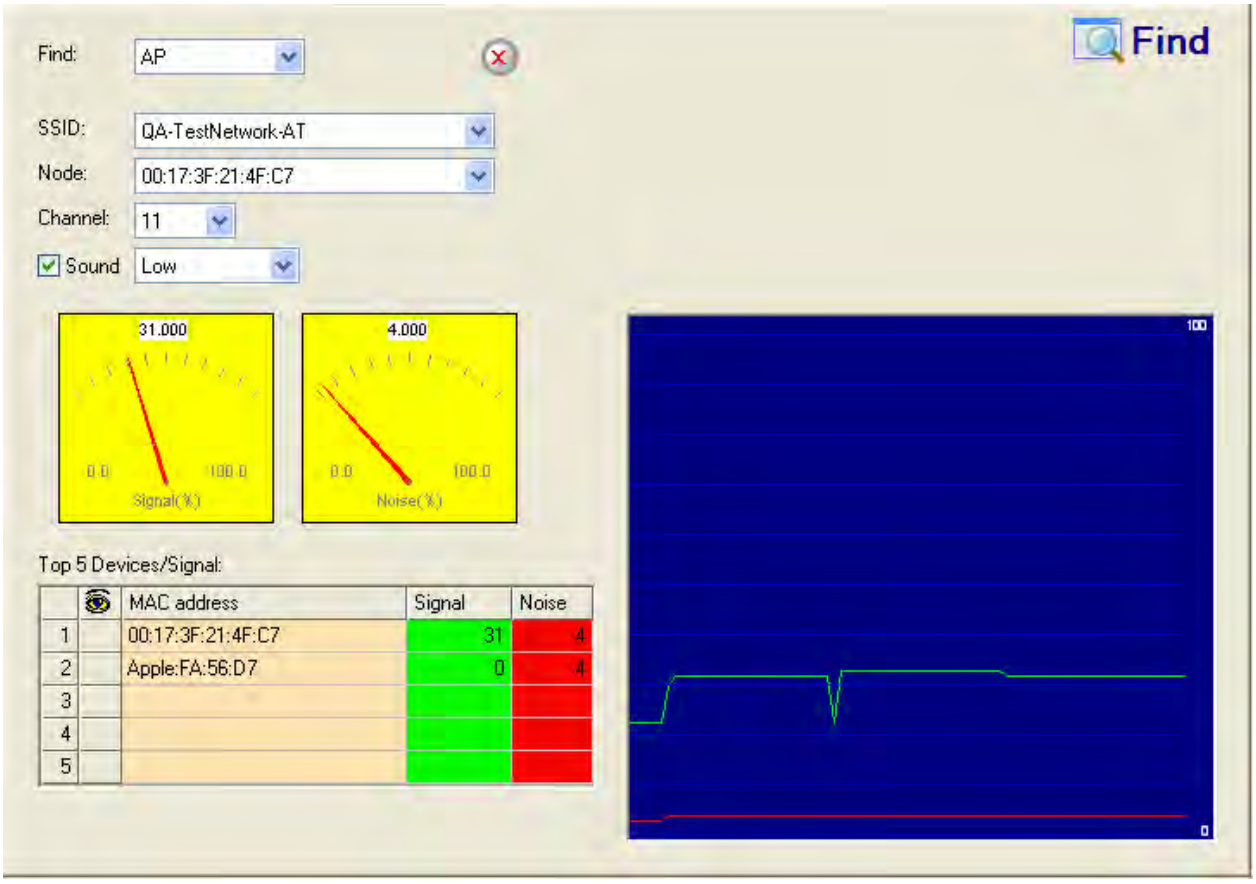
A laptop PC with an open WLAN connection risks exposing data on the laptop and the corporate wired network

AirMagnet WiFi Analyzer detects client stations that constantly search for association, thus leaving themselves vulnerable. Typically, they are client stations mis-configured manually or automatically by the vendor profile selector. This scenario is even more dangerous for an enterprise where the use of wireless is prohibited. The common way this threat takes form is:

- A laptop with built-in Wi-Fi is used at home with minimal or no wireless security.
- The same laptop is used at work where no WLAN is allowed.
- The laptop is connected to the enterprise wired LAN for connectivity.
- The laptop's built-in Wi-Fi card continues to search for service all day.
- An attacker puts up an AP to associate with the laptop.
- Once associated, the attacker gains access to the laptop.
- Since the laptop is also connected to enterprise wired LAN, it puts the wired network at risk.

AirMagnet Solution

Stations that are exposed and are part of the ACL (Access Control List) should be located using the FIND tool and the WLAN administrator should notify the owner or take appropriate action as per the company's security policy.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Device Unprotected by PEAP

Alarm Description & Possible Causes

AirMagnet WiFi Analyzer monitors on **802.1x** transactions and their specific **EAP** (Extensible Authentication Protocol) types. Among all EAP types (such as **PEAP**, **TLS**, **TTLS**, **LEAP**, **OTP**, and so on), **PEAP** (Protected EAP) is especially noteworthy. By adopting PEAP as your authentication method, your 802.1x security authentication protocol will be better protected by TLS (Transport Layer Security). EAP methods running within PEAP are provided with built-in advantages regarding:

- identity protection
- dictionary attack resistance
- protection negotiation from replay attack
- header protection
- protected termination from packet spoofing, flooding, and denial-of-service attack

- fragmentation and re-assembly
- fast reconnection
- proven and method independent key management

Many WLAN equipment vendors (including Cisco) have recently added support for PEAP with a firmware upgrade.

AirMagnet Solution

You can rely on this AirMagnet WiFi Analyzer alarm to alert you of devices that are not using PEAP. Please ensure that the PEAP authentication method is implemented on all devices in the wireless environment.

802.11g AP with Short Slot Time

Alarm Description & Possible Causes

The IEEE 802.11g **short-slot-time** mechanism (**9** microsecond slot time), if used on a pure 802.11g deployment, improves WLAN throughput by reducing the wait time for a transmitter to assure clear channel assessment. According to the IEEE 802.11g specification section 7.3.1.4, an AP shall advertise **long-slot-time** (**20** microsecond slot time) in its beacon once there is an associated station such as an 802.11b device which does not support **short-time-slot**. In cases where this specification is not followed (many 802.11g devices have been known to violate this rule), the impact is uncoordinated and potentially overlapping transmissions resulting in frame collisions and reduced throughput.

AirMagnet Solution

AirMagnet WiFi Analyzer tracks WLAN devices in their ability to support the **short-time-slot** mechanism. Once it detects an AP advertising for **short-time-slot** operation despite the existence of devices incapable of supporting it, an 802.11g performance alarm is raised to alert the network administrator of the potential degradation that may result.

802.11g AP Beacons Wrong Protection

Alarm Description & Possible Causes

In an 802.11b and 802.11g mixed WLAN environment, IEEE 802.11g specifies protection mechanisms to keep 802.11g and 802.11b devices from interfering with each other. Since a pure 802.11b device (using CCK modulation) cannot detect an 802.11g signal (using OFDM modulation) in the same 2.4GHz operating spectrum, the 802.11b device may transmit over an 802.11g OFDM transmission, causing packet collisions. The IEEE 802.11g standard specifies two protection mechanisms to resolve this issue: **RTS/CTS** and **CTS-to-self**. It is controlled by the 802.11g AP, which advertises and triggers the use of a protection mechanism. Because using a protection mechanism can compromise network performance,

IEEE 802.11g does not specify the use of protection mechanisms in a .11b and .11g mixed environment as a **must**. It is, however, a very important 802.11g deployment decision. Generally speaking, turning off a protection mechanism is only beneficial when there is a very small amount of 802.11b traffic.

In an environment when protection is truly needed, malfunctioning or mis-configured APs without advertising protection mechanisms can degrade performance significantly. It has been observed that many pre-802.11g-standard APs do not implement a protection mechanism (and even many that do implement one do so incorrectly). Even when a vendor implementation is correct, a user can still configure the protection mechanism incorrectly by turning it off when it is needed.

AirMagnet Solution

AirMagnet WiFi Analyzer observes and tracks 802.11b and 802.11g co-existence status in a channel. When the protection mechanism is turned off by an AP for a b/g mixed mode deployment, it raises an alarm for further investigation. You can use the AirMagnet Wi-Fi Analyzer's Channel screen to profile your 802.11g and 802.11b traffic load to decide on a protection mechanism configuration.

802.11g Protection Mechanism not Implemented

Alarm Description & Possible Causes

In an 802.11b and 802.11g mixed WLAN environment, IEEE 802.11g specifies protection mechanisms to keep 802.11g and 802.11b devices from interfering with each other. Since a pure 802.11b device (using CCK modulation) cannot detect an 802.11g signal (using OFDM modulation) in the same operating 2.4GHz spectrum, the 802.11b device may transmit over an 802.11g OFDM transmission causing packet collisions. The IEEE 802.11g standard specifies two protection mechanisms to resolve this issue: **RTS/CTS** and **CTS-to-self**. It is controlled by the 802.11g AP, which advertises and triggers the use of a protection mechanism. 802.11g client stations must follow the AP's advertisement on the usage of the protection mechanism.

AirMagnet Solution

AirMagnet WiFi Analyzer monitors the behavior of 802.11g clients regarding protection mechanism usage. If they violate the advisory from their AP by not using the protection mechanism in a mixed 802.11b and 802.11g WLAN environment, AirMagnet raises this alarm to alert the WLAN administrator for correction. The impact of such a violation may be uncoordinated and potentially overlapping transmissions from 802.11b devices resulting in WLAN (.11b and .11g) frame collisions and reduced throughput. Typical causes of this violation are:

- Pre-802.11g-standard equipment that does not support the protection mechanism
- User configuration error

802.11g Pre-Standard Device

Alarm Description & Possible Causes

While the IEEE 802.11g standard was being defined, several vendors were releasing pre-standard 802.11g products which violated the standard ratified later. A few very important 802.11g features finalized in the late stage were not implemented by these pre-standard vendor devices. These important features include the 802.11b **protection mechanism** and **short-time-slot,** among others.

AirMagnet Solution

Besides watching out for these specific 802.11g feature violations, AirMagnet WiFi Analyzer detects 802.11g pre-standard (802.11g draft) protocol usage to identify pre-standard devices. Once these devices are spotted, AirMagnet Wi-Fi Analyzer advises checking with your equipment manufacturer for the latest AP firmware upgrade to be fully 802.11g compliant and, most importantly, to keep your 802.11b and 802.11g devices from interfering with each other.

802.11g Device Using Non-Standard Data Rate

Alarm Description & Possible Causes

802.11g supports data rates up to 54 Mbps; however, practical data throughput is much lower than 54 Mbps due to inter-frame spacing and the random back-off mechanism to avoid collisions. Proprietary technologies are available from various radio chipset vendors to push the theoretical data rate to 108 Mbps. Implementations of such high-speed transmission include **Super G, Turbo mode, Packet Burst**, and so on.

AirMagnet Solution

AirMagnet WiFi Analyzer can detect the use of non-standard speed settings even if your current WLAN card cannot support such speeds. If you wish to enable such proprietary implementations in your WLAN deployment, consideration should be paid in the following areas:

- Some high-speed implementations use channel-binding technologies, which expand the RF spectrum usage beyond the original 802.11g channel definition (22 MHz per channel). If you enable this feature, you may have to revisit the channel allocation from your initial site survey.
- In order to achieve non-standard high speed communication, APs and clients have to be made by the same device or chipset vendor. In deployments where client devices are from heterogeneous vendors, high speed transmission and bandwidth throughput may not be reliable.

802.11g Protection Mechanism Overhead

Alarm Description & Possible Causes

In an 802.11b and 802.11g mixed WLAN environment, IEEE 802.11g specifies protection mechanisms to keep 802.11g and 802.11b devices from interfering with each other. Since a pure 802.11b device (using CCK modulation) cannot detect an 802.11g signal (using OFDM modulation) in the same 2.4GHz operating spectrum, the 802.11b device may transmit over an 802.11g OFDM transmission, causing packet collisions. The IEEE 802.11g standard specifies two protection mechanisms to resolve this issue: **RTS/CTS** and **CTS-to-self**. It is controlled by the 802.11g AP, which advertises and triggers the use of a protection mechanism. Because using a protection mechanism can compromise network performance, IEEE 802.11g does not specify the use of protection mechanisms in a .11b and .11g mixed environment as a **must**. It is, however, a very important 802.11g deployment decision. Generally speaking, turning off a protection mechanism is only beneficial when there is a very small amount of 802.11b traffic.

Ideally, a WLAN deployment involving 802.11g is much more efficient with only 802.11g devices. Under such 802.11g purity, the protection mechanism for mixed-mode operation is not needed and therefore adds no protection overhead.

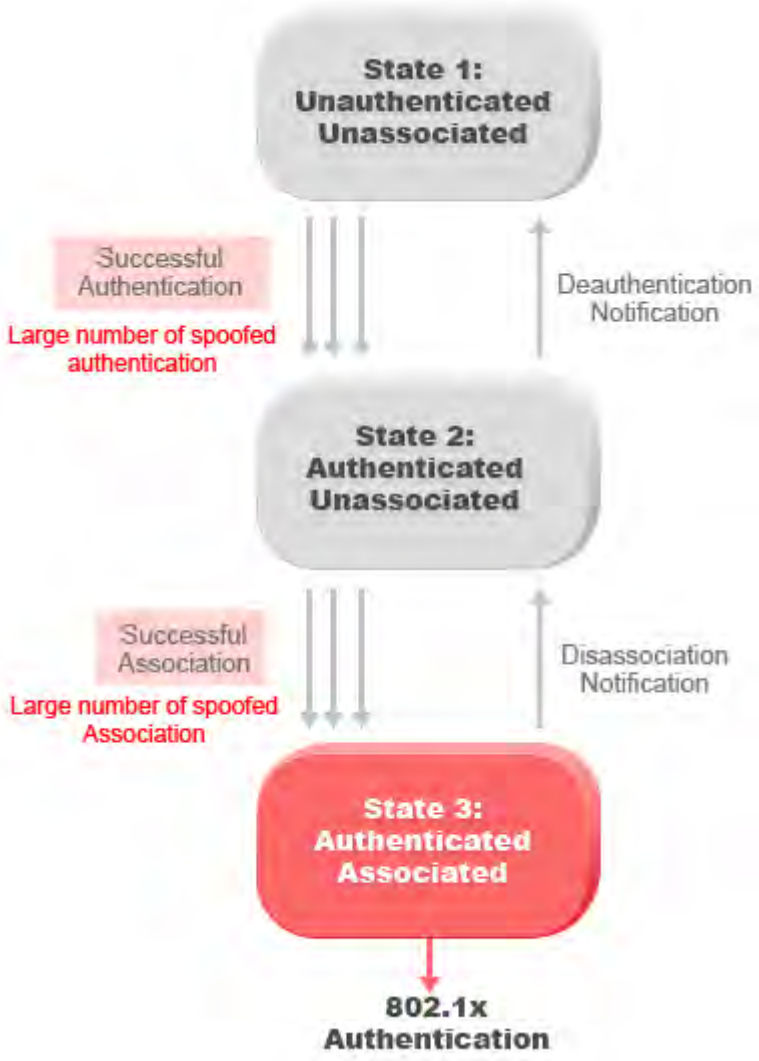
AirMagnet Solution

AirMagnet WiFi Analyzer monitors on such purity and protection mechanism usage. When the protection overhead is re-introduced to a once-pure 802.11g environment, AirMagnet WiFi Analyzer raises an alarm for a purity sweep.

Denial-of-Service Attack: Unauthenticated Association

Alarm Description & Possible Causes

This form of denial-of-service attack attempts to exhaust the AP's resources, particularly the client association table, by flooding the AP with a large number of emulated and spoofed client associations. At the 802.11 layer, **Shared-key** authentication is flawed and rarely used any more. The only other alternative is **Open** authentication (null authentication) that relies on higher-level authentication such as 802.1x or VPN. **Open** authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target AP's client association table by creating many clients reaching **State 3** as illustrated below. Once the client association table overflows, legitimate clients will not be able to get associated, and thus denial-of-serve attack is committed.



