WildPackets' Guide to Wireless LAN Analysis

Executive Summary

The market for wireless communications has grown rapidly since the introduction of 802.11 wireless local area networking (WLAN) standards. Business organizations value the simplicity and scalability of WLANs as well as the relative ease of integrating wireless access with existing network resources. WLANs support user demand for seamless connectivity, flexibility and mobility. This paper provides a brief overview of wireless networks and the 802.11 WLAN standards, followed by a presentation of troubleshooting wireless network problems with the types of analysis required to resolve them. WildPackets' AiroPeek, AiroPeek NX and RFGrabber are expressly designed to meet the challenges of today's 802.11 wireless network demands.

June, 2003

WildPackets' Guide to Wireless LAN Analysis

WildPackets’ Guide to Wireless LAN Analysis

The world is going wireless. The prohibitive costs of building wired network infrastructures have paved the way for wireless networking on a global scale, so that even the most remote parts of the globe have coverage undreamed of only a few years ago.

Today’s corporate network manager needs to understand not only how the wireless revolution is taking place, but also how wireless technology will affect the day to day monitoring and management of network data. This paper provides a brief overview of wireless networks and the 802.11 WLAN standards, followed by a presentation of troubleshooting problems specific to wireless networks with the types of analysis required to resolve them.

Overview of wireless networking

The market for wireless communications has grown rapidly since the introduction of 802.11 wireless local area networking (WLAN) standards in the late 1990s. Business organizations value the simplicity and scalability of WLANs, and the relative ease of integrating wireless access with existing network resources such as servers, printers, and Internet connections. WLANs support user demand for seamless connectivity, flexibility and mobility.

According to research by Infonetics, sales of wireless LAN products will more than double by 2006. Analysts at Infonetics have projected that “international revenues from wireless hardware, primarily based on the 802.11 standard, would reach $2.72 billion in 2006, up from $1.68 billion in 2002.”

Maintaining the security, reliability and overall performance of a wireless LAN requires the same kind of ability to look “under the hood” as the maintenance of a wired network. Wireless networking presents some unique challenges for the network administrator, however, and requires some new approaches to familiar problems. In order to see what these are—and why they are—we need to know something about how WLANs work.

Development of the IEEE 802.11 WLAN standards

In 1997, IEEE approved 802.11, the first internationally sanctioned wireless LAN standard. This first standard proposed any of three (mutually incompatible) implementations for the physical layer: infrared (IR) pulse position modulation, or radio frequency (RF) signalling in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The IR method was never commercially implemented. The RF versions suffered from low transmission speeds (2 Mbps). In an effort to increase throughput, IEEE established two working groups (A and B) to explore alternate implementations of 802.11. A third group, Working Group G, was set up after these two.

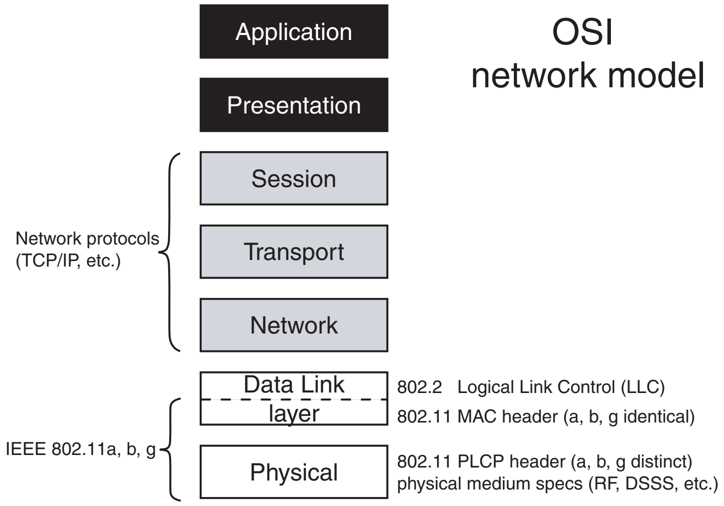

Application
Presentation
Session
Transport
Network
Data Link layer
Physical
OSI network model
Network protocols (TCP/IP, etc.)
IEEE 802.11a, b, g
802.2 Logical Link Control (LLC)
802.11 MAC header (a, b, g identical)
802.11 PLCP header (a, b, g distinct)
physical medium specs (RF, DSSS, etc.)

Figure 1 802.11 and the OSI Model

802.11a

Working Group A explored the 5.0 GHz band, using orthogonal frequency division multiplexing (OFDM) to achieve throughputs in the range of 54 Mbps. The challenges, both to produce low cost equipment operating at such high frequencies and to reconcile competing international uses of this spectrum, kept their 802.11a WLAN standard from reaching the market before mid-2002.

European regulators require 802.11a WLAN devices to support the added functions of dynamic frequency selection (DFS) and transmit power control (TPC). These help to avoid or mitigate interference between 802.11a WLANs and existing 5.0 GHz band uses.

802.11b

Working Group B explored more sophisticated DSSS techniques in the original 2.4 GHz band. Their 802.11b WLAN standard, published in September 1999, can deliver raw data rates of up to 11 Mbps. The majority of WLAN systems in the market today follow the 802.11b WLAN standard.

802.11g

The IEEE Working Group G began by exploring a variety of methods to further improve throughput in the 2.4 GHz spectrum used by the 802.11b standard, In May 2001, the FCC removed its ban on the use of OFDM technology in the 2.4GHz band. In November of 2001, Working Group G tabled a draft standard adopting OFDM, the same signalling method used in the 802.11a WLAN standard. The 802.11g WLAN standard is not absolutely finalized at this writing, but the main outlines are clear. One significant aspect of 802.11g is the degree to which it supports backward compatibility with the older 802.11b standard, which uses the same spectrum. When 802.11b nodes are present, 802.11g nodes use the RTS/CTS as a prelude to each packet transmission. Although the maximum raw data rates for 802.11g WLANs are as high as those of 802.11a WLANs, the actual data throughput for 802.11g drops significantly when 802.11b nodes are present. Mixed 802.11b/g networks are possible, but the maximum performance will be much higher in a pure 802.11g WLAN.

