

Assessing Wireless Security with AiroPeek





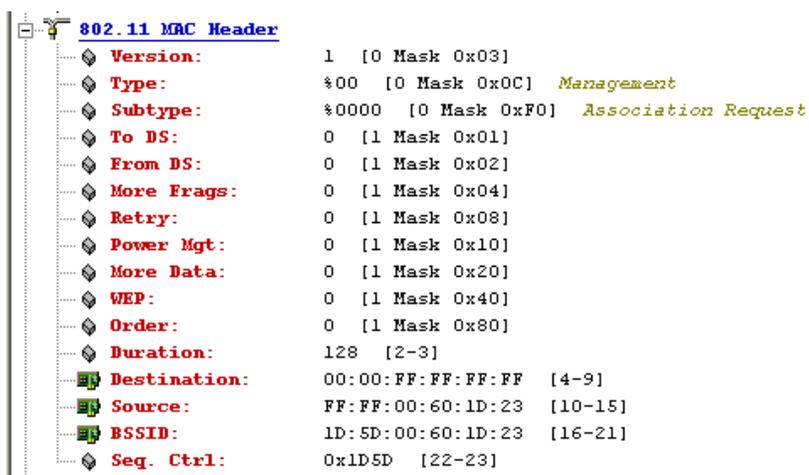
Joe Bardwell
Vice President of Professional Services
WildPackets, Inc.

Intrusion Detection with AiroPeek

It is possible for a user to plug an unauthorized access point into an 802.11 wireless LAN and create a security exposure for the network. The determination of the identity of an unauthorized 802.11 user, or access point, is easily accomplished using AiroPeek. AiroPeek can readily identify this type of security breach as well as notify the appropriate people by paging or email. In this way, you can create an automated intrusion detection scenario for your wireless LAN environment.

For this intrusion detection system to be effective, it is assumed that the person doing the intrusion detection knows the ESSIDs or BSSIDs associated with the WLAN being inspected. Armed with that information, it is a matter of setting appropriate filters and configuring AiroPeek to capture and send notification when a foreign participant joins the WLAN.

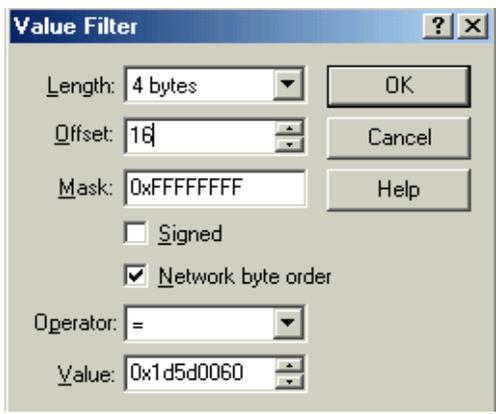
The first step in setting up AiroPeek to identify rogue access points is to create a list of the authorized BSSIDs or ESSIDs in use in the network. An AiroPeek Advanced Filter is then created to EXCLUDE all of the authorized access points. This filter is created by capturing normal network traffic and determining the data offset in an 802.11 frame corresponding to the ESSID or BSSID.