Large number of emulated client associations overflow AP's client association table

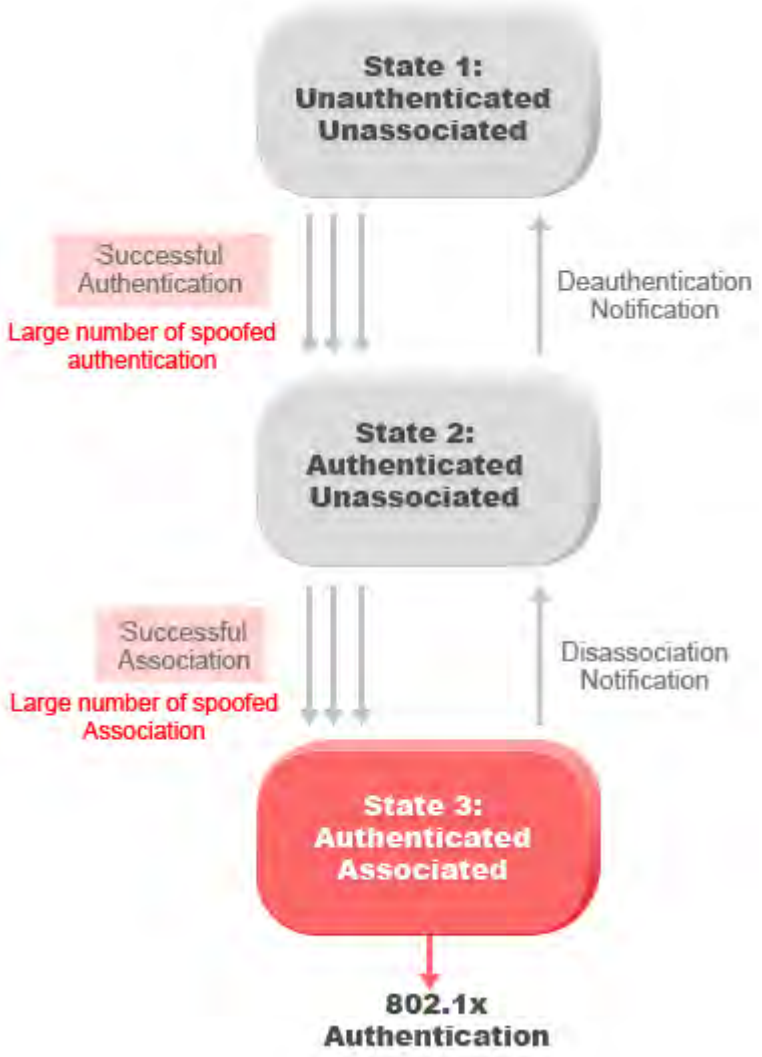
AirMagnet Solution

AirMagnet WiFi Analyzer detects spoofed MAC addresses and tracks the follow-up 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by AirMagnet Wi-Fi Analyzer, you may use the AirMagnet active tools (survey, performance, DHCP) to check if the AP is still functioning properly. You can also log on to this AP to inspect its association table for the number of client associations.

Denial-of-Service Attack: Association Flood

Alarm Description & Possible Causes

One form of denial-of-service attack is to exhaust the AP's resources, particularly the client association table, by flooding the AP with a large number of emulated and spoofed client associations. At the 802.11 layer, **Shared-key** authentication is flawed and rarely used any more. The only other alternative is **Open** authentication (null authentication) that relies on higher-level authentication such as 802.1x or VPN. **Open** authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target AP's client association table by creating many clients reaching **State 3** as illustrated below. Once the client association table overflows, legitimate clients will not be able to get associated, and thus a denial-of-serve attack is committed.



Large number of emulated client associations overflow AP's client association table

AirMagnet Solution

AirMagnet WiFi Analyzer detects spoofed MAC addresses and tracks the follow-up 802.1x actions and data communication after a successful client association to detect this form of

DoS attack. After this attack is reported by AirMagnet WiFi Analyzer, you may use the AirMagnet active tools (survey, performance, DHCP) to check if the AP is still functioning properly. You may also log on to this AP to inspect its association table for the number of client associations.

Rogue AP by IEEE ID (OUI)

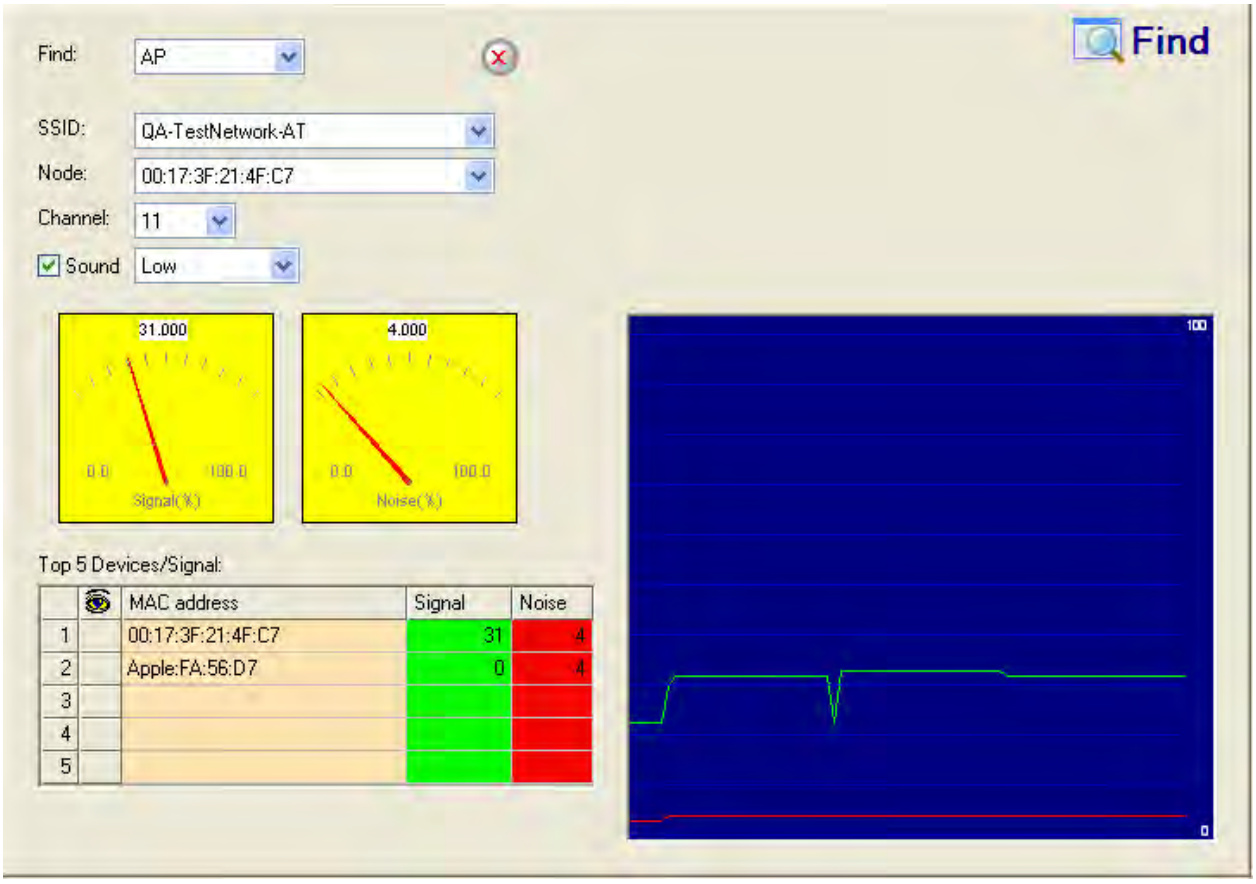
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator of a rogue AP by checking against a pre-configured authorized AP equipment vendor list. For example, if your enterprise has deployed only Cisco Aironet or Symbol Technologies APs, you would then include Cisco and Symbol in the authorized vendor list. After the vendor list is imported, AirMagnet Wi-Fi Analyzer raises a rogue AP alarm whenever an AP is discovered outside of the vendor list, that is, a non-Cisco Aironet or non-Symbol Technologies AP.

Rogue APs installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue AP may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet WiFi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use AirMagnet WiFi Analyzer's FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue Station by IEEE ID (OUI)

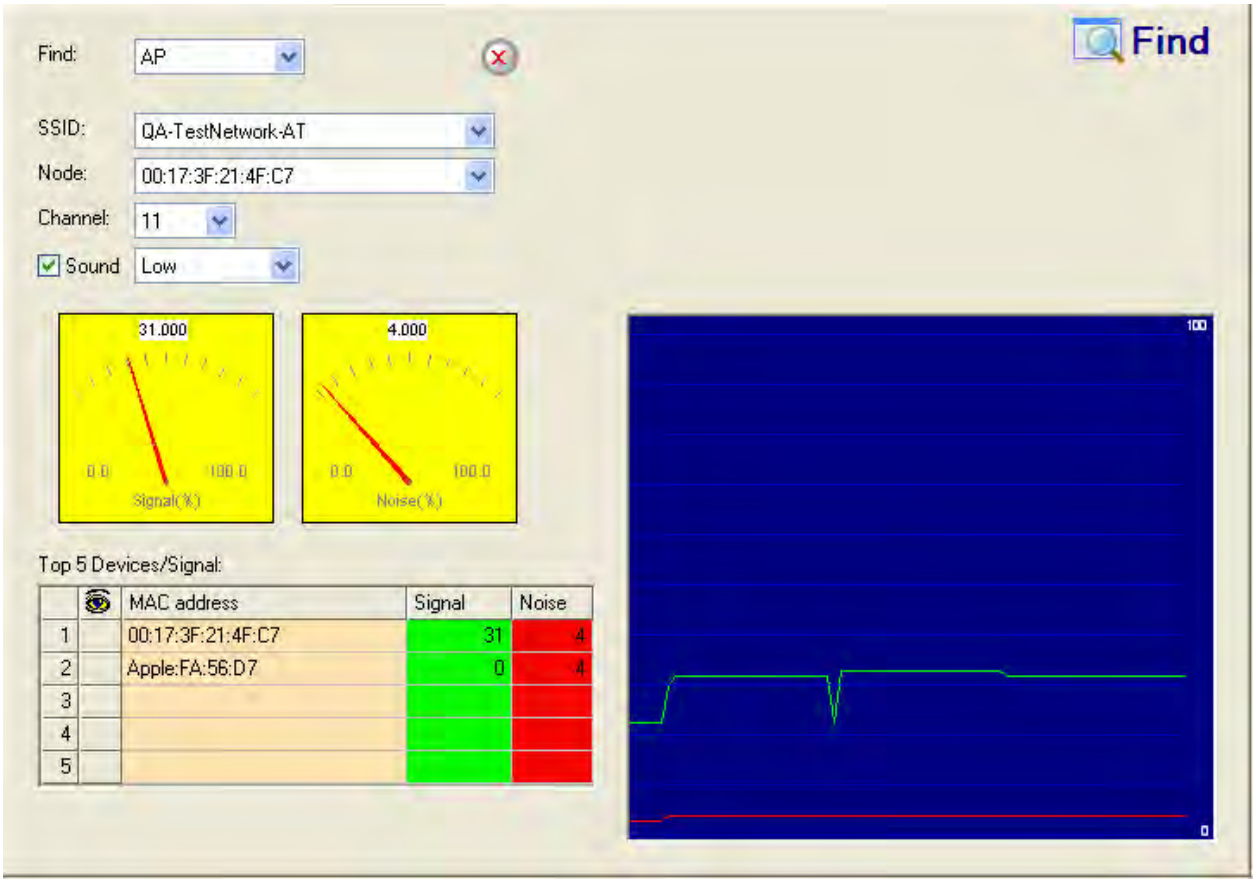
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator of a rogue station by checking against a pre-configured authorized station equipment vendor list. For example, if your enterprise has deployed only Cisco Aironet or Symbol Technologies stations, you would then include Cisco and Symbol in the authorized vendor list. After the vendor list is imported, AirMagnet WiFi Analyzer raises a rogue station alarm whenever a station is discovered outside of the vendor list, that is, a non-Cisco Aironet or non-Symbol Technologies station.

Rogue stations installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue station may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet Wi-Fi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue station is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue AP by SSID

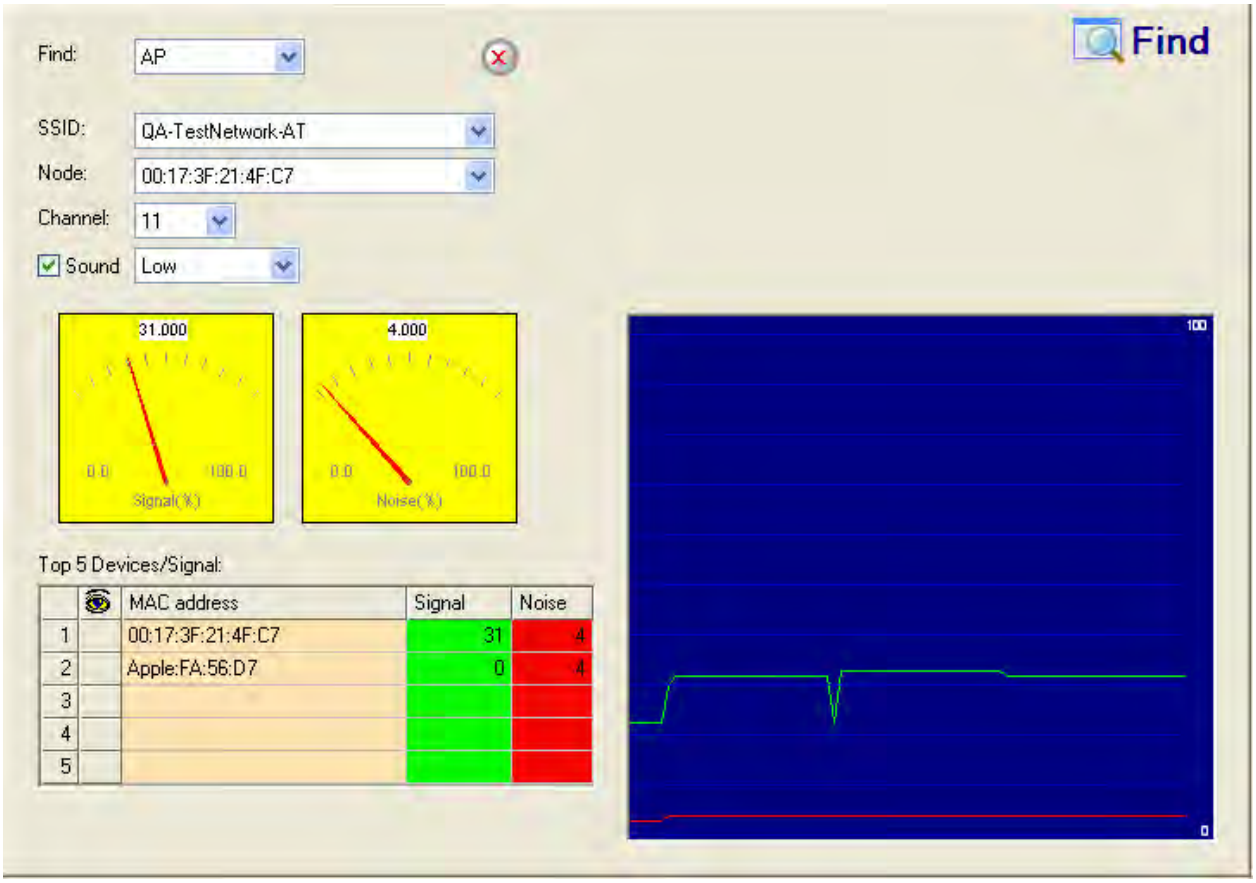
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator of a rogue AP by checking against a pre-configured authorized SSID list. For example, if your enterprise-deployed WLAN is configured only with *MyOfficeWlan* and *MyVoIPWlan*, you would then include these two SSIDs in the authorized SSID list. After this list is imported, AirMagnet WiFi Analyzer raises a rogue AP alarm when an AP operating in a different SSID is discovered.