A family of wireless standards

The 802.11 WLAN protocols specify the lowest layer of the OSI network model (physical) and a part of the next higher layer (data link). A stated goal of the initial IEEE effort was to create a set of standards which could use different approaches to the physical layer (different frequencies, encoding methods, and so forth), and yet share the same higher layers. They have succeeded, and the Media Access Control (MAC) layers of the 802.11a, b, and g protocols are substantially identical. At the next higher layer still, all 802.11 WLAN protocols specify the use of the 802.2 protocol for the logical link control (LLC) portion of the data link layer. In the OSI model of network stack functionality (see Figure 1), such protocols as TCP/IP, IPX, NetBEUI, and AppleTalk exist at still higher layers, and utilize the services of the layers underneath.

Radio frequencies and channels

The most striking differences between WLANs and wired networks such as Ethernet are those imposed by the difference in the transmission medium. Where Ethernet sends electrical signals through wires, WLANs send radio frequency (RF) energy through the air. Wireless devices are equipped with a special network interface card (NIC) with one or more antennae, a radio transceiver set, and circuitry to convert between the analog radio signals and the digital pulses used by computers.

Radio waves broadcast on a given frequency can be picked up by any receiver within range tuned to that same frequency. Effective or usable range depends on a number of factors. In general, higher power and lower frequency increase the range at which a signal can be detected. Distance from the signal source and interference from intervening objects or other signals all tend to degrade reception. Filtering, accurate synchronous timing, and a variety of error correcting approaches can help distinguish the true signal from reflections and interference.

Information is carried by modulating the radio waves. In spread spectrum technologies, additional information is packed into a relatively small range of frequencies (a section of bandwidth called a channel) by having both sender and receiver use the same set of codes, such that each small modulation of the set of radio waves carries the greatest possible information. Direct sequence spread spectrum (DSSS) is one particular approach to packing more data into a given piece of RF spectrum. OFDM is another.

The FCC in the United States and other bodies internationally control the use of RF spectrum and limit the output power of devices. The 802.11 WLAN standards attempt to deliver maximum performance within the limits set by these bodies, current radio technology and the laws of physics.

Low output power, for example, limits 802.11 WLAN transmissions to fairly short effective ranges measured in hundreds of feet. Signal quality, and hence network throughput, diminishes with distance and interference. The higher data rates rely on more complex spectrum spreading techniques. These in turn require an ability to distinguish very subtle modulations in the RF signals.

Signal and noise measurement

The electrical energy in radio waves and other electrical signals is often measured in the unit of power Watts or, in the case of 802.11 WLANs, milliwatts (mW). For example, a typical 802.11b WLAN card might have a transmit power of 32 mW. The energy detected at the receiving antenna would be several orders of magnitude smaller than this. The wide range of values encountered in radio engineering could be expressed with exponential notation, but radio engineers came up with a simpler solution. They measure signal strength with a unit called the decibel milliwatt, or dBm.

A decibel is simply a unit of relationship between two power measurements. It is, in fact, one tenth of the exponent of ten. That is, 10 decibels denotes an increase by a factor of 10, 20 decibels an increase by a factor of 100, and 30 decibels an increase by a factor of 1,000. These correspond to 10 raised to the power of (10/10), 10 raised to the power of (20/10), and 10 raised to the power of (30/10), respectively.

Decibels are dimensionless. By associating decibels with a particular unit, it is possible to write and compare a wide range of power values easily. By the definition of the decibel milliwatt, 0 dBm = 1 mW. Power values larger than 1 mW are positive numbers. Power values smaller than 1 mW are expressed as negative numbers. Remember, this is an exponent. For example, the power output of 32mW mentioned above could be written as 15 dBm. A typical lower limit of antenna sensitivity for an 802.11b WLAN card might be expressed as -83 dBm. A more practical lower limit might be -50 dBm, or 0.00001 mW.

Not all 802.11 WLAN cards report signal strength in dBm. The 802.11 WLAN standard itself calls for makers to implement their own scale of received signal strength, and report that within the protocol as a value called Received Signal Strength Indicator (RSSI). While one manufacturer might use a scale of 0-31, another might use 0-63. AiroPeek regularizes these values to a percentage and reports them as signal strength.

Noise is also a form of electrical energy, and is reported in the same way, either as a percentage or in dBm. The signal to noise ratio is simply the difference between signal and noise.

Transmission rates and channels

To overcome signal degradation problems, 802.11 WLANs can gracefully step down to a slower but more robust transmission method when conditions are poor, then step back up again when conditions improve.

The full set of data rates for all three standards is shown in Table 1. For 802.11a WLANs, the 6, 12, and 24 Mbps data rates are mandatory; all others are optional. The 802.11g WLANs will support all the same data rates as 802.11a WLANs when communicating with other 802.11g WLAN nodes, but can also use the same rates as the 802.11b WLAN when communicating with nodes using that older standard. In addition, 802.11g WLANs may support rates in the range of 22 Mbps using optional encoding methods such as PBCC.

Table 1 **Supported data rates by WLAN standard**

802.11a	802.11b	802.11g
	1 Mbps	1 Mbps
	2 Mbps	2 Mbps
	5.5 Mbps	5.5 Mbps
6 Mbps		6 Mbps
9 Mbps		9 Mbps
	11 Mbps	11 Mbps
12 Mbps		12 Mbps

Table 1 **Supported data rates by WLAN standard (continued)**

802.11a	802.11b	802.11g
		22 Mbps
24 Mbps		24 Mbps
36 Mbps		36 Mbps
48 Mbps		48 Mbps

The 802.11b WLAN standard uses DSSS in the 2.4 GHz band. Taking 2412 MHz as the center frequency of the first channel, the standard described 14 channels, 5 MHz apart, numbered 1 to 14. In the United States, the FCC allocated bandwidth to support the first 11 channels. Regulatory bodies in other jurisdictions made different allocations from within this same band.

The 802.11g WLAN standard uses the same spectrum and channels as 802.11b WLANs, but uses the OFDM encoding and transmission methods of the 802.11a WLAN standard.

The 802.11a WLAN standard uses OFDM in the 5.0 GHz band. The standard defines channels 1-199, starting at 5.005 GHz, with their center frequencies spaced 5 MHz apart. The FCC in the United States has allocated bandwidth in three parts of the spectrum, as shown in Table 2. The ETSI and ERM in Europe, MKK in Japan, and other regulatory agencies in other jurisdictions have made their own allocations within this band.