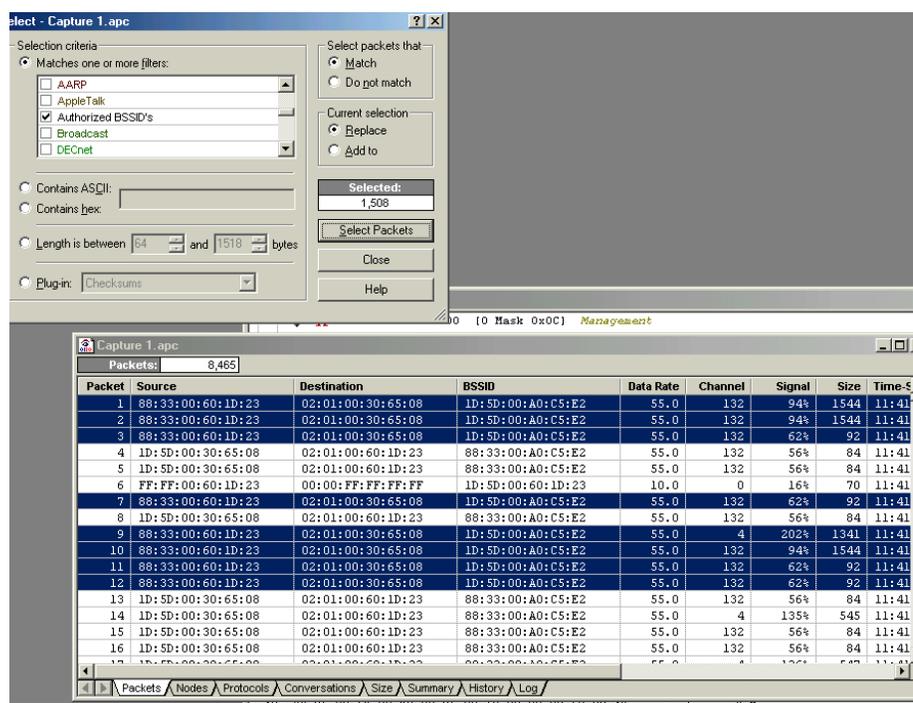
The image shows a Wireshark packet capture of an 802.11 MAC Header. The packet is expanded to show the following fields:

Field Name	Value	Offset
Version:	1	[0 Mask 0x03]
Type:	0000	[0 Mask 0x0C] Management
Subtype:	0000	[0 Mask 0xF0] Association Request
To DS:	0	[1 Mask 0x01]
From DS:	0	[1 Mask 0x02]
More Frags:	0	[1 Mask 0x04]
Retry:	0	[1 Mask 0x08]
Power Mgt:	0	[1 Mask 0x10]
More Data:	0	[1 Mask 0x20]
WEP:	0	[1 Mask 0x40]
Order:	0	[1 Mask 0x80]
Duration:	128	[2-3]
Destination:	00:00:FF:FF:FF:FF	[4-9]
Source:	FF:FF:00:60:1D:23	[10-15]
BSSID:	1D:5D:00:60:1D:23	[16-21]
Seq. Ctrl:	0x1D5D	[22-23]

The portion of the AiroPeek packet detail window, pictured above, discloses a BSSID that is in use in the WLAN. AiroPeek indicates that this value is located at offset 16.



Next, you must specify the BSSID value in the creation of an AiroPeek Advanced Filter, as shown above. If more than one BSSID is in use in the WLAN, then they can all be specified in the single Advanced Filter. This filter might be named, "Authorized BSSIDs" for convenience.



When the Advanced Filter is applied to a previously captured trace file, you will see the AiroPeek screen pictured above. Notice that only those frames that are part of the "Authorized BSSID" list are highlighted (selected) in the display.

AiroPeek can perform multiple, simultaneous, independent capture operations, each having its own separate buffer space into which frames are placed. You create a capture buffer and specify that all frames that MATCH the Authorized BSSID list are to be EXCLUDED from the buffer. That means that ONLY ROGUE ACCESS POINTS WILL BE CAPTURED INTO THIS BUFFER.

In addition to managing captured data in separate buffers, AiroPeek allows buffer-specific alarms to be configured. In this Rogue Access Point buffer, an alarm is created that is triggered on the basis of Frame Count. If the Frame Count exceeds zero, the alarm goes off. (That is, if any frames are detected from a rogue access point, then an alarm will be triggered.)

Finally, a notification process is specified. AiroPeek can either send an email, assuming an Ethernet connection is available for mail transmission, or operate in its capacity as an analyzer. When any wireless NIC is configured in promiscuous mode (for use with any protocol analyzer), it is no longer able to communicate as a participant in the WLAN. This is an either/or situation. Either the computer is a node on the WLAN or it is functioning as an analyzer. Alternatively, AiroPeek can use a modem interface to dial out to a pager.