Rogue APs installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue AP may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet Wi-Fi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue Station by SSID

Alarm Description & Possible Causes

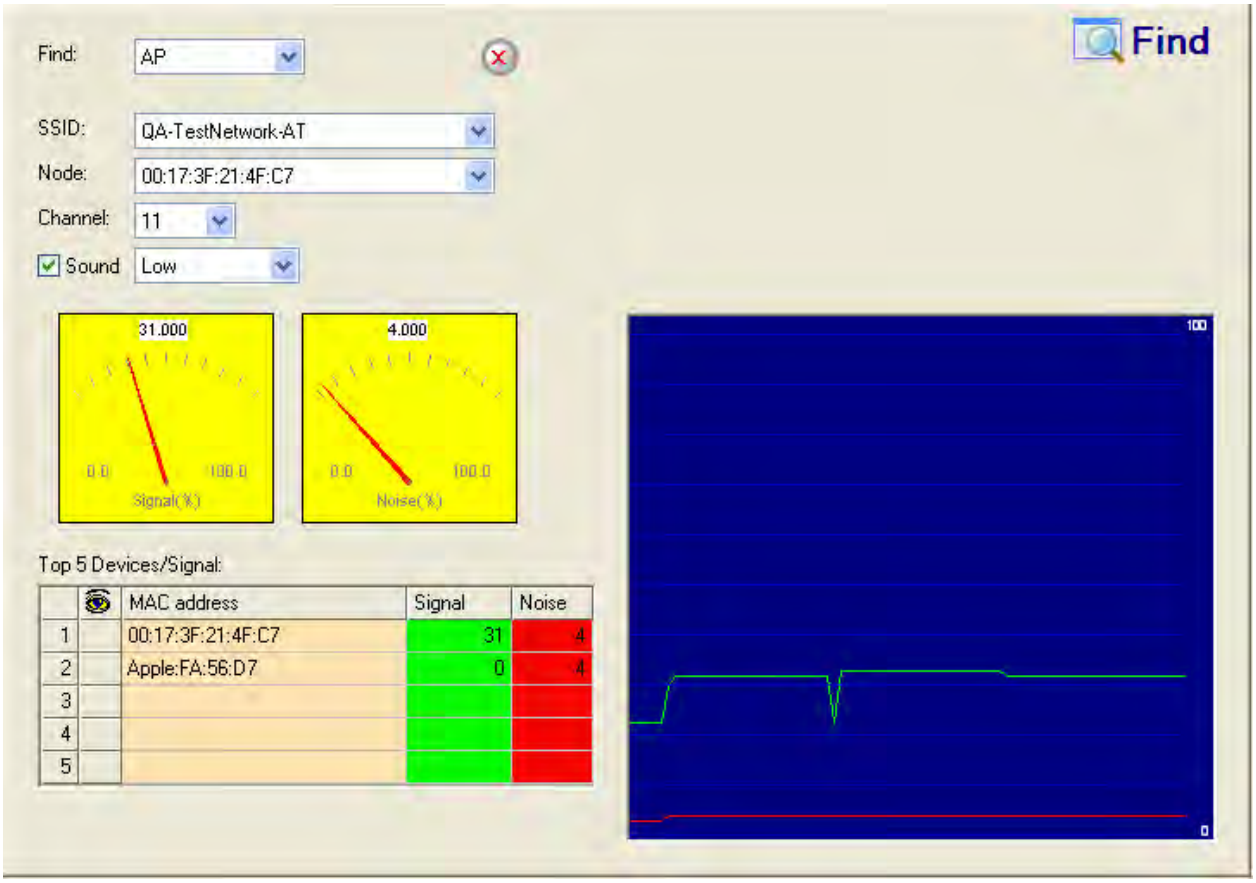
AirMagnet WiFi Analyzer alerts the WLAN administrator of a rogue station by checking against a pre-configured authorized SSID list. For example, if your enterprise-deployed WLAN is configured only with *MyOfficeWlan* and *MyVoIPWlan*, you would then include these two SSIDs in the SSID list. AirMagnet WiFi Analyzer raises a rogue station alarm when a station operating in a different SSID is discovered.

Rogue stations installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue station may also indicate malicious intruders attempting to hack into the

enterprise wired network. Rogue devices discovered by AirMagnet Wi-Fi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue station is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue AP by Wireless Media Type

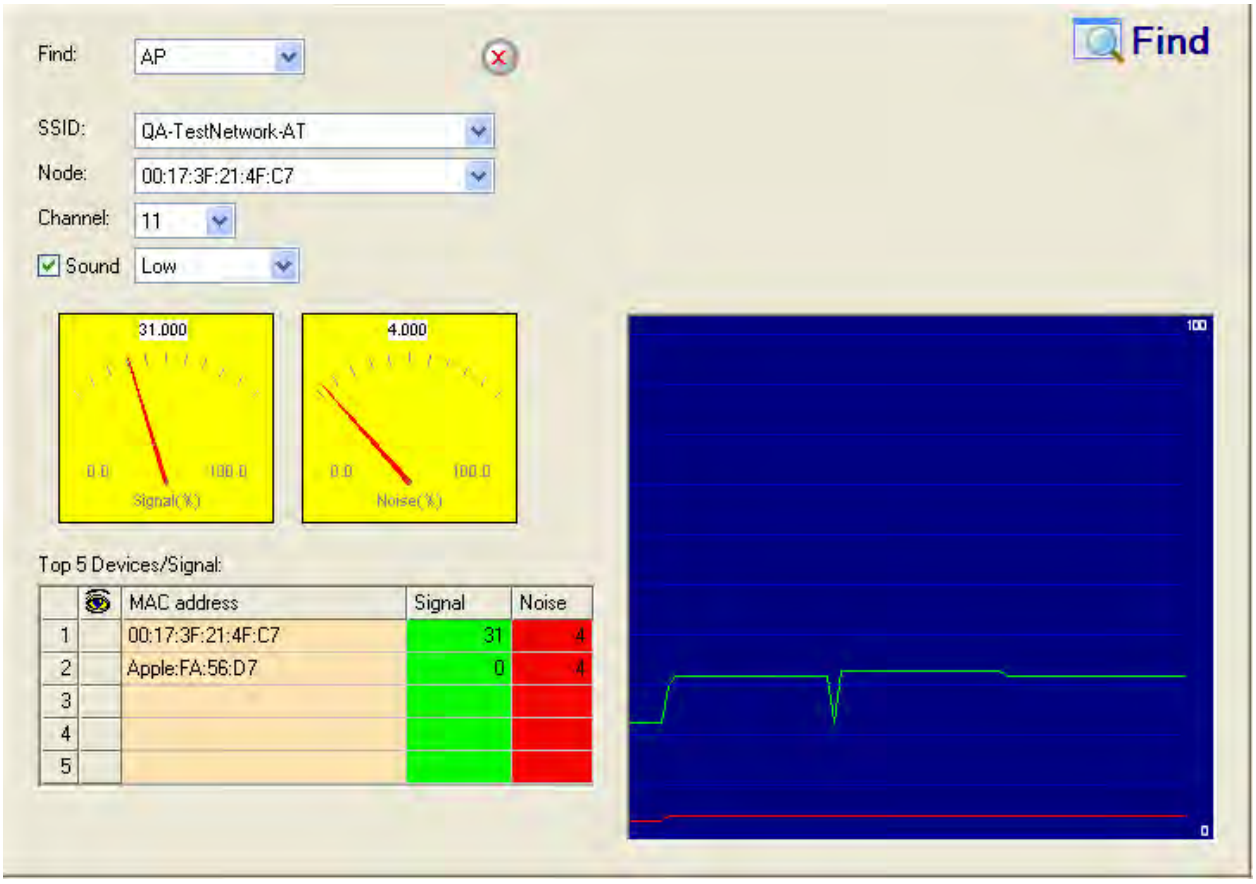
Alarm Description & Possible Causes

WiFi Analyzer alerts the WLAN administrator of a rogue AP by checking against enterprise standardized operating radio frequencies and media such as 802.11a, 802.11b, 802.11g, or 802.11n. Whenever an AP operating outside of the enterprise standardized radio media is discovered by AirMagnet WiFi Analyzer, a rogue AP alarm will be generated. For example, consider a case in which the enterprise implements only 802.11b/g/n APs. If there is an 802.11a AP detected, AirMagnet WiFi Analyzer will immediately raise an alarm.

Rogue APs installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue AP may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet WiFi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue AP is identified and reported by AirMagnet Wi-Fi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue Station by Wireless Media Type

Alarm Description & Possible Causes

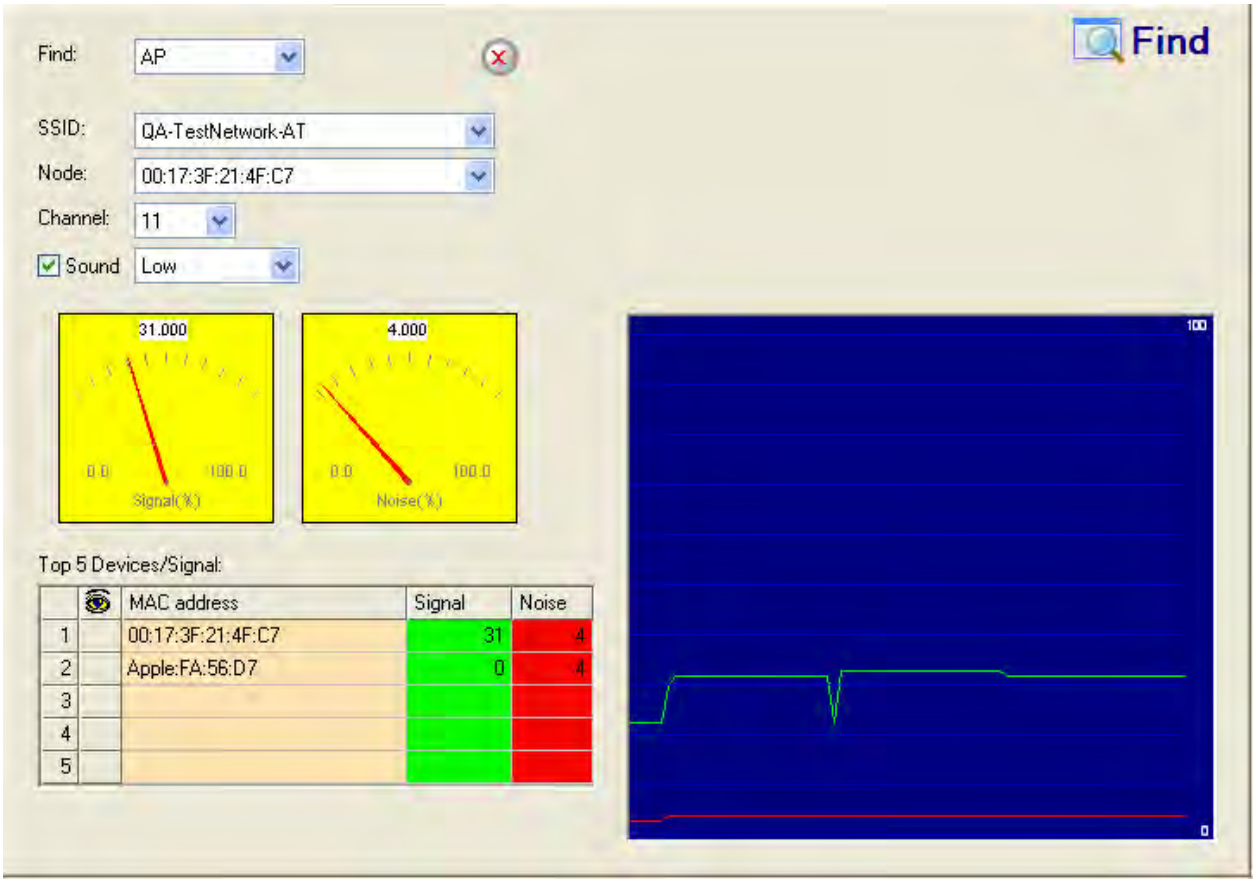
AirMagnet WiFi Analyzer alerts the WLAN administrator of rogue stations by checking against enterprise standardized radio frequencies and media such as 802.11a, 802.11b, 802.11g, or 802.11n. Whenever a client station operating outside of the enterprise

standardized radio media is discovered by AirMagnet WiFi Analyzer, a rogue station alarm will be generated. For example, consider a case in which the enterprise implements only 802.11b/g/n stations. If there is an 802.11a station detected, AirMagnet WiFi Analyzer will immediately raise an alarm.

Rogue stations installed by unauthorized employees usually do not follow enterprise standard deployment practices, and can thus compromise security on the wireless and wired networks. A rogue station may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet Wi-Fi Analyzer should be investigated carefully.

AirMagnet Solution

Once a Rogue station is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Suspicious After-Hour Traffic Detected

Alarm Description & Possible Causes

One way to detect a wireless security penetration attempt is to analyze wireless usage during a time in which there is not supposed to be any wireless traffic (such as after business hours). AirMagnet WiFi Analyzer monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage tracked by AirMagnet WiFi Analyzer during after-office hours include the following:

- Client station initiating authentication or association requests to the office WLAN, which may indicate a security breach attempt.
- Wireless data traffic that may indicate suspicious downloads or uploads over the wireless network.

AirMagnet Solution

For global AirMagnet WiFi Analyzer deployment, the configurable office-hour range is defined in local time. For the office and manufacturing floor mixed WLAN, one can define office hours (for example, 9am to 5pm) for the office WLAN SSID and separate set of hours (for example, 6am to 9pm) for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for devices responsible for the suspicious traffic and take appropriate steps to locate it and remove it from the wireless environment.

Fake APs Detected

Alarm Description & Possible Causes

The Fake AP tool is meant to protect your WLAN by acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames emulating thousands of counterfeit 802.11b access points. War-drivers encountering such large amount of APs will not be able to identify the real APs deployed by the user. This tool, though very effective in discouraging war-drivers, poses many other disadvantages such as bandwidth consumption, misleading legitimate client stations, interference with the WLAN management tools, and so on. AirMagnet Wi-Fi Analyzer does not recommend running the Fake AP tool in your WLAN.

AirMagnet Solution

AirMagnet recommends that the administrator locate the device running the Fake AP tool and take appropriate steps to remove it from the wireless environment.

Device Unprotected by Fortress Encryption

Alarm Description & Possible Causes

If your WLAN security deployment mandates the use of encryption technologies provided by Fortress Technologies, Inc., you can enable this alarm to alert you on devices that are participating in WLAN communication without Fortress encryption.

Being an overlay solution, Fortress Secure Gateways can be easily deployed in any network regardless of topology, infrastructure vendor or wireless technology being used. Whether protecting small pockets of WLAN users, or an entire enterprise, Fortress has models suitable for your specific requirements.

Fortress Secure Gateways provide security between wireless devices, users and network infrastructure. All critical security operations — encryption, authentication, data integrity checking, key exchange, and data compression — are optimized to minimize hands-on management. It also provides secure service for multiple access points simultaneously and scales for various architectures.

Fortress Technologies provides a comprehensive, robust wireless solution that is easy to implement and maintain. By securing the device, data and network, Fortress is the strongest commercially available security platform for wireless networks.

AirMagnet Solution

You should enable the use of Fortress encryption for various devices in the wireless environment. This new security alert identifies users who fail to run Fortress Security System. This will allow security-conscious customers who have chosen Fortress to verify that their authentication/encryption policies are being followed in every installation worldwide. The combined product offering brings together Fortress's robust security infrastructure that encrypts at Layer 2, eliminating the opportunity for hackers to intercept important network data, view internal network addresses, or interrupt availability through denial-of-service attacks, and AirMagnet Wi-Fi Analyzer security and performance management system which manages and monitors wireless security. With this solution, organizations benefit from Fortress’s robust wireless solution that is easy to implement and maintain, combined with the most complete monitoring of rogues, wireless exploits and network intrusions.

Device Thrashing Between 802.11g and 11b

Alarm Description & Possible Causes

The IEEE 802.11g standard requires an 802.11g device to be backward compatible with the IEEE 802.11b standard. For each frame transmission, an 802.11g device can decide to switch between the 802.11b mode (using **CCK** modulation) or 802.11g mode (using **OFDM** modulation). 802.11g APs use this feature to support mixed mode (802.11b and 802.11g devices) deployment in the same wireless environment. An 802.11g client station uses this

feature to optimize performance and to associate with the best service provided by either the 802.11b or 11g AP.

Mode switching is a feature. However, a client station constantly thrashing its RF mode between 802.11g (**OFDM**) and 802.11b (**CCK**) indicates an unstable RF environment. It degrades the 802.11g throughput by reducing the maximum speed from 54 mbps to 11 mbps. It may even cause interrupted WLAN service to the client if association to AP is also switched. Excessive mode switching may be caused by 802.11g implementation that is too sensitive to the dynamic mix of traffic and devices between 802.11b and 11g. Client station mode switching may also be caused by mode switches on the APs.

AirMagnet Solution

To further investigate this problem, you may use the AirMagnet WiFi Analyzer's Infrastructure page and select the List-by-Station view option to show all historical sessions a client station has with various APs. You may also monitor on the client RF mode switch in real time by observing the transmit speeds used by the client on the Infrastructure page after selecting the target client station.

AP With Flawed Power-Save Implementation

Alarm Description & Possible Causes

The IEEE 802.11 standard defines the power-save operation for mobile devices to conserve power by entering sleep mode. While the client remains in sleep mode, the AP will buffer data intended for it for delivery at a later time. The standard defines the power-save mode handshake involving the following important procedure:

- Client informs AP of its power-save mode status (going to sleep)
- AP informs client how often data destined to client will be indicated in beacon
- AP buffers data intended for the client in sleep mode
- Client wakes up periodically to check on the AP beacons to see if there is data buffered for it to receive
- If there is no data, client goes back to sleep mode. If there is data, client informs the AP its power-save mode status to trigger the AP to send the buffered data

APs failing to conform to this procedure may experience client data loss. There are two well-known AP implementation defects in this area:

- AP not buffering client data while client is in power-save mode.
- AP did not notify the power-save mode client of data arrival.