Table 2 **FCC Channels for 802.11a WLANs**

Band	Center frequency	Channel number	Maximum power
U-NII low band (5150 MHz to 5250 MHz)			
	5180 MHz	**36**	40 mW
	5200 MHz	**40**	40 mW
	5220 MHz	**44**	40 mW
	5240 MHz	**48**	40 mW
U-NII medium band (5250 MHz to 5350 MHz)			
	5260 MHz	**52**	200 mW
	5280 MHz	**56**	200 mW
	5300 MHz	**60**	200 mW
	5320 MHz	**64**	200 mW
U-NII high band (for outdoor use) (5725 MHz to 5825 MHz)			
	5745 MHz	**149**	800 mW

Table 2 FCC Channels for 802.11a WLANs (continued)

Band	Center frequency	Channel number	Maximum power
	5765 MHz	**153**	800 mW
	5785 MHz	**157**	800 mW
	5805 MHz	**161**	800 mW

Notice that the channel numbers for 802.11a WLANs appear in a gapped sequence, with 20 MHz separating the center frequency of one allocated channel from the next. This is a recognition of the fact that the spectrum spreading approaches used in all 802.11 WLAN standards actually take up far more spectrum than 5 MHz. In fact an active channel fills more than 16 MHz.

Collision avoidance and media access

One of the most significant differences between Ethernet and 802.11 WLANs is the way in which they control access to the medium, determining who may talk and when. Ethernet uses CSMA/CD (carrier sense multiple access with collision detection). This is possible because an Ethernet device can send and listen to the wire at the same time, detecting the pattern that shows a collision is taking place. However, when a radio attempts to transmit and listen on the same channel at the same time, its own transmission drowns out all other signals. Collision detection is impossible.

The carrier sense capability of Ethernet and WLANs is also different. On an Ethernet segment, all stations are within range of one another at all times, by definition. When the medium seems clear, it is clear. Only a simultaneous start of transmissions results in a collision. As shown in Figure 2, nodes on a WLAN cannot always tell by listening alone whether or not the medium is in fact clear.

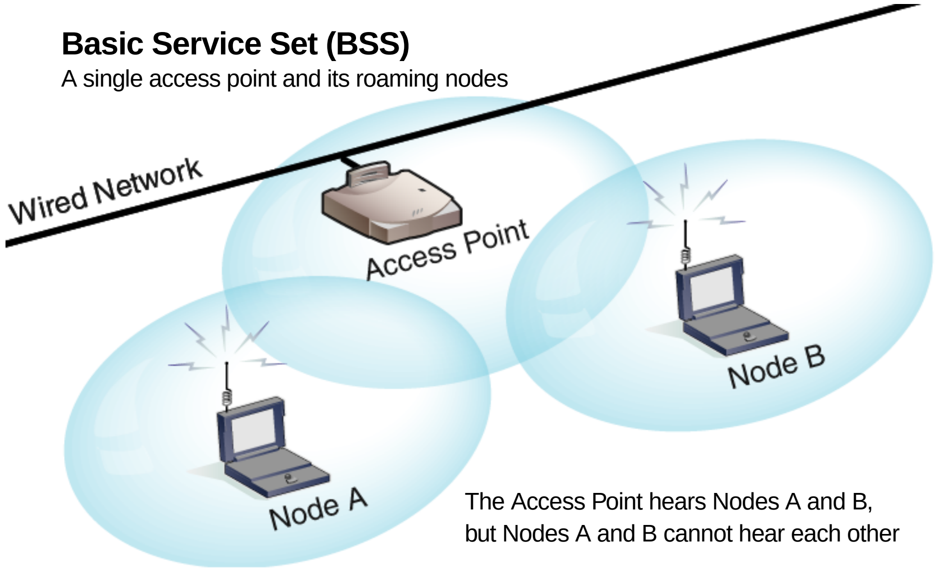

Basic Service Set (BSS)
A single access point and its roaming nodes
Wired Network
Access Point
Node B
Node A
The Access Point hears Nodes A and B,
but Nodes A and B cannot hear each other

Figure 2 Basic Service Set (BSS), showing the hidden node problem.

In a wireless network, a device can be in range of two others, neither of which can hear the other, but both of which can hear the first device. The access point in Figure 2 can hear both node A and node B, but neither A nor B can hear each other. This creates a situation in which the access point could be receiving a transmission from node B without node A sensing that node B is transmitting. Node A, sensing no activity on the channel, might then begin transmitting, jamming the access point's reception of node B's transmission already under way. This is known as the "hidden node" problem.

To solve the hidden node problem and overcome the impossibility of collision detection, 802.11 WLANs use CSMA/CA (carrier sense multiple access with collision avoidance). Under CSMA/CA, devices use a four-way handshake (Figure 3) to gain access to the airwaves to ensure collision avoidance. To send a direct transmission to another node, the source node puts a short Request To Send (RTS) packet on the air, addressed to the intended destination. If that destination hears the transmission and is able to receive, it replies with a short Clear to Send (CTS) packet. The initiating node then sends the data, and the recipient acknowledges all transmitted packets by returning a short ACK (Acknowledgement) packet for every transmitted packet received.

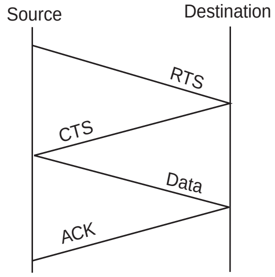


Figure 3 A Four-Way Handshake ensures collision avoidance in 802.11 networks.

Timing is critical to mediating access to the airwaves in WLANs. To ensure synchronization, access points or their functional equivalents periodically send beacons and timing information.

Wireless LAN topologies

Wireless LANs behave slightly differently depending on their topology, or make-up of member nodes. The simplest arrangement is an *ad hoc* group of independent wireless nodes communicating on a peer-to-peer basis, as shown in Figure 4. The standard refers to this topology as an Independent Basic Service Set (IBSS) and provides for some measure of coordination by electing one node from the group to act as the proxy for the missing access point or base station found in more complex topologies. Ad hoc networks allow for flexible and cost-effective arrangements in a variety of work environments, including hard-to-wire locations and temporary setups such as a group of laptops in a conference room.

The more complex topologies, referred to as *infrastructure* topologies, include at least one access point or base station. Access points provide synchronization and coordination, forwarding of broadcast packets and, perhaps most significantly, a bridge to the wired network.