While AiroPeek is functioning as an automatic rogue access point detector, it can still be used normally to troubleshoot and analyze WLAN traffic. Since multiple capture buffers can be created, it is simply a matter of opening a new buffer and using AiroPeek in the normal manner for network troubleshooting and analysis. The Rogue Access Point buffer continues to operate in the background. All simultaneous buffers have access to all packets. The buffers are not implemented as "leaky buckets." That is, if a "leaky bucket" implementation were used, then frames that were acquired in Buffer #1 would not "leak out" into Buffer #2. AiroPeek does not use a leaky bucket algorithm when processing multiple buffers. All buffers have access to all packets, and all buffers operate independently.

In this way, AiroPeek acts as an automated rogue access point detection tool while maintaining all of its normal functionality as a WLAN analyzer.

Locating A Rogue Access Point's Physical Position

As far as physically locating an intruder, it must be remembered that AiroPeek is a PROTOCOL analyzer, and not an RF test tool. Tools are available on the market that allow directional identification of RF signals. AiroPeek can quickly pinpoint the 802.11 channels that are in use in a particular environment. Knowing the channel usage in a particular location provides the information about the signal frequencies that are being used. By using a directional RF signal strength meter, it is possible to triangulate the location of an RF transmitter. Suffice it to say, a high-end directional RF signal strength meter (and hence, an expensive device) can pinpoint the location

with great accuracy. More realistically, a lower-end tool will be able to provide the location of an intruder to within several meters.

In the same way that AiroPeek is most effective when used by an experienced, trained engineer, so too, an RF signal strength meter is simply a tool that is dependent on the user's expertise to provide accurate information. When one thinks about RF signal detection, it is easy to slip into pictures of clandestine operatives working for the intelligence agency; locating foreign intruders in sensitive networks. The realm of signal detection engineering and methodology can seem somewhat "cloak-and-dagger" and the techniques, tools, and methodologies are, without a doubt, being used for national security.

The network manager of a commercial, corporate, or educational network should carefully weigh the need for RF-level network analysis, since this area of technology is significantly different from the LAN/WAN world of TCP/IP protocols with which we are all familiar.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

On-Site Consulting

When protocol analysis support is needed at your site, the network experts at WildPackets will work with you and your support team to resolve network problems.

Performance Baseline and Network Capacity Planning Report

When it is necessary to know the real performance and capacity issues facing your network, a WildPackets consultant can create a baseline report, from a simple evaluation of a single critical server or router up to an assessment of your overall network infrastructure.

Infrastructure Design Analysis Services

The network experts at WildPackets can help you sort through the details of multi-vendor proposals for hardware and software installation and systems integration, providing you with an un-biased, third party perspective on your proposed network planning,

Remote Consulting Services

WildPackets' Remote Consulting Services may resolve challenging network problems for you without requiring an on-site visit. Our protocol analysis experts will accurately analyze specific trace files you send in to them or capture live traffic from your network and provide a general characterization of network performance and potential problems.

WildPackets Academy

WildPackets Academy offers the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for both Ethernet and 802.11b wireless LANs. WildPackets Academy also provides instruction and testing for the industry-standard **NAX™ (Network Analysis Expert) Certification**.

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit <http://www.wildpacketsacademy.com>. NAX examination and certification details are available at <http://www.nax2000.com>.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek and AiroPeek, led by a WildPackets Academy Instructor. Please visit <http://www.wildpackets.com/events> for complete details and scheduling information.

WildPackets, Inc.

Since its inception in 1990, WildPackets has been developing affordable tools designed to simplify the complex tasks associated with designing, maintaining, troubleshooting and optimizing computer networks. In the past eighteen months, WildPackets has acquired two key partner organizations and greatly expanded its product development expertise and professional services capabilities in the process. WildPackets customers include Ameritech, Cisco Systems, Lucent Technologies, Microsoft, National Institutes of Health, Yahoo! and others. Strategic partners include Cisco Systems, Symbol Technologies and Agere Systems.

WildPackets, Inc.
2540 Camino Diablo
Walnut Creek, CA 94596
Tel 925-937-7900
Fax 925-937-2479