Both scenarios result in client data loss, which will eventually be retransmitted by an upper-layer protocol such as TCP. However, the incurred delay degrades application performance drastically. For some specific applications such as VoIP on WLAN, the lost data will not be

retransmitted resulting in jitter in voice quality. This may be prohibitive, resulting in retransmission, long delays, and degraded performance.

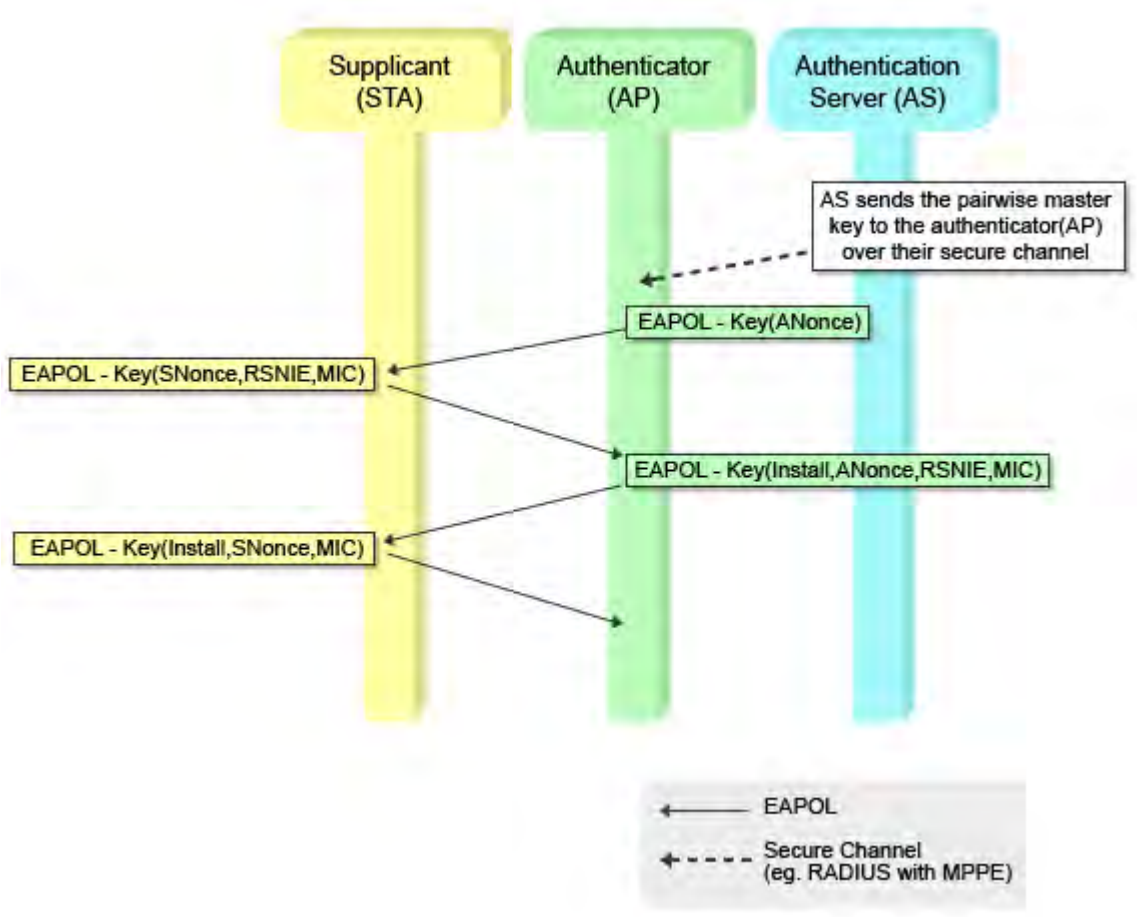
AirMagnet Solution

AirMagnet WiFi Analyzer detects APs with flawed 802.11 power-save implementations similar to the two defects mentioned above. This problem generally does not cause any wireless connection issues but causes severe quality of service degradation. An AP firmware upgrade may help address this problem.

WPA or 802.11i Pre-Shared Key Used

Alarm Description & Possible Causes

WPA and the **802.11i standard** provide a pre-shared key (**PSK**) mechanism as an alternative to using the IEEE 802.1x-based key establishment. 802.1x-based key management requires an authentication server such as a **RADIUS** server to securely and dynamically distribute session keys (Pairwise Master Key or **PMK**). When **PSK** is used instead of 802.1x, the passphrase **PSK** is converted into a 256-bit value needed for the PMK. In **PSK** mode, the 802.11i-defined 4-way handshake is used for encryption key management, with no **EAP** exchange. As there is no **RADIUS** server and no EAP methods (such as EAP-TLS or LEAP) involved, the **PSK** mode is less secure.



4-way handshake completes the key exchange for the Pre-shared Key mode operation
(Authenticator AP and Authentication Server AS are on the AP device)

PSK is used to eliminate the need to set up an authentication server (RADIUS), but comes with reduced security. The 802.11i specification specifies that security can be considered weak if the passphrase is less than 20 characters, as it can be easily broken via an off-line dictionary attack once the 4-way handshake is captured. The problem is that vendors do not provide any easy-to-use tool that can generate and manage 20-character passphrases. Refer to article ***Weakness in Passphrase Choice in WPA Interface*** By Robert Moskowitz, November 4, 2003.

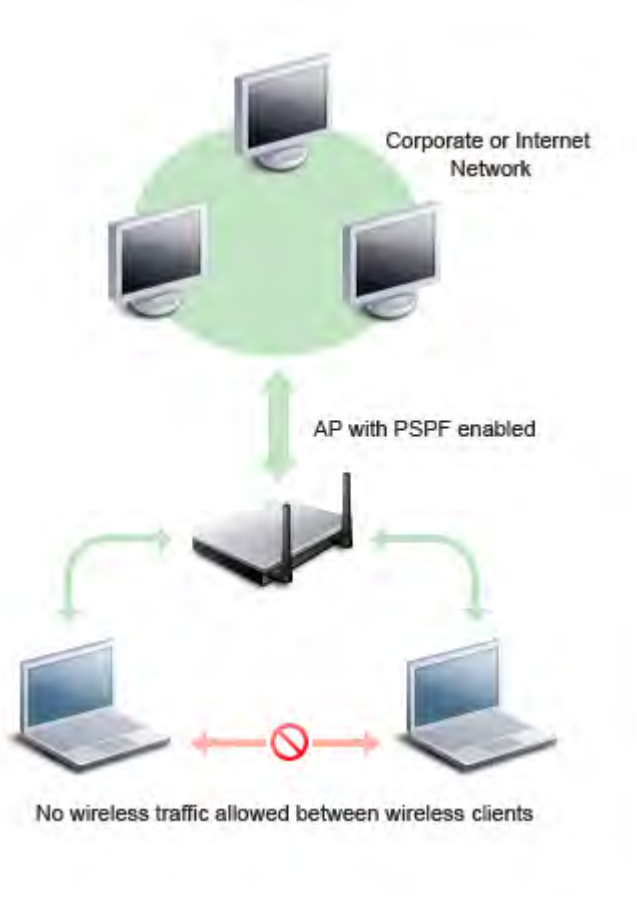
AirMagnet Solution

AirMagnet WiFi Analyzer detects the use of the **PSK** mode and recommends switching to the more secure 802.1x-EAP based key management and authentication system. If you decide to stay with **PSK** mode key management, please make sure your choice of the passphrase is longer than 20 characters and does not contain any words from a dictionary, thus preventing possible attacks.

Publicly Secure Packet Forwarding (PSPF) Violation

Alarm Description & Possible Causes

Publicly Secure Packet Forwarding (**PSPF**) is a feature implemented on WLAN Access Points to block wireless clients from communicating with other wireless clients. With **PSPF** enabled, client devices cannot communicate with other client devices on the wireless network.



PSPF protects public network by prohibiting wireless traffic between wireless clients

For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. Enabling PSPF protects wireless clients from being hacked by a wireless intruder. **PSPF** (this term is commonly used by Cisco. Other vendors may call this differently) is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, and so on, where authentication is null and anyone can associate with the APs. The **PSPF** feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

AirMagnet Solution

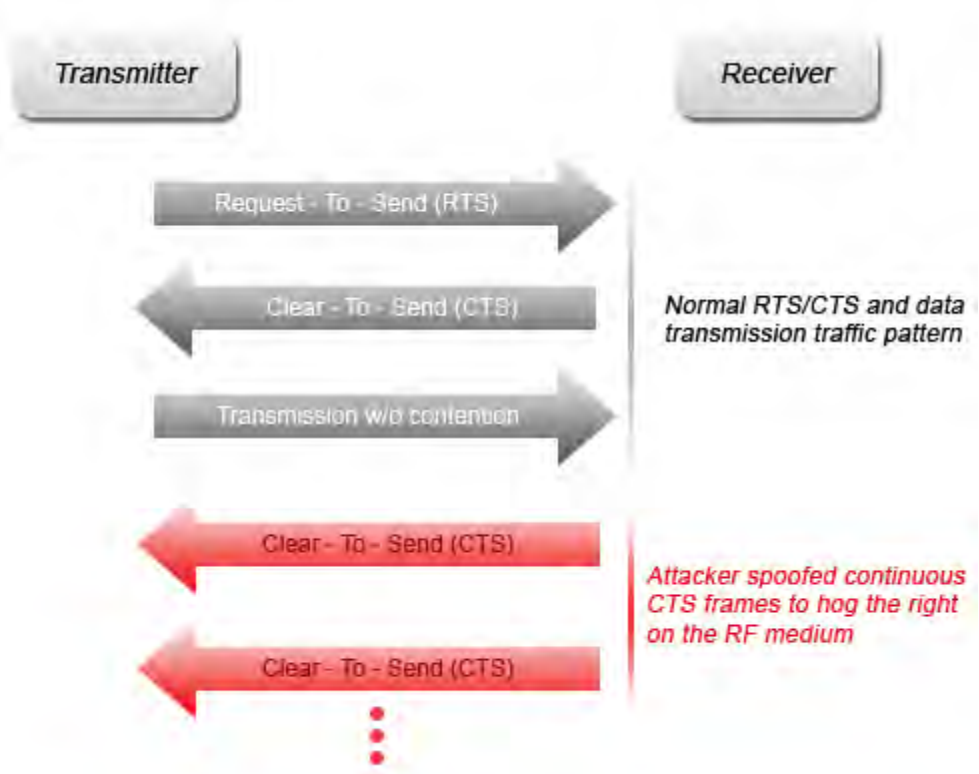
AirMagnet WiFi Analyzer detects PSPF violations. That is, if a wireless client attempts to communicate with another wireless client, AirMagnet Wi-Fi Analyzer raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication.

Denial-of-Service Attack: CTS Flood

Attack tool: CTS Jack

Alarm Description & Possible Causes

As an optional feature, the IEEE 802.11 standard includes the **RTS**/**CTS** (Request-To-Send/Clear-To-Send) functionality to control the station's access to the RF medium. The wireless device ready for transmission sends a **RTS** frame in order to acquire the right to the RF medium for a specified time duration. The receiver grants the request by sending a **CTS** frame of the same time duration. All wireless devices observing the **CTS** frame should yield the media to the transmitter for transmission without contention. While this method helps reduce network traffic, it leaves your network vulnerable to a particular DoS attack in which a hacker spoofs repeated CTS frames. These frames inform other devices that the network is in use, and thus other traffic must wait. See the illustration below.

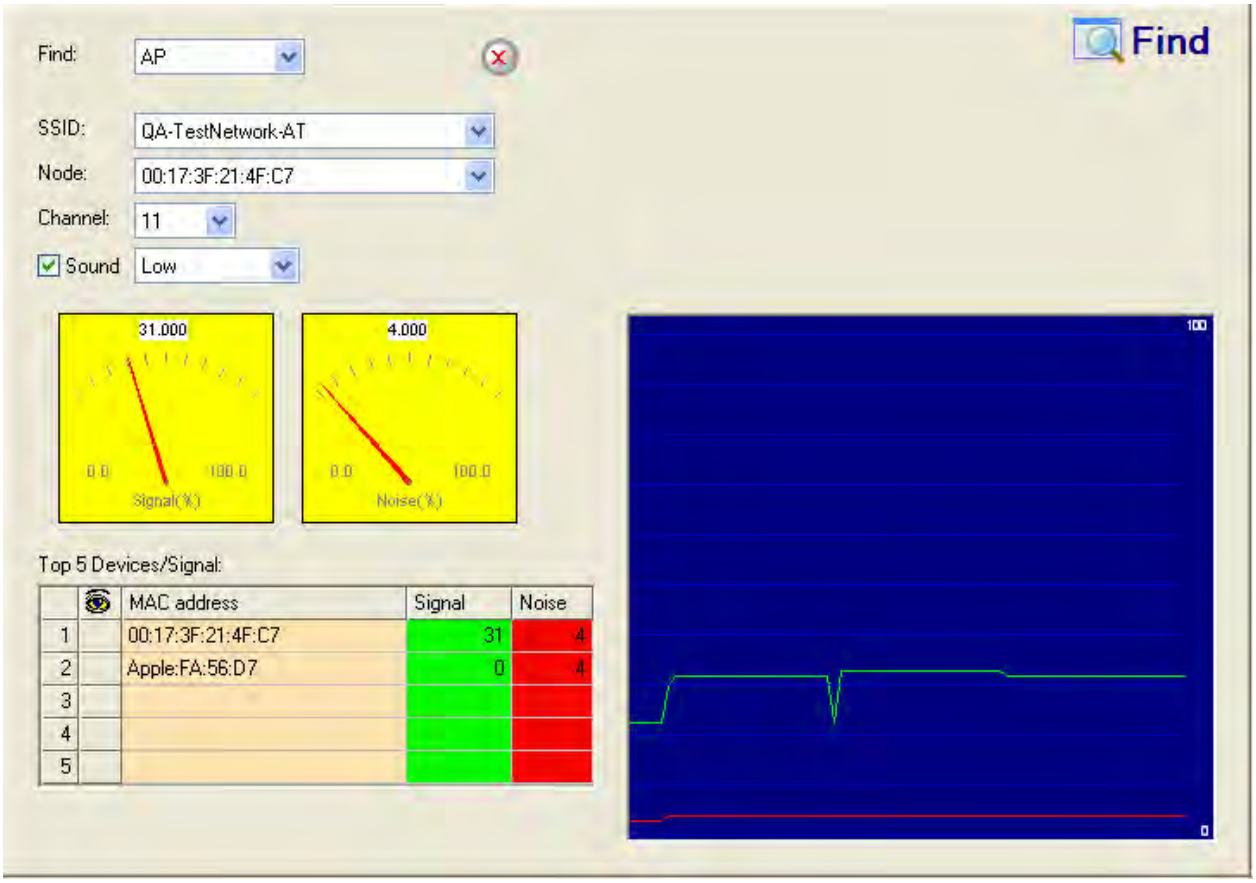


Standard RTS/CTS mechanism vs the intruder injected CTS denial-of-service attack

A wireless denial-of-service attacker may take advantage of the privilege granted to the **CTS** frame to reserve the RF medium for transmission. By transmitting back-to-back **CTS** frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the **CTS** frames.

AirMagnet Solution

AirMagnet WiFi Analyzer detects the abuse of **CTS** frames for a denial-of-service attack. Similar to an RF jamming attack, security personnel can use the AirMagnet WiFi Analyzer's **FIND** tool to locate the source of the excess **CTS** frames.