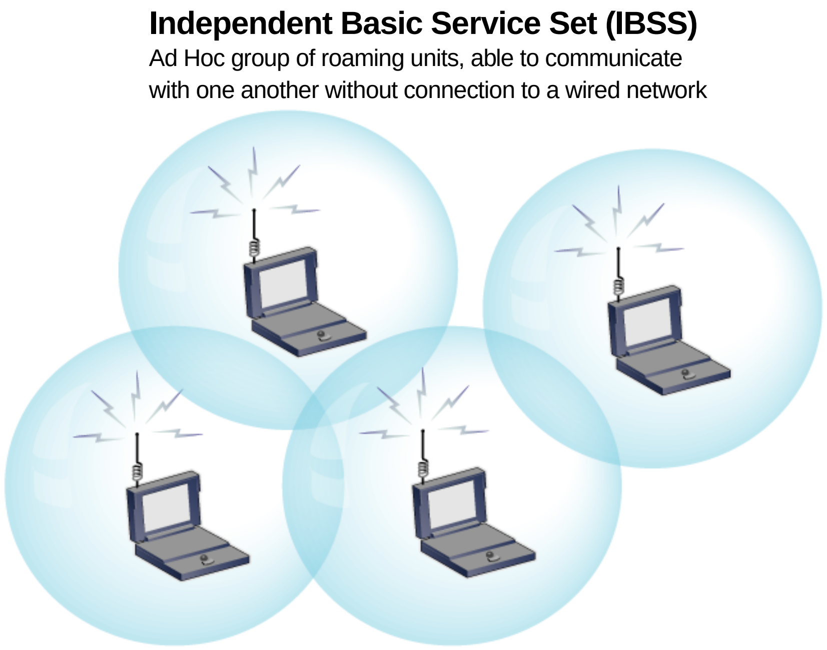

Independent Basic Service Set (IBSS)
Ad Hoc group of roaming units, able to communicate with one another without connection to a wired network

Figure 4 An IBSS or “Ad Hoc” Network.

The standard refers to a topology with a single access point as a Basic Service Set (BSS) as shown in Figure 2. A single access point can manage and bridge wireless communications for all the devices within range and operating on the same channel.

To cover a larger area, multiple access points are deployed. This arrangement (shown in Figure 5) is called an Extended Service Set (ESS). It is defined as two or more Basic Service Sets connecting to the same wired network. Each access point is assigned a different channel wherever possible to minimize interference. If a channel must be reused, it is best to assign the reused channel to the access points that are the least likely to interfere with one another.

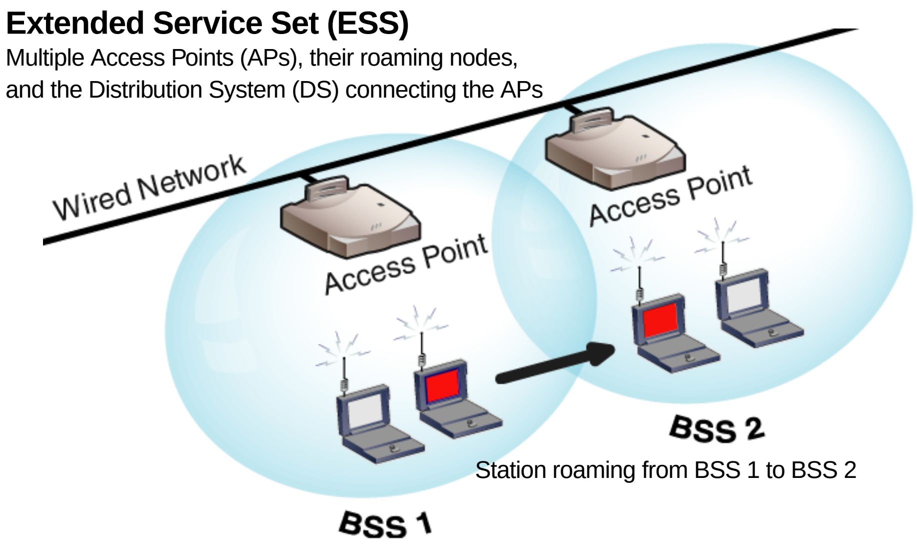

Extended Service Set (ESS)
Multiple Access Points (APs), their roaming nodes, and the Distribution System (DS) connecting the APs
Wired Network
Access Point
Access Point
BSS 2
Station roaming from BSS 1 to BSS 2
BSS 1

Figure 5 Extended Service Set (ESS) supports roaming from one cell to another.

When users roam between cells or BSSs, their mobile device will find and attempt to connect with the access point with the clearest signal and the least amount of network traffic. This way, a roaming unit can transition seamlessly from one access point in the system to another, without losing network connectivity.

An ESS introduces the possibility of forwarding traffic from one radio cell (the range covered by a single access point) to another over the wired network. This combination of access points and the wired network connecting them is referred to as the Distribution System (DS). Messages sent from a wireless device in one BSS to a device in a different BSS by way of the wired network are said to be sent by way of the DS.

Note: To meet the needs of mobile radio communications, 802.11 WLAN standards must be tolerant of connections being dropped and reestablished. The standards attempt to ensure minimum disruption to data delivery, and provide some features for caching and forwarding messages between BSSs. Particular implementations of some higher layer protocols such as TCP/IP may be less tolerant. For example, in a network where DHCP is used to assign IP addresses, a roaming node may lose its connection when it moves across cell boundaries and have to reestablish it when it enters the next BSS or cell. Software solutions are available to address this particular problem. In addition, IEEE may revise the standards in ways that mitigate this problem in future versions.

Whether they have one base station or many, most corporate WLANs will operate in infrastructure mode to access servers, printers, Internet connections and other resources already established on wired networks. Even users seeking an “all wireless” solution may find that an access point does a better job of mediating communications with an Internet connection, for example, and is worth the additional expense.

Security

Secure communications is problematic in all radio networks. A wired network can be secured at its edges, by restricting physical access and installing firewalls, for example. A wireless network with the same measures in place is still vulnerable to eavesdropping. Wireless networks require a more focused effort to maintain security.

This section presents a few basic concepts of communications security, then describes the three main generations of security enhancements to 802.11 WLANs.

Concepts of secure communications

Communications security is often described in terms of three elements:

Authentication ensures that nodes are who and what they say they are.

Privacy ensures that eavesdroppers cannot read network traffic.

Integrity ensures that messages are delivered without alteration.

In the 802.11 WLAN standards, authentication can be open or based on knowledge of a shared key. In any case, authentication is the first step for a device attempting to connect to an 802.11 WLAN. The function is handled by an exchange of management packets. If authentication is open, then any standards-compliant device will be authenticated. If authentication is based on a shared secret, then a device must prove it knows this shared secret in order to be authenticated. Under WEP, the shared secret is a WEP key. Under WPA, the shared secret is evaluated by a separate authentication process, such as RADIUS (Remote Authentication Dial-In User Service).

Privacy is typically protected by encrypting the contents of the message. Encryption applies a known, reversible method of transformation (called a *cipher* or encryption *algorithm*) to the original message contents (called the *plaintext*), scrambling or disguising them to create the *ciphertext*. Only those who know how to reverse the process (*decrypt* the message) can recover the original text. The most common forms of encryption are mathematical transformations which use a variable called a *key* as a part of their manipulations. The intended receiver must know both the correct method and the value of the key that was used, in order to be able to decrypt the message. For commercial encryption schemes, the method will be public knowledge. Protecting the secrecy of the key becomes crucial.

In the context of communications security, integrity refers to the ability to make certain that the message received has not been altered in any way and is identical to the message that was sent. The frame check sequence (FCS) bytes are one example of an integrity check, but they are not considered secure. The ordinary FCS bytes are not calculated over the plaintext message and protected by encryption. Instead they are calculated over the ciphertext, using a known method and sent *in the clear* (unencrypted). The FCS bytes help to identify packets that have been accidentally damaged in transit. An attacker, however, could recalculate the ordinary FCS (for example, to hide their deliberate alteration of a packet they captured and retransmitted). The harder it is for an attacker to correctly recalculate the integrity check sequence or security *hash* function, the more reliable a test of message integrity it is.

The concept of integrity is sometimes extended to include verifying that the source of the message is the same as the stated source. Timestamps and message sequence numbers can protect against “replay attacks,” but, again, they are not considered secure unless they are protected by encryption.

Security is always relative, never absolute. For every defence, there is (or will soon be) a successful attack. For every attack, there is (or will soon be) a successful defense. Only time and effort are really at issue. The better the defense, the more time and effort it takes to breach.

The right defense is the one that is balanced and that matches the expected range of attacks. Balance is important in two senses. First, the weakest link must be secure enough. Second, the passive elements of authentication, encryption, and integrity check must be backed up by active elements such as monitoring for and pursuing attempted breaches, maintaining security discipline, and so forth. The right defense is one in which a breach requires just slightly more time and effort from attackers than they are willing to invest. Security measures impose costs and constraints on the defender. Like any other business decision, these trade-offs must be made with eyes open.

Wired equivalent privacy (WEP)

When the first IEEE 802.11 WLAN standards were being developed, the designers faced many trade-offs. Though they recognized the need for enhanced security, they also wanted the products based on the new standard to be exportable from the United States. In the late 1990s, it appeared that strong encryption would have prevented 802.11 WLAN equipment from being granted export licenses. The designers settled on a very modest (and optional) secure authentication method and encryption scheme called Wired Equivalent Privacy (WEP). The scheme was really only intended to prevent inadvertent eavesdropping, a job it does quite well.

WEP uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. The 802.11 WLAN network headers themselves are not encrypted. Under WEP, the user typically enters from one to four keys of variable length. The software provides the remainder of each key to fill them out to their full length (64, 128, or more bits).

Users of AiroPeek can enter the appropriate WEP keys and have the program decrypt packets on the fly. This makes it possible to troubleshoot higher layer protocols on networks protected by WEP.

In the competitive atmosphere of cryptanalysis, it was not long before the weaknesses of WEP were noted, analyzed, exploited, and the results published. Subsequent versions of WEP made provisions for longer key lengths, but this did not address the frequent reuse of keys, which proved a fatal weakness of WEP. A competent amateur with publicly available tools can crack even the longer WEP keys in a matter of minutes, given a large enough sample of traffic.

While WEP remains useful for casual purposes, large enterprise users soon began to employ it in conjunction with other security technologies such as Virtual Private Networks (VPNs).

802.11i standard

Even before the WEP scheme was published, IEEE had begun various initiatives aimed at improving network security, such as 802.1x. The forthcoming 802.11i standard will provide an integrated framework for network security implemented at the MAC and PHY layers.

The IEEE 802.11i standard is not expected to be fully ratified until late in 2003 or early in 2004. When it is finalized, it will provide a framework capable of accommodating new authentication, encryption, and message integrity check methods as they are developed. Encryption will be based on the Advanced Encryption Standard (AES), among others. Stronger encryption will require hardware acceleration. This means that the strongest implementations of 802.11i will not be backward compatible with older 802.11 WLAN equipment.

Wi-Fi Protected Access (WPA)

While wireless vendors eagerly anticipate the 802.11i standard and have said they will support it, they were unwilling to wait to improve security. In March 2002, the Wi-Fi Alliance (a trade group) published their own set of proposals based on early drafts of the 802.11i standard. They called this set of proposals Wi-Fi Protected Access (WPA).

WPA can be thought of as a subset of 802.11i. It provides a very useful set of stop-gap measures which could be implemented with little or no change to the 802.11 WLAN hardware then in design. The stronger security features, and particularly the stronger encryption methods anticipated from 802.11i will need to be accelerated in hardware if network performance is to be maintained.

WPA makes significant improvements in authentication using 802.1x and Extensible Authentication Protocol (EAP), and in the protection of key secrecy using the Temporal Key Integrity Protocol (TKIP).

EAP comes in several flavors, all of which rely on a central authentication server, such as RADIUS, to authenticate each user on the network before they join. It also employs “mutual authentication” so users don’t accidentally join a rogue network that might steal their own network credentials.

TKIP provides important data encryption enhancements, including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (EIV) with sequencing rules, and a re-keying mechanism. TKIP successfully addresses the most vulnerable aspect of WEP by dramatically reducing the reuse of keys. Michael represents the beginnings of a cryptographic integrity check function.

Packet structure and packet types

Like the rest of the 802 family of LAN protocols, 802.11 WLAN sends all network traffic in packets. There are three basic types: data packets, network management packets and control packets. The first section describes the basic structure of 802.11 WLAN data packets and the information they provide for network analysis. The second section describes the management and control packets, their functions and the role they play in network analysis.

Packet structure

All the functionality of the protocol is reflected in the packet headers. RF technology and station mobility impose some complex requirements on 802.11 WLAN networks. This added complexity is reflected in the long physical layer convergence protocol (PLCP) headers as well as the data-rich MAC header.