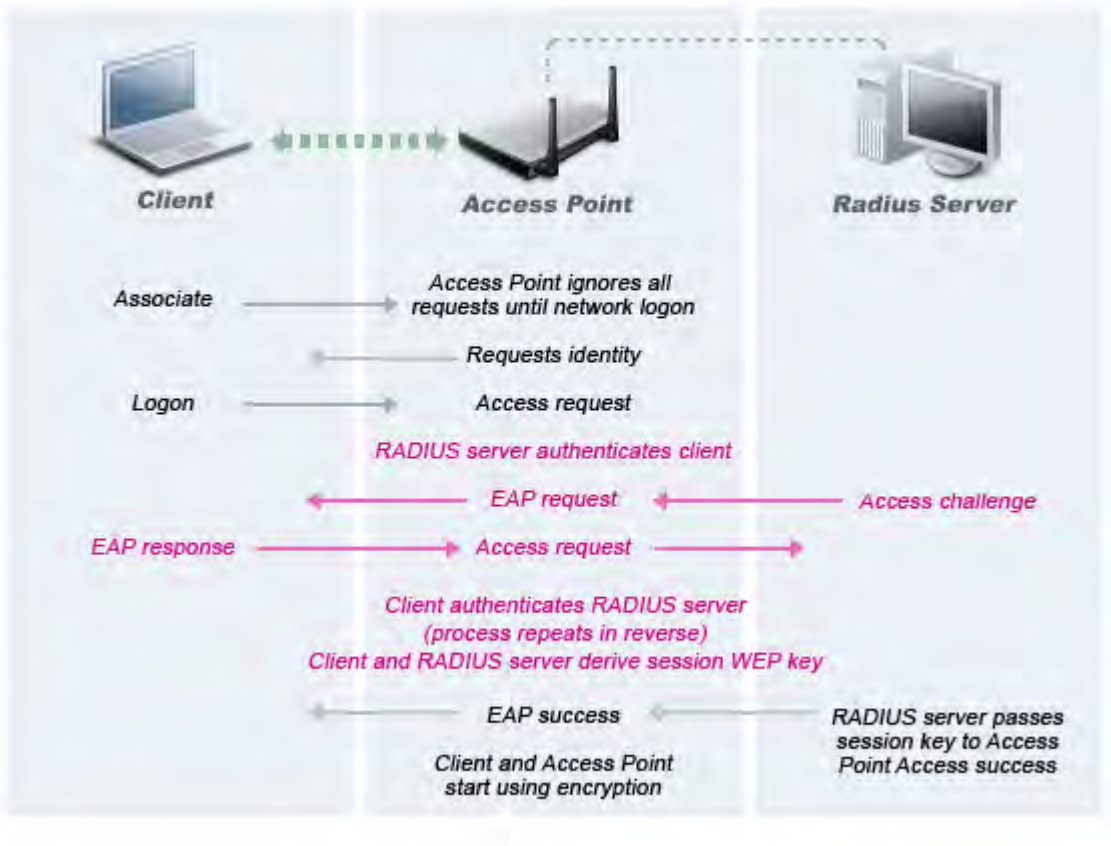


AirMagnet WiFi Analyzer's FIND tool locates intruders by tracking down their signal level

802.1x Unencrypted Broadcast or Multicast

Alarm Description & Possible Causes

802.1x has a framework allowing a system to use per-session encryption keys to defend against the weakness inherited from the global static WEP key mechanism. Additionally, 802.1x also facilitates the session key rotation mechanism, thus ensuring that the encryption keys are updated periodically. This enhances security by eliminating the use of static encryption keys and preventing attacks that require the collection of large amounts of data encrypted with a single static key.



802.1x key exchange protocol distributes per-session encryption key to the AP and client station

For multicast and broadcast packets, in which there are multiple recipients, a per-session encryption key cannot be applied. In order to secure multicast and broadcast communication, a shared encryption key and re-key mechanism has to be implemented. It has been found that very few wireless devices implement the multicast and broadcast encryption key mechanism correctly. In reality, multicast and broadcast packets tend not to be encrypted at all. To make matters more complicated, enterprise-grade APs with multiple SSIDs are frequently deployed with 802.1x security for one SSID (corporate WLAN) and no encryption for another SSID (guest WLAN). This deployment scenario is usually coupled with the VLAN configuration so that client devices using the guest SSID can only access the Internet but not the corporate wired network. An AP supporting multiple SSIDs transmits broadcast and multicast frames thus making the encryption option selection (802.1x or no encryption), an implementation challenge.

AirMagnet Solution

AirMagnet WiFi Analyzer detects unencrypted multicast and broadcast frames caused by mis-configuration or vendor implementation errors. AirMagnet recommends that the user use APs that implement the encryption of multicast and broadcast frames in a proper manner.

Rogue AP by Channel

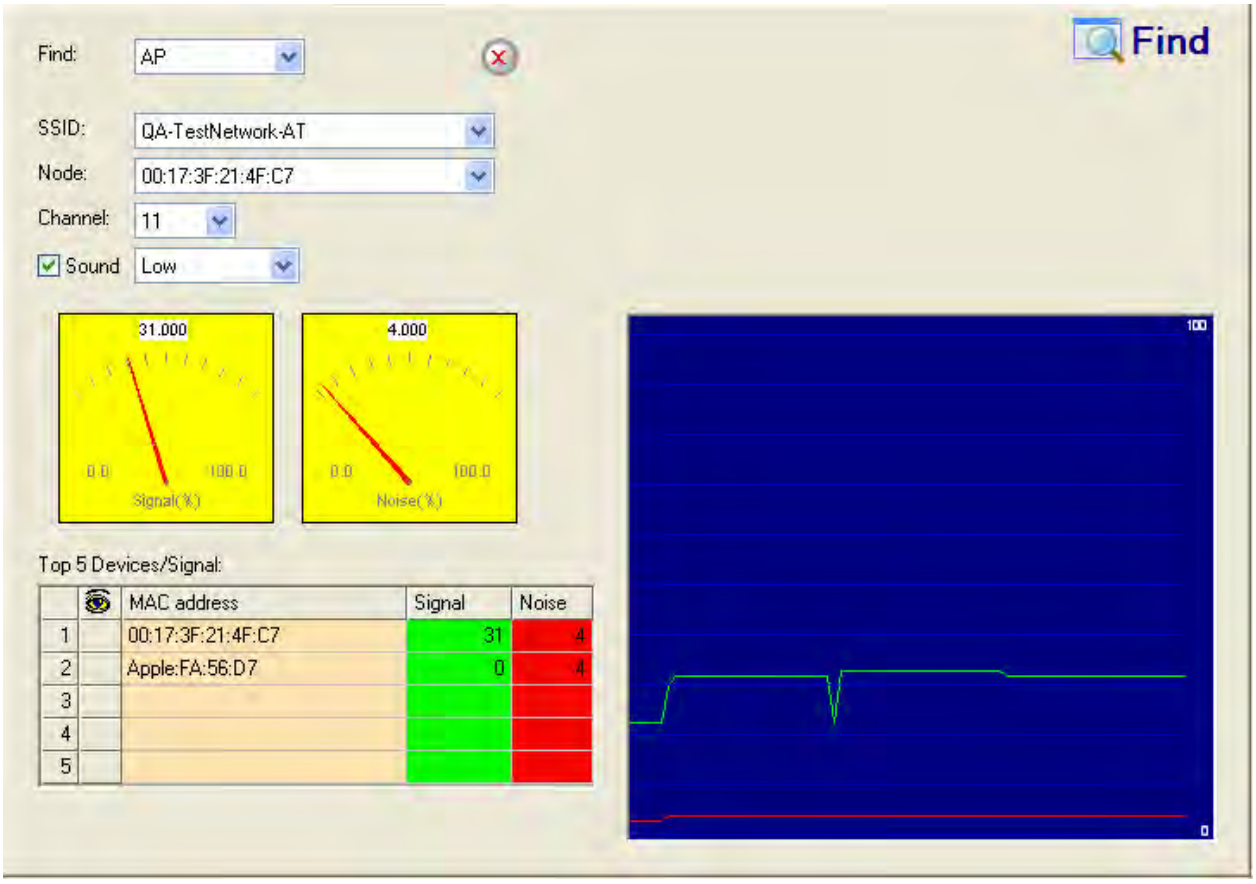
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator on rogue APs by checking against enterprise standardized operating radio channel assignments for the 802.11a, 802.11b, or 802.11g standards. When an AP operating in a non-enterprise standardized radio channel is discovered by AirMagnet WiFi Analyzer, a rogue AP alarm will be generated.

Rogue APs installed by unauthorized employees may not follow enterprise standard deployment procedures, and may thus compromise security on the wireless and wired network. The presence of rogue APs may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet WiFi Analyzer discovered should be thoroughly investigated.

AirMagnet Solution

Once a Rogue AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Rogue Station by Channel

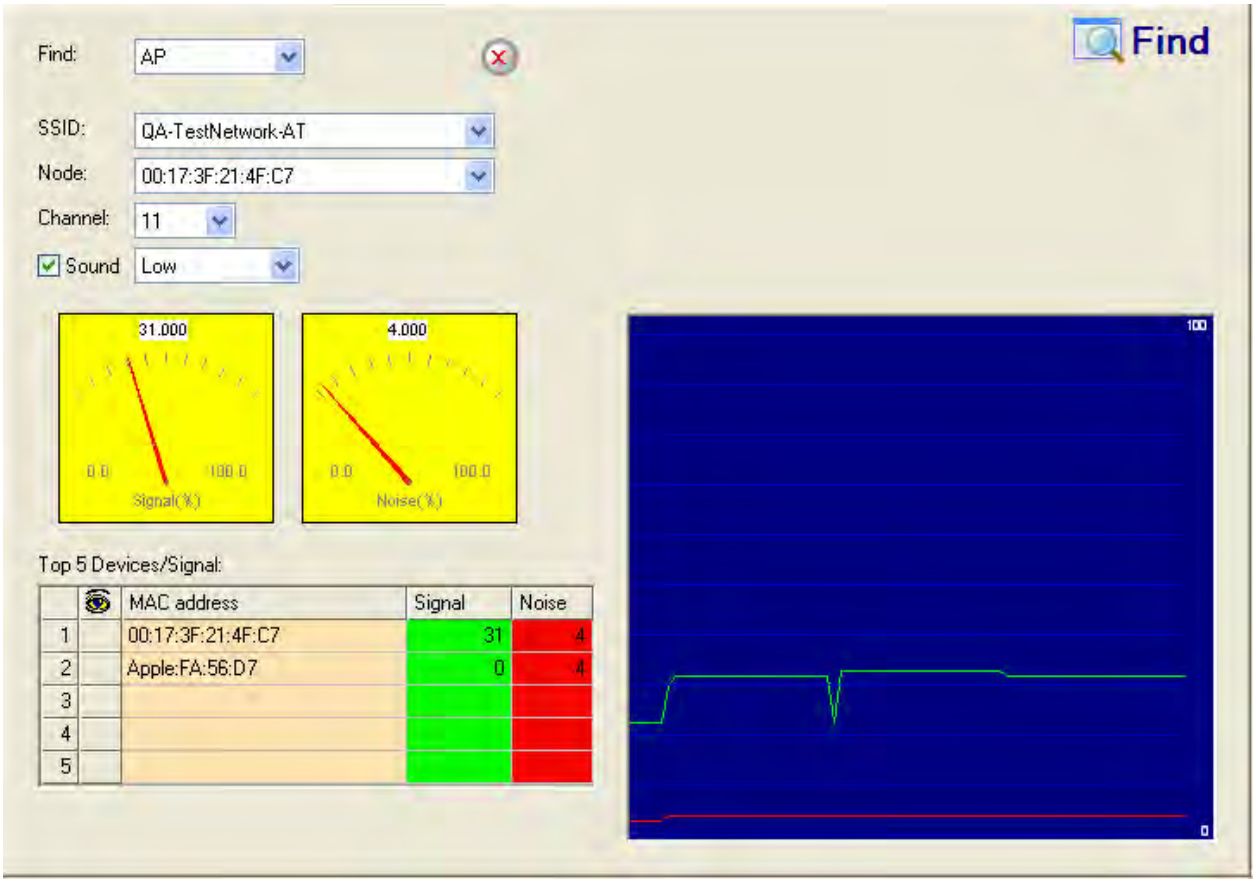
Alarm Description & Possible Causes

AirMagnet WiFi Analyzer alerts the WLAN administrator on rogue stations by checking against enterprise standardized operating radio channels for the 802.11a, 802.11b, or 802.11g standards. When a station operating in a non-enterprise standardized radio channel is discovered by AirMagnet WiFi Analyzer, a rogue station alarm will be generated.

Rogue stations installed by unauthorized employees may not follow enterprise standard deployment procedures, and may thus compromise security on the wireless and wired network. The presence of rogue stations may also indicate malicious intruders attempting to hack into the enterprise wired network. Rogue devices discovered by AirMagnet Wi-Fi Analyzer should be thoroughly investigated.

AirMagnet Solution

Once a Rogue station is identified and reported by AirMagnet Wi-Fi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Soft AP or Host AP Detected

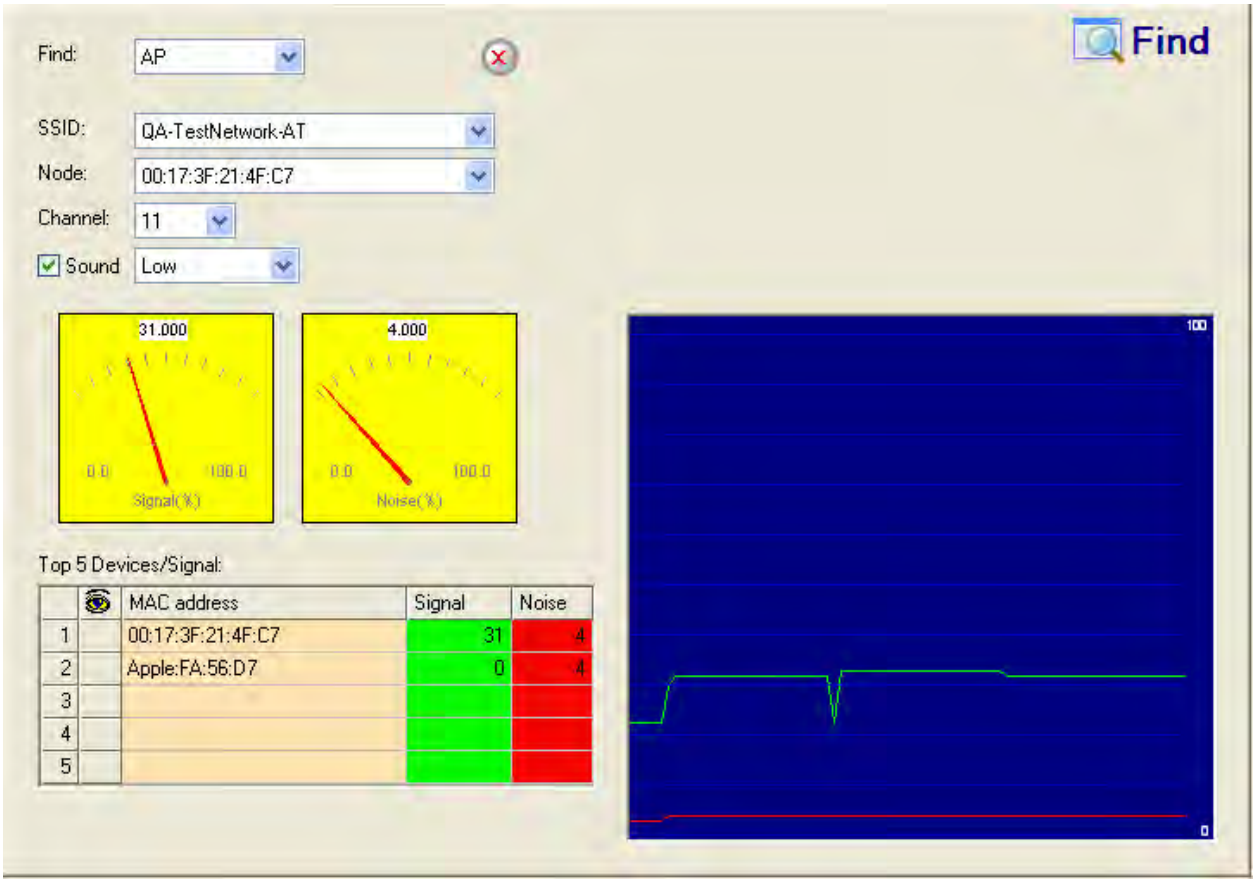
Host AP tools: Cqure AP

Alarm Description & Possible Causes

A host-based Access Point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. Firstly, host-based APs are typically not part of the enterprise wireless infrastructure and are likely to be rogue devices that do not conform to the corporate security policy. Secondly, they can be used by wireless attackers as a convenient platform to implement various known intrusions, such as man-in-the-middle, honey-pot AP, AP impersonation, denial-of-service attacks, and so on. Since software tools for turning a desktop or laptop into an AP can be easily downloaded from the Internet, host-based APs are more than just a theoretical threat. Furthermore, some laptops are shipped with the HostAP software pre-loaded and activated. Once these laptops connect to the enterprise wireless network, they expose the wireless network to hackers.

AirMagnet Solution

Any soft AP detected by AirMagnet WiFi Analyzer should be treated as a rogue AP as well as a potential intrusion attempt. Once the soft AP is identified and reported by AirMagnet WiFi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Security IDS/IPS

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue Access Points installed by employees for their personal use usually do not adhere to the corporate security policy. A single Rogue AP can put the entire corporate network at risk of outside penetration and attack, and there are many other possible wireless security risks and intrusions such as mis-configured AP, unconfigured AP, and Denial-of-Service attacks.