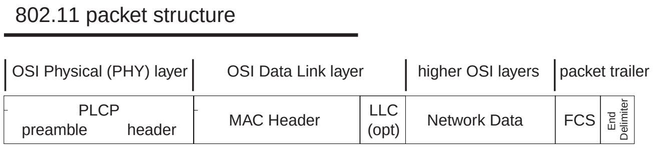
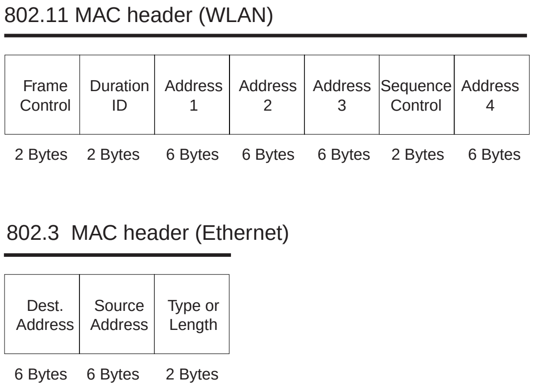


Figure 6 802.11 WLAN data packet structure

Because 802.11 WLANs must be able to form and re-form their membership constantly, and because radio transmission conditions themselves can change, coordination becomes a large issue in WLANs. Management and control packets are dedicated to these coordination functions. In addition, the headers of ordinary data packets contain a great deal more information about network conditions and topology than, for example, the headers of Ethernet data packets would contain.



802.11 MAC header (WLAN)

Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes

802.3 MAC header (Ethernet)

Dest. Address	Source Address	Type or Length
6 Bytes	6 Bytes	2 Bytes

Figure 7 Comparison of MAC headers: 802.11 WLAN to 802.3 Ethernet

A complete breakout of all the fields in the packet headers and the values they may take is beyond the scope of this white paper. For this overview, Table 3 below presents a list of the types of information 802.11 WLAN data packet headers convey. The table also shows the types of information carried in management and control packets.

Table 3 Protocol functions in 802.11 WLANs

Authentication / Privacy	
The first step for a device in joining a BSS or IBSS is authentication. This can be an open or a shared key system. If WEP encryption of packet data is enabled, shared key authentication should be used. Authentication is handled by a request/response exchange of management packets.	
authentication ID	This is the name under which the current station authenticated itself on joining the network.

Table 3 **Protocol functions in 802.11 WLANs (continued)**

WEP enabled	If this field is true, then the payload of the packet (but not the WLAN headers) will be encrypted using Wired Equivalent Privacy.
Network membership / Topology	
The second step for a device joining a BSS or IBSS is to associate itself with the group, or with the access point. When roaming, a unit also needs to disassociate and reassociate. These functions are handled by an exchange of management packets. The current status is shown in packet headers.	
association	Packets can show the current association of the sender. Association and Reassociation are handled by request/ response management packets. Disassociation is a simple declaration from either an access point or a device.
IBSSID or ESSID	The ID of the group or its access point. A device can only be associated with one access point (shown by the ESSID) or IBSS at a time.
probe	Probes are supported by request/response management packets used by roaming devices in search of a particular BSS or access point. They support a roaming unit’s ability to move between cells while remaining connected.
Network conditions / Transmission	
The 802.11 WLAN protocol supports rapid adjustment to changing conditions, always seeking the best throughput.	
channel	The channel or radio frequency used for the transmission
data rate	The data rate used to transmit the packet. 802.11 WLAN nodes can rapidly adjust their transmission data rate to match conditions.
fragmentation	802.11 WLANs impose their own fragmentation on packets, completely independent of any fragmentation imposed by higher level protocols such as TCP/IP. A series of short transmissions is less vulnerable to interference in noisy environments. This fragmentation is dynamically set by the protocol in an effort to reduce the number, or at least the cost, of retransmissions.
synchronization	Several kinds of synchronization are important in WLANs. Network management packets called “beacon” packets keep members of a BSS synchronized. In addition, devices report the state of their own internal synchronization. Finally, all transmissions contain a timestamp.
power save	Laptops in particular need to conserve power. To facilitate this, the protocol uses a number of fields in data packets plus the PS-Poll (power save-poll) control packet to let devices remain connected to the network while in power save mode.
Transmission control	
While the protocol as a whole actually controls the transmission of data, certain header fields and control packets have this as their particular job:	
RTS, CTS, ACK	Request to send, clear to send, and acknowledgement, respectively, these control packets are used in the four way handshake in support of collision avoidance.
version	The version of the 802.11 protocol used in constructing the packet.

Table 3 **Protocol functions in 802.11 WLANs (continued)**

type and sub-type	The type of packet (data, management, or control), with a sub-type specifying its exact function.
duration	In support of synchronization and orderly access to the airwaves, packets contain a precise value for the time that should be allotted for the remainder of the transaction of which this packet is a part.
length	Packet length
retransmission	Retransmissions are common. It is important to declare which packets are retransmissions.
sequence	Sequence information in packets helps reduce retransmissions and other potential errors.
order	Some data, such as voice communications, must be handled in strict order at the receiving end.
Routing	
Again, many fields are related to routing traffic, but the following are most directly related:	
addresses	There are four address fields in 802.11 WLAN data packets, instead of the two found in Ethernet or IP headers. This is to accommodate the possibility of forwarding to, from, or through the distribution system (DS). In addition to the normal Destination and Source addresses, these fields may show the Transmitter, the Receiver, or the BSSID. The type of address shown in each address field depends on whether (and how) the packet is routed by way of the DS. Control and management packets need only three address fields because they can never be routed both to and from (that is, through) the DS.
to/from DS	In an ESS, traffic can be routed from a device using one access point to a device using a different access point somewhere along the wired network. These fields describe routing through the distribution system (DS) and tell the receiving device how to interpret the address fields.
more data	Access points can cache data for other devices. This serves both roaming across BSS or cell boundaries and the power save features. When a device receives a message from an access point, it may be told the access point has more data waiting for it as well.

Management and control packets

Control packets are short transmissions which directly mediate or control communications. Control packets include the RTS, CTS and ACK packets used in the four way handshake (see Figure 3), as well as power save polling packets and short packets to show (or show and acknowledge) the end of contention-free periods within a particular BSS or IBSS.

Management packets are used to support authentication, association, and synchronization. Their formats are similar to those of data packets, but with fewer fields in the MAC header. In addition, management packets may have data fields of fixed or variable length, as defined by their particular sub-type. The types of information included in management and control packets are shown in Table 3, along with the related information found in data packet headers.