Wireless Security Methods

AirMagnet WiFi Analyzer is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, AirMagnet Wi-Fi Analyzer alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on denial-of-service attacks

To maximize the power of AirMagnet WiFi Analyzer, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, AirMagnet WiFi Analyzer can be customized to generate the rogue AP alarm when an AP made by another vendor is detected.

Performance Violation

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely-monitored and well-tuned WLAN system can achieve a higher throughput than a poorly managed one. AirMagnet WiFi Analyzer provides a site survey tool to assist precise WLAN installation and deployment. AirMagnet Wi-Fi Analyzer ensures better WLAN performance and efficiency by monitoring the WLAN and alerting the wireless administrator of early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

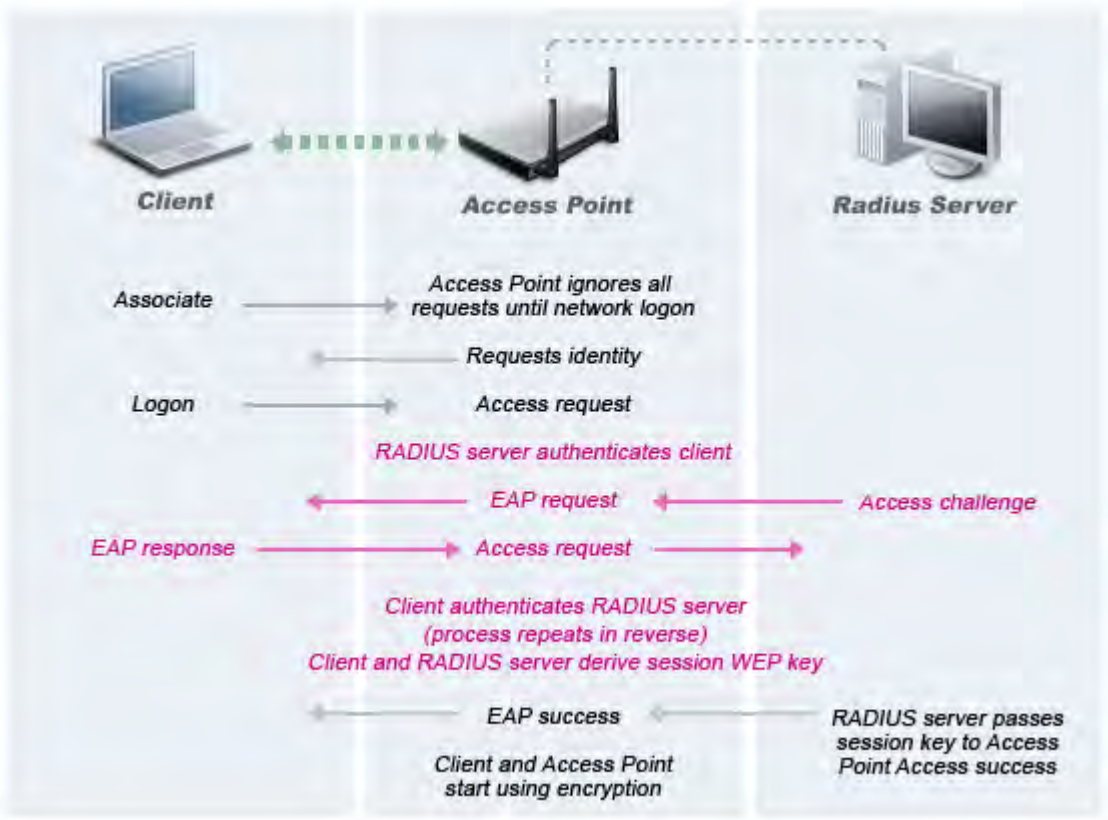
- RF Management
- Problematic traffic pattern
- Channel or device overload
- Deployment and operation error

- IEEE 802.11e & VoWLAN issues

To maximize the power of AirMagnet WiFi Analyzer, performance alarms can be customized to best match your WLAN deployment specification. For example, if your WLAN is designed for all users to use 5.5- and 11-Mbps speeds only, you can customize the threshold for performance alarm 'Low speed tx rate exceeded' to reflect such an expectation.

User Authentication and Traffic Encryption

The first line of defense for WLAN security is user authentication and wireless traffic encryption. Centralized WLAN user authentication based on the IEEE 802.1x standard with a RADIUS server at the back-end is a flexible and strong mechanism. The figure below diagrams the 802.1x authentication process:



802.1x User Authentication Process

Other authentication methods (such as VPN) may also be used to achieve the same goals. User authentication blocks out unauthorized access to your wired and wireless resources. Traffic encryption goes hand-in-hand with user authentication, during which the encryption secrets are exchanged between AP and authorized users. Traffic encryption prevents intruders from eavesdropping on your wireless traffic.

AirMagnet Wi-Fi Analyzer validates your WLAN security deployment by monitoring on the authentication transactions and traffic encryption methods against the specified security deployment policy, which it learns from the AirMagnet policy configuration. For example, AirMagnet WiFi Analyzer generates the ***Device unprotected by PEAP*** alarm if the **802.1x EAP** type-**PEAP** is your enterprise standardized authentication protocol. Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software/firmware, and suboptimal choice of corporate security policy. AirMagnet Wi-Fi Analyzer alerts the administrator on these issues and provides countermeasures.

Rogue AP and Station

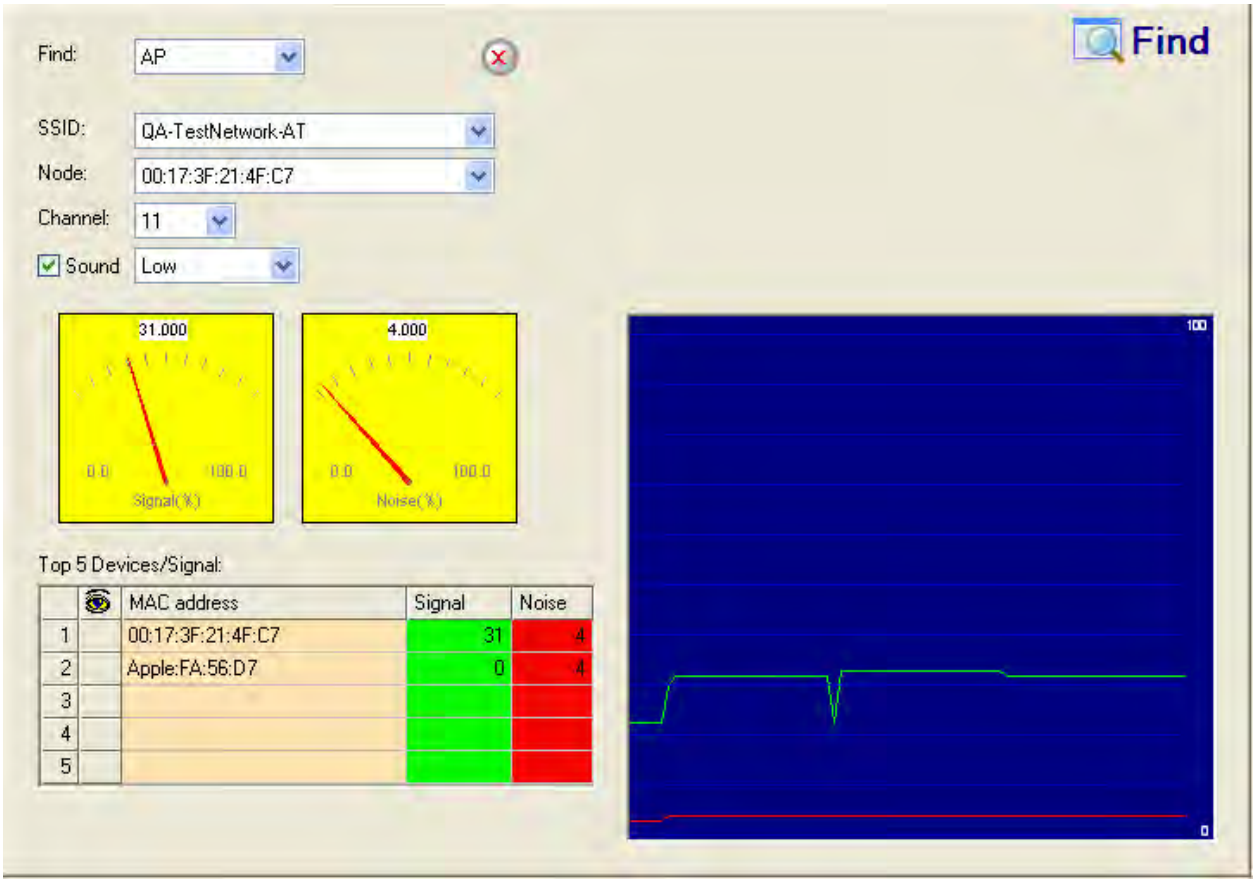
As WLAN gains popularity in enterprise and home networks, it is common for enterprise IT professionals to discover unauthorized WLAN devices connected to the corporate wired network. These unauthorized WLAN devices are installed by intruders or ignorant employees and usually do not conform to the enterprise WLAN security policy that requires strong user authentication infrastructure and strong traffic encryption standards. Rogue devices have to be detected and removed immediately in order to protect the integrity of the wireless and the wired enterprise network.

AirMagnet Wi-Fi Analyzer provides the following methods to detect rogue devices. One or more of these methods can be used to differentiate authorized and rogue devices.

- By MAC address (access control list)
- By equipment vendor ID
- By SSID
- By media type (802.11a/b/g/n)
- By channel

For example, if your WLAN deployment includes implementing only APs made from Cisco operating in the 802.11b mode, you may enter that information in the rogue device alarm configuration. AirMagnet WiFi Analyzer will then generate rogue device alarms if a non-Cisco AP or an 802.11g/n AP is detected in the wireless environment.

Once a Rogue device is identified and reported by AirMagnet Wi-Fi Analyzer, the WLAN administrator may use the FIND tool to locate the rogue device.



AirMagnet WiFi Analyzer's FIND tool locates devices by tracking down their signal level

Configuration Vulnerabilities

Implementing a strong deployment policy is fundamental to constructing a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With more and more laptops coming packaged with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond the Access Points and to the stations. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi. Besides checking policy validations, AirMagnet also provides suggestions for best configuration practices in case a suboptimal configuration choice is detected. For example, AirMagnet WiFi Analyzer generates a warning alarm when it detects an AP broadcasting its SSID. The AirMagnet Wi-Fi Analyzer alarm description in this case will recommend that the wireless administrator turn off the SSID broadcast as a good security practice.

Intrusion Detection - Security Penetration

One common form of wireless intrusion is to breach the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. **Dictionary attacks** on the authentication method represent a very common attack against an AP. The intruder can

also attack the wireless client station during its association process with an AP. For example, a **faked AP attack** on a unsuspecting wireless client may fool the client into associating with faked AP. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if **mutual authentication** and **strong encryption** techniques are used. AirMagnet Wi-Fi Analyzer looks for weak security deployment practices as well as any penetration attack attempts. AirMagnet WiFi Analyzer ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, AirMagnet WiFi Analyzer generates alarms to bring these intrusion attempts to the administrator's notice.

Intrusion Detection - Denial-of-Service Attack

Wireless Denial-of-Service (DoS) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layers one and two. DoS attacks may target the physical RF environment, APs, client stations, or the back-end authentication RADIUS servers. For example, an RF jamming attack with high power directional antenna can be performed from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Fortunately, WLAN vendors are now aware of these attacks and are developing new standards like **802.11i** to tackle these issues. AirMagnet Wi-Fi Analyzer contributes to this solution by providing an early detection system where the attack signatures are matched. AirMagnet WiFi Analyzer's DoS detection focuses on WLAN layers one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. AirMagnet WiFi Analyzer tightens your WLAN defense by validating strong authentication and encryption policies with its AirWISE technologies. In addition, AirMagnet WiFi Analyzer's Intrusion Detection of DoS attacks and security penetration provides 24x7 airtight monitoring of potential wireless attacks.

RF Management

AirMagnet WiFi Analyzer monitors the physical RF environment, which is dynamic and very often the source of WLAN performance problems. Through this, the AirWISE technology characterizes the following WLAN fundamentals and reports problems accordingly:

- Channel interference and channel allocation problems
- Channel noise and non-802.11 signals
- WLAN RF service under-coverage area
- Classic RF hidden-node syndrome
- Many more...

In addition to complicated technical RF issues, there are regulatory rules specified by governing authorities (such as the FCC, ETSI, TELEC, and so on.--see the table below) that need to be met. A successful WLAN operation should not only be within the boundaries specified by the regulating authority but should also take the technical issues into consideration.

Channel number	Frequency (GHz)	North America/ &ANZ	Europe/ EMEA	France/ Singapore	Spain	Mexico	Israel	China	Japan
1	2412	●	●	●				●	●
2	2417	●	●	●				●	●
3	2422	●	●	●			●	●	●
4	2427	●	●	●			●	●	●
5	2432	●	●	●			●	●	●
6	2437	●	●	●			●	●	●
7	2442	●	●	●			●	●	●
8	2447	●	●	●			●	●	●
9	2452	●	●	●				●	●
10	2457	●	●	●	●	●		●	●
11	2462	●	●	●	●	●		●	●
12	2467		●	●					●
13	2472		●	●					●
14	2484								●
Maximum Power (mW)		100	100				100	5	50

World Wide RF 2.4 GHz Spectrum Regulatory Rules on Channel allocation and Output Power

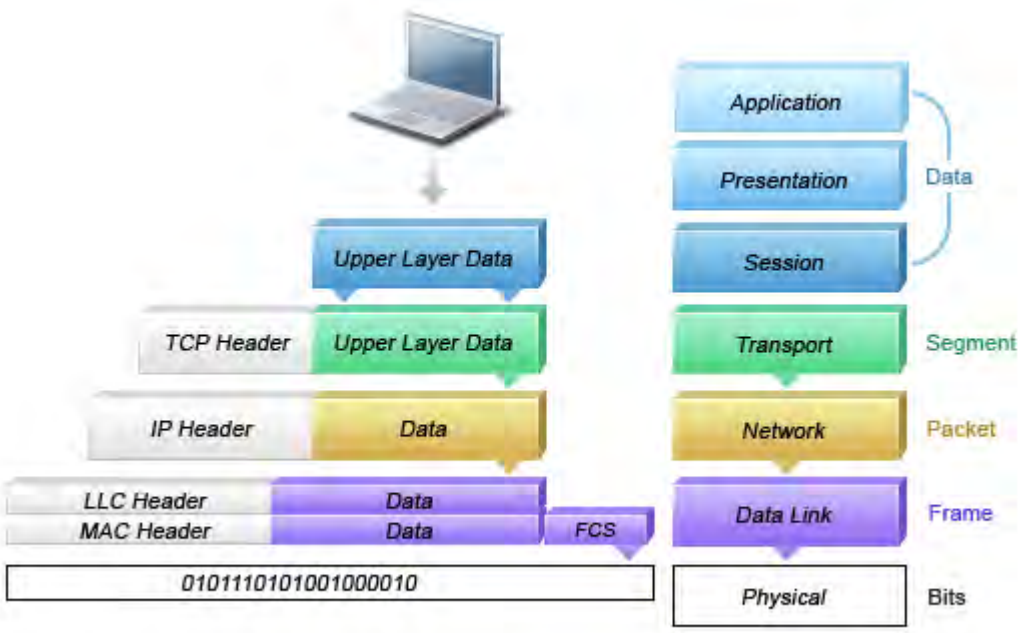
Note: Please note that channel utilization, 802.11a/b/g modulation issues, and MAC layer protocol problems are classified in AirMagnet Wi-Fi Analyzer's performance categories rather than the RF Management category.

Problematic Traffic Pattern

Many WLAN performance problems (including the RF multipath problem) manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, AirMagnet WiFi Analyzer is able to spot performance inefficiencies and degradations early on. In many cases, AirMagnet Wi-Fi Analyzer can even determine the cause of the detected performance problem and suggest countermeasures. AirMagnet WiFi Analyzer tracks MAC layer protocol characteristics, including the following:

- Frame CRC error
- Frame re-transmission

- Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
- Layer 2 frame fragmentation
- AP and station association/re-association/dis-association relationship
- Roaming hand-off
- More...

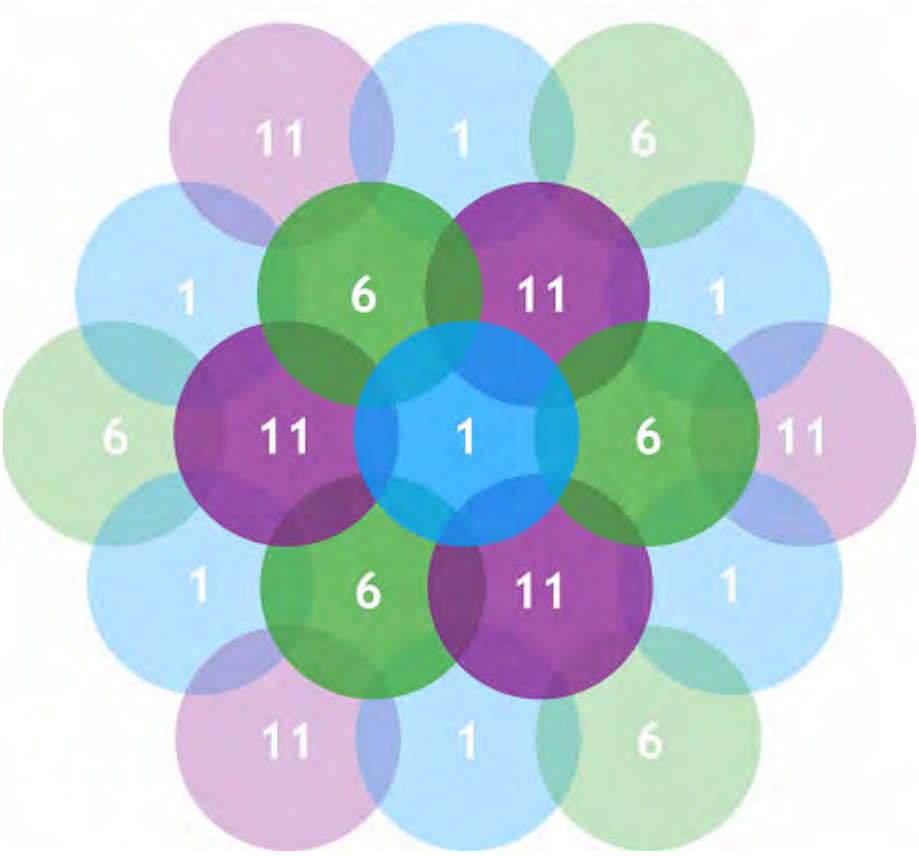


WLAN Data Packet Format and Protocol Encapsulation

AirMagnet WiFi Analyzer analyzes layers one and two (physical and data link layer, as illustrated in the picture above) to identify issues that are unique to WLAN operations. Higher layer protocol analysis (including IP/TCP/UDP/DHCP) can also be processed by AirMagnet WiFi Analyzer if it is not encrypted.

Channel or Device Overload

WLAN technologies use the radio frequency spectrum as a shared physical medium similar to the original 10-Mbps Ethernet technology, which later evolved into Ethernet switches. Even for the latest WLAN standards for 802.11a and 802.11g, there is still a 54-Mbps shared media bandwidth ceiling. In reality, the ceiling is much lower, considering the necessary MAC protocol overhead, inter-frame spacing, collision, and random transmission back-offs.



Optimized Channel Allocation is Critical in Maximizing WLAN Throughput and Minimizing Interference

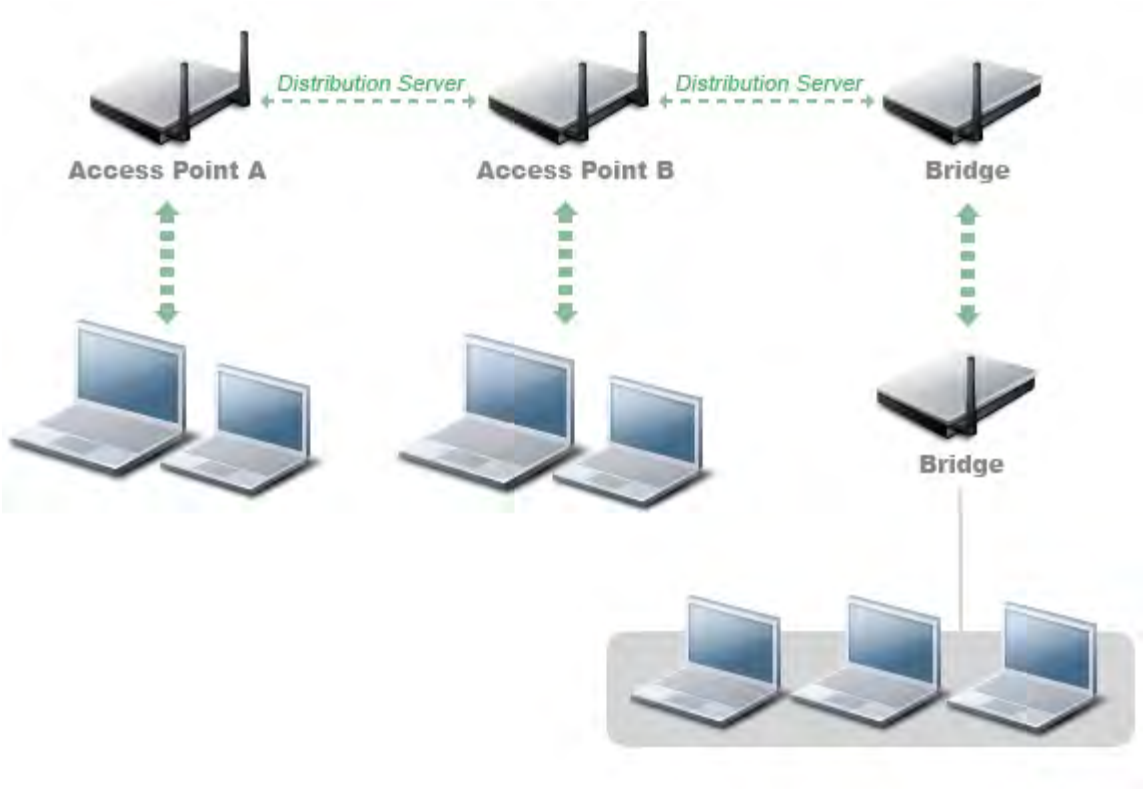
Not only does the radio medium have bandwidth limitations, WLAN Access Points have limitations and can be overloaded by heavy traffic or a large number of associated clients. Like the wired LAN, excessive multicast and broadcast frames can put extra burden on the WLAN devices. Overloaded devices suffer from degraded performance and cause connectivity problems; for example, the AP association table may be overflowed by large number of clients.

Be it channel bandwidth limitation or the WLAN device resource capacity, AirMagnet WiFi Analyzer monitors and tracks the load to ensure smooth operation. In the event of the WLAN not performing satisfactorily due to under-provisioning or over-growth, AirMagnet WiFi Analyzer raises alarms and offers specific details. One thing to note about RF is that it has no boundaries that could lead your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. AirMagnet Wi-Fi Analyzer monitors your WLAN to ensure proper bandwidth and resource provisioning.

Deployment and Operation Error

An important part of ensuring WLAN performance efficiency and reliability is properly configuring the WLAN infrastructure. Wireless configuration management products assist in consistent configuration for large-scale deployments; however, the RF performance impact

resulting from a set of chosen configuration parameters is usually not predictable and may require validation.



WLAN Deployment Involves Configuration for Access Points, Wireless Bridges, and Back-end Distribution Service

AirMagnet WiFi Analyzer monitors these configuration parameters and their mutual interactions for potential errors. In addition, AirMagnet Wi-Fi Analyzer monitors the RF environment to ensure reliable wireless service and provide early warning for other operational exceptions such as damaged antennas, power failures, implementation flaws, and AP resets.

AirMagnet WiFi Analyzer scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:

- **Inconsistent configuration among APs servicing the same SSID**
- **Configuration against the principles of best practice**
- **Connection problems caused by client/AP mismatch configuration**
- **WLAN infrastructure device down or reset**
- **Flaws in WLAN device implementation**
- **More...**

IEEE 802.11e & Voice over Wireless Local Area Network (VoWLAN)

The IEEE 802.11e standard adds Quality-of-Service (QoS) features and multimedia support to the existing 802.11 a/b/g wireless standards while maintaining full backward compatibility with them. The QoS feature is very critical to voice and video applications. Wireless LAN provides more limited bandwidth and higher overheads than traditional wired Ethernet. The throughput is reduced for a variety of reasons, including the RTS/CTS mechanism, packet fragmentation, packet re-transmission, acknowledgements, collisions, and so on.

The IEEE 802.11 standard MAC protocol was designed with two modes of communication for wireless devices that is DCF (Distributed Coordination Function) and PCF (Point Coordination Function). The DCF mechanism involves waiting if someone else is transmitting, which is part of the CSMA/CA mechanism. The data traffic in DCF is based on a first-come first-serve basis: the access point has the same priority as the other stations. This is very critical for DCF, as the number of devices increases in the BSS, and so do the collisions.

The PCF mechanism provides data transfer via a polling mechanism. In this, the Access Point controls the transfer of frames to and from the stations. The Access Point sends beacons, which contain all the necessary parameters. The station can transmit data during the Contention Free Period (CFP). There are very few vendors that support the PCF method and PCF suffers from unpredictable polling schedules. Also absent is any mechanism through which the stations can notify the access point about any QoS requirements.

A station that includes the QoS enhancements is designated as QSTA (QoS STA), while the AP is designated as QAP (QoS AP). A QSTA that associates to an AP with no QoS enhancements can still be provided non-QoS data services by the AP.

The IEEE 802.11e standard includes two mechanisms for application support:

- Enhanced Distributed Channel Access (EDCA): This mechanism delivers traffic based on the different user priorities associated with every MSDU (MAC Service Data Unit) assigned at layers above the MAC layer. Different user priorities can be obtained by modifying:

  a) the amount of time a station senses the channel to be idle before backoff or transmission.

  b) the length of the contention window for the backoff.

  c) the duration a station may transmit after it acquires the channel.

  - HCF Controlled Channel Access (HCCA): This mechanism allows reservation of transmission opportunities (TXOPs: Time intervals in which the QSTA can transmit frames) with the Hybrid Co-ordinator (HC: co-located with the QAP). A QSTA requests the HC for TXOPs - both for its own transmissions as well as transmissions from the QAP to itself. The request is initiated by the Station Management Entity (SME) of the QSTA. Based on the admission control policy, if the request is accepted, the HC schedules TXOPs for both the QAP and the QSTA. For transmissions from the QSTA, the HC polls the QSTA based on the parameters supplied by the QSTA at the time of its request. For transmissions to the QSTA, the QAP directly obtains TXOPs from the

collocated HC and delivers the queued frames to the QSTA, again based on the parameters supplied by the QSTA.

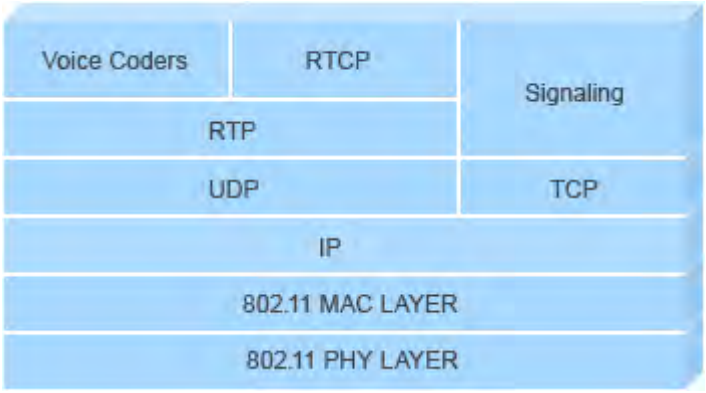
MAC frame format

VoWLAN, an extension of VoIP, is considered to be the next killer application for WLANs. The various components are:

- a Wi-Fi enabled phone
- an access point to which the phone will associate
- At upper layers, a PBX system that may connect to a public telephone network (or the communication could be through the Internet).

The two most important issues that need to considered in a VoWLAN deployment are:

- capacity: number of phones or concurrent calls per cell
- roaming: how the network deals with phones roaming from one access point to another



VoWLAN system with the UDP protocol and the 802.11 MAC and PHY layers

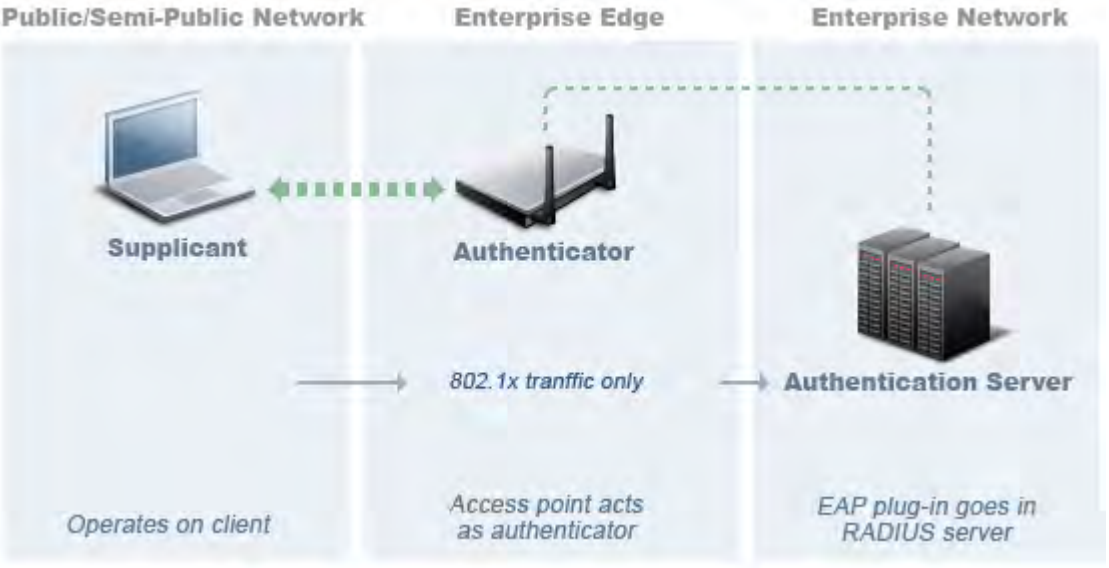
Static WEP Encryption

Static WEP encryption was specified in the IEEE 802.11 standard in 1999. Since then, several papers (for example, *Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir*) have been published on the vulnerabilities of this algorithm (WEP using RC4 with static key). For security-sensitive WLAN deployments, other alternatives such as WPA (Wireless Protected Access - TKIP and 802.1x) and 802.11i exist to address the encryption tasks.

Interestingly enough, statistics show that more than 50% of WLANs do not implement any encryption method. Even with the potential vulnerability of static WEP, it is still safer than no encryption at all. If you decide to use static WEP, there are ways to keep it as secure as WEP can be. AirMagnet WiFi Analyzer assists you in accomplishing that goal by monitoring on static WEP usage and identifying security holes such as crackable WEP key usage and shared-key authentication, and by detecting devices that do not use WEP.

WPA and 802.11i

The Wi-Fi published **WPA** (Wireless Protected Access) specification identifies a feature subset of the IEEE **802.11i** standard. WPA is one of the answers to the well-publicized vulnerability of static WEP as specified by the original IEEE 802.11 specification. Most wireless vendors support **WPA** and consider it to be a more secure alternative to static **WEP**.



802.1x user-based authentication and encryption framework

There are three major end-user benefits provided by the **WPA** products:

- **802.1x** allows user-based authentication instead of the vulnerable global encryption key method
- **TKIP** (Temporal Key Integrity Protocol) enhances industrial strength encryption with dynamic keying
- **PMK** (Pre-shared Master Key) allows small- and medium-sized deployments to use **802.1x** and **TKIP** without complex infrastructure back-end servers (such as **RADIUS**).
- **CCMP** is the advanced encryptions system using Counter-Mode with Cipher Block Chaining (CBC) message Authentication Code (MAC) protocol. In CCMP, key management and message integrity is handled by a single component built around AES.

AirMagnet Wi-Fi Analyzer monitors **WPA** transactions and alerts the administrator when it detects non-compliant devices and weak configurations.

VPN

Instead of (or in addition to) wireless layer 2 authentication and encryption methods such as 802.1x/EAP, TLS, and TKIP, some WLANs use layer 3 VPN technologies to maintain tight security. For a VPN deployed environment, AirMagnet WiFi Analyzer detects devices that are not protected by VPN technologies such as:

- **IPsec** - IP Security
- **L2TP** - Layer 2 Tunneling Protocol
- **PPTP** - Point to Point Tunneling Protocol
- **SSH** - Secure Shell

Other Encryption and Authentication Methods

AirMagnet WiFi Analyzer security offerings cover most standard technologies such as WEP, 802.1x, TKIP, and VPN. It also supports proprietary security technologies deployed by AirMagnet customers (such as Cranite Systems, Inc. and Fortress Technologies, Inc.). These alarms are not enabled by default. If your network utilizes any non-standard security technologies, you must enable the appropriate alarms to ensure that AirMagnet WiFi Analyzer monitors your network accordingly.