Wireless network analysis

Wireless networks require the same kinds of analytical and diagnostic tools as any other LAN in order to maintain, optimize and secure network functions. The 802.11 WLAN standard offers even more data to packet analysis than any of the other members of the 802 family of protocols. This section describes four broad areas in which wireless network analyzers can be of particular use in network troubleshooting and administration.

Configuration and site surveys

One of the advantages of 802.11 WLANs is their ability to dynamically adjust to changing conditions and to almost configure themselves to make the best use of available bandwidth. These capabilities work best, however, when the problems they address are kept within limits.

For example, where interference is high, 802.11 WLAN nodes will continue to increase fragmentation, simplify spectrum spreading techniques and decrease transmission rates. Another symptom of high interference is increased retransmissions, especially when they occur despite high fragmentation. While some network applications may show no ill effects from this condition, others may begin to lag with too many retransmissions of packets already reduced well below their most efficient transmission size. Remember that 802.11 WLAN packet headers are quite large. This means high overhead and a low usable data rate when packet fragmentation and retransmissions are both high. If only one or two network applications seem to be affected, it may not be immediately obvious that there is a more general problem. Using a wireless packet analyzer in such a case can quickly determine the state of the network. Possible sources of interference can be examined and the results tested in near real time.

802.11 WLAN BSSs and ESSs also have the ability to dynamically configure themselves, associating and reassociating roaming nodes, first with one access point and then with another. The physical location and RF channel used by each access point must be chosen by humans, however. These choices can lead to smooth network functioning or to unexpected problems. To help evaluate network topologies, a packet analyzer must be able to display signal strength and transmission rate for each packet found on a given channel. Further, the user must have control over what channel—better still, which base station—the packet analyzer will scan. With these tools, a packet analyzer can be used to build a picture of conditions at the boundaries between cells in an ESS.

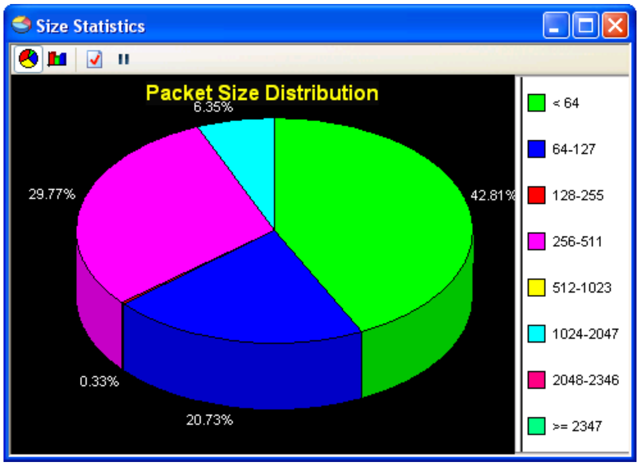


Figure 8 An unusual predominance of small packets may indicate interference.

Such a survey may find dead spots in a particular configuration or identify places where interference seems to be unusually high. Solving the problem may require changing the channel of one or more access points, or perhaps moving one or more to a new location. The effects of each change can quickly be monitored with a packet analyzer.

A wireless analyzer can provide an accurate display of signal and noise on your WLAN by showing a continuously updated bar graph of the most recently reported signal strength, noise, or signal to noise comparison on every channel on which traffic is detected.

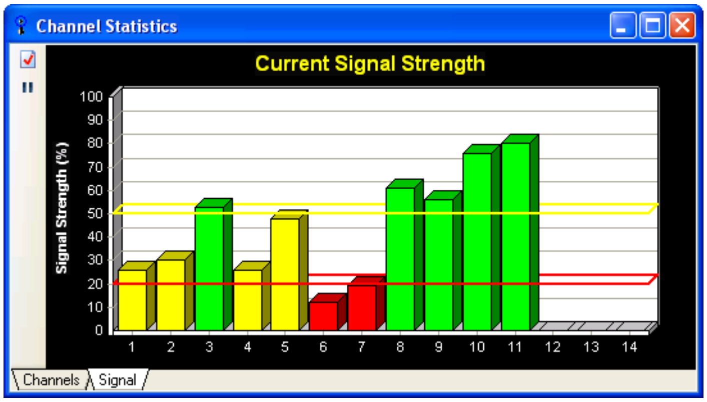
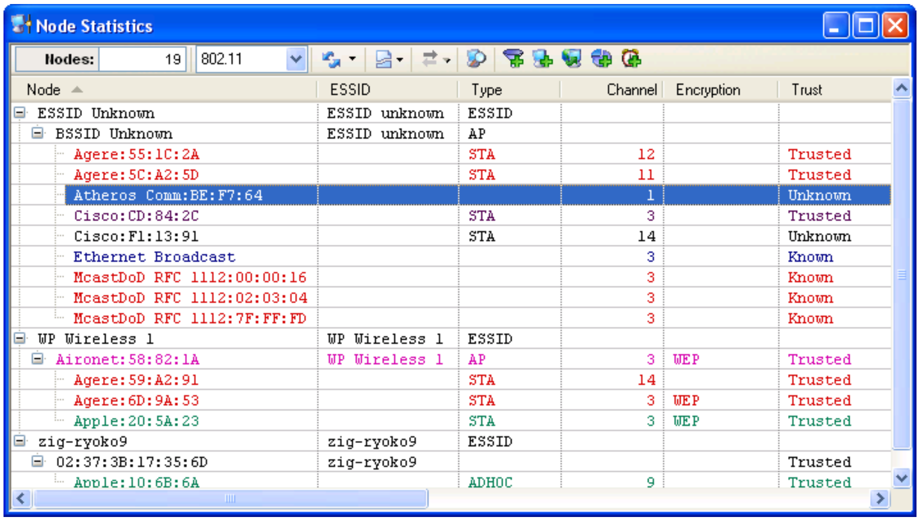


Figure 9 Channel Statistics display channel signal strength.

Wireless networks are made up of one or more radio cells, centered on Access Points (APs). Unlike wired networks, the precise topology of the WLAN changes as clients roam from one AP to the next. The topology can be expressed as a hierarchical tree, with the ESSs (all APs connected to the same DS) at the top, then individual BSSs (individual APs and their clients), then the individual client nodes or stations (STAs).