Rogue AP

AirMagnet WiFi Analyzer detects rogue APs by MAC address, vendor ID, SSID, radio media type, and RF channels. For AirMagnet Enterprise, the AirMagnet sensor can be configured to auto-respond to detected rogue APs. In such a case, the AirMagnet Smartedge Sensor emulates a wireless client using the rogue AP's announced SSID to associate with the AP. After associating, the sensor performs an IP level trace to track down the IP address that is being used to enter your enterprise wired network. This IP address can then be used by IT personnel to track down a switch port where the rogue AP is connected. Disabling the switch port will then effectively disconnect the rogue AP from your enterprise network immediately.

Rogue Station

With the ubiquity of wireless devices (especially laptops with built-in Wi-Fi cards), it is getting increasingly difficult to manage wireless clients. Rogue stations may be intruders as well as legitimate enterprise computers/laptops that are not authorized to utilize wireless services. Unauthorized wireless stations failing to conform to the stringent enterprise security policies risks exposing sensitive and confidential information on their systems. For example, a dangling unassociated station searching for a wireless AP used at the employee's home risks a fake AP attack from intruders.

To ensure that only legitimate stations are present on your WLAN, AirMagnet WiFi Analyzer uses the same rogue AP detection mechanism to detect rogue stations. These detection

mechanisms are by MAC address, vendor ID, SSID, radio media type, and RF channels. In addition, any station that is associated with a rogue AP also triggers a rogue station alarm.

Denial-of-Service Attack Against AP

Denial-of-Service attacks against APs are typically carried out on the basis of the following assumptions:

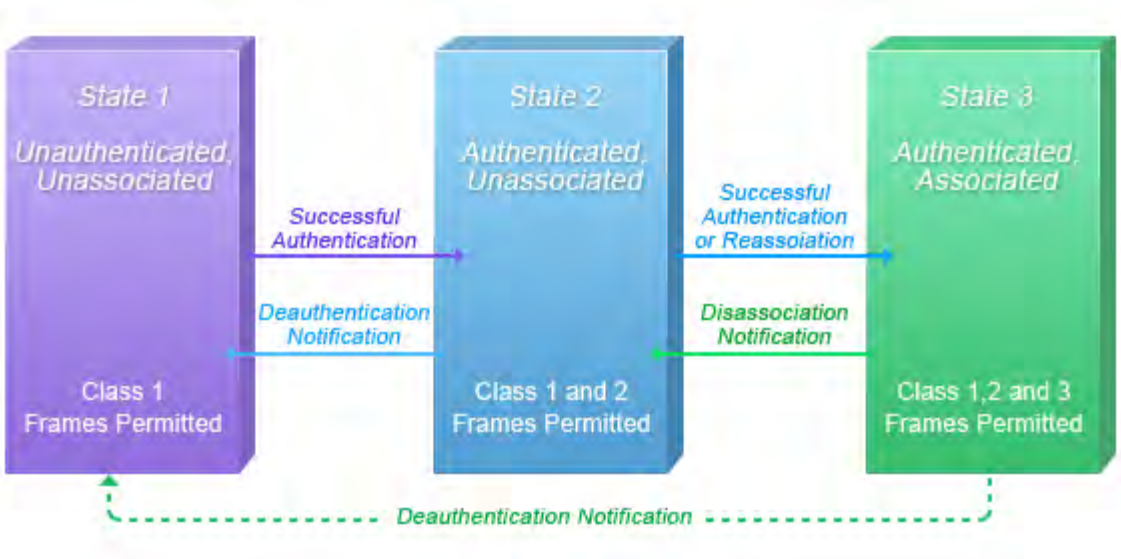
- APs have limited resources. For example, the per-client association state table can only hold a certain number of entries.
- WLAN management frames and authentication protocols, 802.11 and 802.1x, have no inherent encryption mechanisms.

Wireless intruders can exhaust AP resources, most importantly the client association table, by emulating a large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients would attempt association and authentication with the target AP but would leave the protocol transaction mid-way. Once the AP's resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked AP - thus forming a denial of service attack.

AirMagnet WiFi Analyzer tracks the client authentication process and identifies DoS attack signatures against the AP. Incomplete authentication and association transactions trigger the AirMagnet WiFi Analyzer attack detection and statistical signature matching process. Detected DoS attacks result in AirMagnet WiFi Analyzer alarms that include a detailed description of the alarm and target device information.

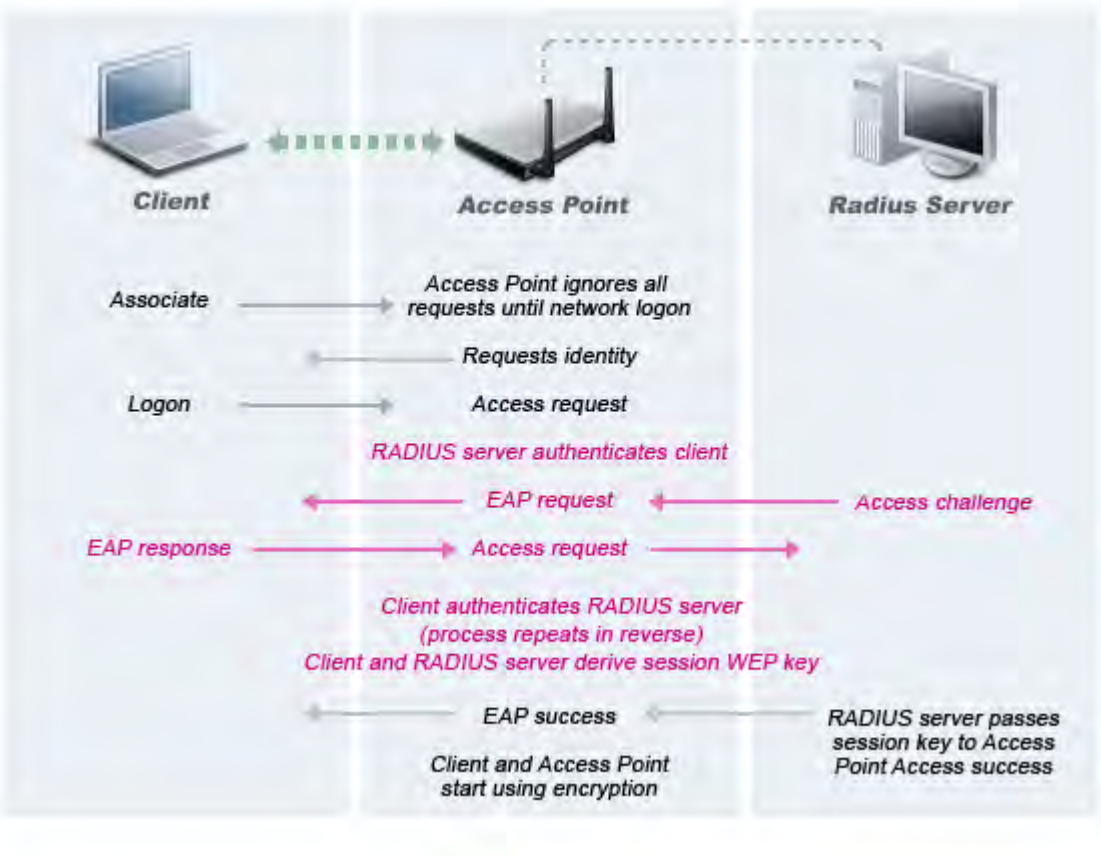
Denial-of-Service Attack Against Client Station

Denial-of-Service attacks against wireless client stations are typically carried out based upon the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and can therefore be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 dis-association or de-authentication frame from the AP to the client station. The 802.11 association state machine as specified by the IEEE standard is illustrated below to show how an associated station can be tricked out of the ***authenticated and associated*** state by various types of spoofed frames.



802.11 Association and Authentication State Machine

Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state, thus disrupting wireless service. See the diagram below for 802.1x authentication and key exchange state change.



802.1x User Authentication Process

AirMagnet WiFi Analyzer tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the AirMagnet WiFi Analyzer attack detection and statistical signature matching process. Detected DoS attacks result in AirMagnet WiFi Analyzer alarms that include a detailed description of the alarm and target device information.

Denial-of-Service Attack Against Infrastructure

In addition to attacking APs or client stations, a wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for Denial-of-Service attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a Distributed Denial-of-Service (DDoS) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not even require a successful authentication, but just the act of attempting authentication to perform the attack.

Several different attacks are covered under this section:

- CTS flood attack
- Queensland University of Technology exploit
- RF jamming attack

- Virtual carrier attack

Configuration Error

It is relatively easy to get the WLAN up and running, but it can be much harder to keep a medium- to large-scale WLAN deployment running efficiently and reliably. Sometimes the WLAN efficiency and reliability issues are caused by configuration errors. Some of the most important configuration parameters to optimize performance are:

- minimum transmit speed
- long or short preamble
- **PCF**/**DCF** function
- **RTS**/**CTS** threshold
- fragmentation threshold
- maximum retry count
- multiple **SSIDs**
- More...

AirMagnet WiFi Analyzer monitors and tracks the usage of these configuration parameters. Alarms are raised when errors are detected; for example, when the SSID used by infrastructure mode devices and ad-hoc mode devices is the same, which should never be the case in a secure WLAN environment. In addition, inconsistent configurations between devices using the same SSID triggers AirMagnet WiFi Analyzer alarms; for example, when within the same SSID, an AP uses short RF preamble while another uses long RF preamble. This can cause problems for the wireless stations that roam between these two APs with different configurations. AirMagnet WiFi Analyzer keeps your WLAN configuration consistent and optimal by notifying you of any abnormal configuration issues and also suggests the optimal configuration that should be used.

Device Down or Malfunction

When wireless service is disrupted, it is usually due to infrastructure equipment failure (broken antenna, power failures, or the AP radio interface going down). Some of these problems may eventually recover by themselves, leaving no trace of evidence for tracking down the root cause until they happen again. Others, however, may not recover, disrupting wireless service for a prolonged period of time. These are some of the most critical issues that need to be detected and dealt with immediately.

AirMagnet WiFi Analyzer can detect these problems by monitoring the airwaves and analyzing information collected by the AirMagnet-supported WLAN cards. In addition to detecting any infrastructure devices missing in action (typically, AP down), AirMagnet Wi-Fi Analyzer also detects AP firmware resets and 802.11 power-save management function implementation flaws, both of which are known problems for some wireless devices.

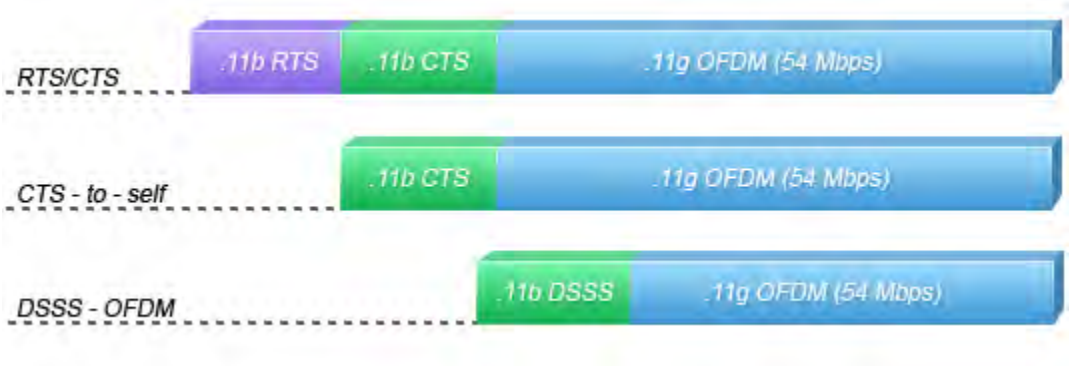
IEEE 802.11n and 802.11g Issues

IEEE 802.11n Issues

The ‘n’ amendment to the 802.11 specification provides many new features and enhancements to achieve maximum throughput of at least 100 Mbps. Both the physical (PHY) and medium access control (MAC) layers are enhanced such that it is possible to achieve data rates of 600 Mbps. At the PHY layer, features such as MIMO, Spatial Multiplexing, Transmit Beamforming, Space-time Block Coding, 40-MHz Channel Width and Short Guard Interval were introduced; and efficiency at the MAC layer is improved by techniques such as Frame Aggregation and Block ACK. In addition, coexistence features are specified, which allow the 802.11n network to be backwards-compatible and coexist with legacy (that is, 802.11 a/b/g) systems. For a detailed discussion of the features of the 802.11n wireless network protocol and their impact on the wireless LAN industry, please refer to the AirMagnet technical white paper titled "The Benefits and Challenges of 802.11n" which is posted on AirMagnet's Web site at https://airmagnet.netally.com/my_airmagnet/.

IEEE 802.11g Issues

When the 802.11g standard got approved by the Institute of Electrical and Electronic Engineers (IEEE), it generated a great deal of interest among wireless users. This interest level was second only to the interest generated during the introduction of the 802.11b standard. The 802.11g standard not only makes high data rates comparable to the 802.11a standard available, but most importantly provides backward compatibility to the widely implemented 802.11b standard.



IEEE Standards on 802.11 a/b/g and other related MAC layer specification

Just like 802.11b devices, 802.11g devices operate in the 2.4 Ghz Industrial Scientific Medical (**ISM**) band, except they use Orthogonal Frequency Division Multiplexing (**OFDM**) technology for extended speed and bandwidth (6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates). The 802.11g standard also supports Barker Code and Complementary Code Keying (**CCK**) modulation, which gives it 1, 2, 5.5 and 11 Mbps data rates for backward compatibility with the 802.11b standard. Similar to the 802.11b standard, 802.11g devices are limited to three non-overlapping channels and the new physical layer is called the Extended Rate Physical (**ERP**) layer. Traditionally, 802.11b and 802.11g devices communicate using **CCK** and **OFDM** modulation schemes respectively but 802.11g devices have to support both modulation schemes to ensure backward compatibility.

Standard Approved	802.11	802.11a	802.11b	802.11g
Available Bandwidth	83.5MHz	300MHz	83.5MHz	83.5MHz
Unlicensed Frequencies	2.4 - 2.835GHz	5.150 - 5.250GHz (UNI-1) 5.150 - 5.250GHz (UNI-1) 5.150 - 5.250GHz (UNI-1)	2.4 - 2.835GHz	2.4 - 2.835GHz
Spread Spectrum	FHSS & DSSS	OFDM	DSSS	DSSS & OFDM
Non-overlapping Channels	3 (indoor and outdoor)	4 (indoor UNII-1) 4 (indoor/outdoor UNII-2) 4 (outdoor UNII-3)	83.5MHz	83.5MHz
Channels	FHSS - 78	36, 40, 44, 48 (UNII-1) 52, 56, 60, 64 (UNII-2) 149, 153, 157, 161 (UNII-3)	1-11 1, 6, 11(nonoverlapping)	1-11 1, 6, 11(nonoverlapping)
Data Rates per Channel	2, 1 Mbps	54, 48, 36, 24, 18 ,12 ,9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps
Modulation Type	DQPSK: 2Mbps DSSS DBPSK: 1Mbps DSSS 4GFSK: 2Mbps FHSS 2GFSK: 1Mbps FHSS	BPSK: 6, 9 Mbps QPSK: 12, 18 Mbps 16-QAM: 24, 36 Mbps 64-QAM: 48, 54Mbps	DQPSK/CCK: 11, 5.5 Mbps DQPSK: 1Mbps	OFDM/CCK: 6, 9, 12, 18, 24, 36, 48, 54 OFDM: 6, 9, 12, 18, 24, 36, 48, 54 DQPSK/CCK: 33, 22, 11, 5.5 Mbps DQPSK: 1Mbps DBPSK: 1Mbps
Power: North America	1000 mW 36 dBM EIRP Using a 6dBI Antenna	UNII - 1: 40mW UNII - 2: 200mW UNII - 3: 800mW Using a 6dBI Antenna	1000 mW 36 dBM EIRP Using a 6dBI Antenna	1000 mW 36 dBM EIRP Using a 6dBI Antenna
Power: Europe			100 mW	
Power: Japan			100 mW	

802.11 a/b/g Range and Modulation Types

Pure 802.11g WLAN (WLAN without 802.11b devices) implements the extra speed and bandwidth supported by the 802.11g standard easily; however, when 802.11b devices are introduced into the network, they add a new level of complexity for the b/g mixed mode environment. Then 802.11g devices can only obtain the benefit through their backward compatibility mode, and this backward compatibility feature of the 802.11g standards comes with overheads. If it is not managed and configured carefully, the benefits 802.11g can be easily lost, and the performance of the existing 802.11b devices could be reduced as well. For more details, please refer to the AirMagnet web site (https://airmagnet.netally.com/my_airmagnet/) to download the AirMagnet white paper "802.11g - the need for speed."

Policy

Desc

 Alarm

Index