In AiroPeek, the ***802.11*** view of **Node Statistics** displays the wireless devices on your network in just such a hierarchical tree (Figure 10). Individual devices are identified by their ESSID, BSSID, or MAC address (as appropriate). The view tracks dozens of 802.11 characteristics for each node, including encryption state, authentication method, channel, data rate, signal and noise statistics (dBm or %), and throughput statistics. In AiroPeek NX, the view also shows the Trust value assigned to each node, allowing you to quickly distinguish friend from (potential) foe.



Node	ESSID	Type	Channel	Encryption	Trust
⊟ ESSID Unknown	ESSID unknown	ESSID			
⊟ BSSID Unknown	ESSID unknown	AP			
Agere:55:1C:2A		STA	12		Trusted
Agere:5C:A2:5D		STA	11		Trusted
Atheros Comm:BE:F7:64			1		Unknown
Cisco:CD:84:2C		STA	3		Trusted
Cisco:F1:13:91		STA	14		Unknown
Ethernet Broadcast			3		Known
McastDoD RFC 1112:00:00:16			3		Known
McastDoD RFC 1112:02:03:04			3		Known
McastDoD RFC 1112:7F:FF:FD			3		Known
⊟ WP Wireless 1	WP Wireless 1	ESSID			
⊟ Aironet:58:82:1A	WP Wireless 1	AP	3	WEP	Trusted
Agere:59:A2:91		STA	14		Trusted
Agere:6D:9A:53		STA	3	WEP	Trusted
Apple:20:5A:23		STA	3	WEP	Trusted
⊟ zig-ryoko9	zig-ryoko9	ESSID			
⊟ 02:37:3B:17:35:6D	zig-ryoko9				Trusted
Apple:10:6B:6A		ADHOC	9		Trusted

Figure 10 802.11 view of Node Statistics in AiroPeek NX, showing Trust values and SSIDs.

Identifying potential security problems

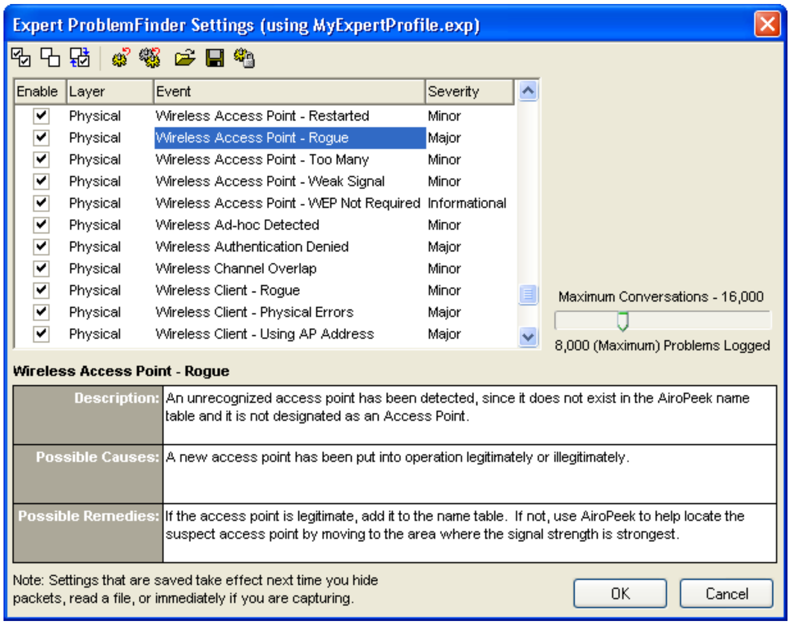
Because they use radio transmissions, WLANs are inherently more difficult to secure than wired LANs. Simple encryption and authentication measures such as WEP prevent outsiders from casually or inadvertently browsing your WLAN traffic, but they cannot stop a deliberate attack. WPA, particularly in its strongest implementations, is quite secure today.

Even the best passive defenses, however, must be paired with an active defense in order to really work. First, attempted breaches must be identified and stopped. Second, networks must be monitored to ensure that security policies are followed.

A good wireless analyzer can be used to monitor compliance with security policies, and to identify, intercept, log, and analyze unauthorized attempts to access the network. Modern network analyzers can automatically respond to security threats in a variety of ways, making them ideal tools both for monitoring and for more focused analysis.

Expert, real-time analyzers scan traffic on a network, looking for anomalies and sub-optimal performance. They provide a set of expert troubleshooting and diagnostic capabilities and problem detection heuristics based on the network problems found. Some examples of security related expert diagnoses include:

- Denial of Service (DoS) attacks
- Man-in-the-Middle attacks
- Lapses in security policy (such as wrong or default configurations)
- Intrusion detection
- Rogue access point and unknown client detection



Expert ProblemFinder Settings (using MyExpertProfile.exp)

Enable	Layer	Event	Severity
☑	Physical	Wireless Access Point - Restarted	Minor
☑	Physical	Wireless Access Point - Rogue	Major
☑	Physical	Wireless Access Point - Too Many	Minor
☑	Physical	Wireless Access Point - Weak Signal	Minor
☑	Physical	Wireless Access Point - WEP Not Required	Informational
☑	Physical	Wireless Ad-hoc Detected	Minor
☑	Physical	Wireless Authentication Denied	Major
☑	Physical	Wireless Channel Overlap	Minor
☑	Physical	Wireless Client - Rogue	Minor
☑	Physical	Wireless Client - Physical Errors	Major
☑	Physical	Wireless Client - Using AP Address	Major

Maximum Conversations - 16,000

8,000 (Maximum) Problems Logged

Wireless Access Point - Rogue

Description:	An unrecognized access point has been detected, since it does not exist in the AiroPeek name table and it is not designated as an Access Point.
Possible Causes:	A new access point has been put into operation legitimately or illegitimately.
Possible Remedies:	If the access point is legitimate, add it to the name table. If not, use AiroPeek to help locate the suspect access point by moving to the area where the signal strength is strongest.

Note: Settings that are saved take effect next time you hide packets, read a file, or immediately if you are capturing.

Figure 11 Expert detection and description of a rogue access point, with possible causes and remedies

With AiroPeek NX, you can assign levels of trust to any node, making it easy to tell at a glance who is who. Keeping a current list of your own network's members is easy, and allows you, for example, to automatically identify and easily locate rogue access points (see Figure 11). Assign a value of Trusted to the devices that belong to your own network. The intermediate value of Known lets you segregate sources that are familiar, but beyond your own control, such as an access point in a neighboring office. Nodes classified as Unknown (the default) can be quickly identified.

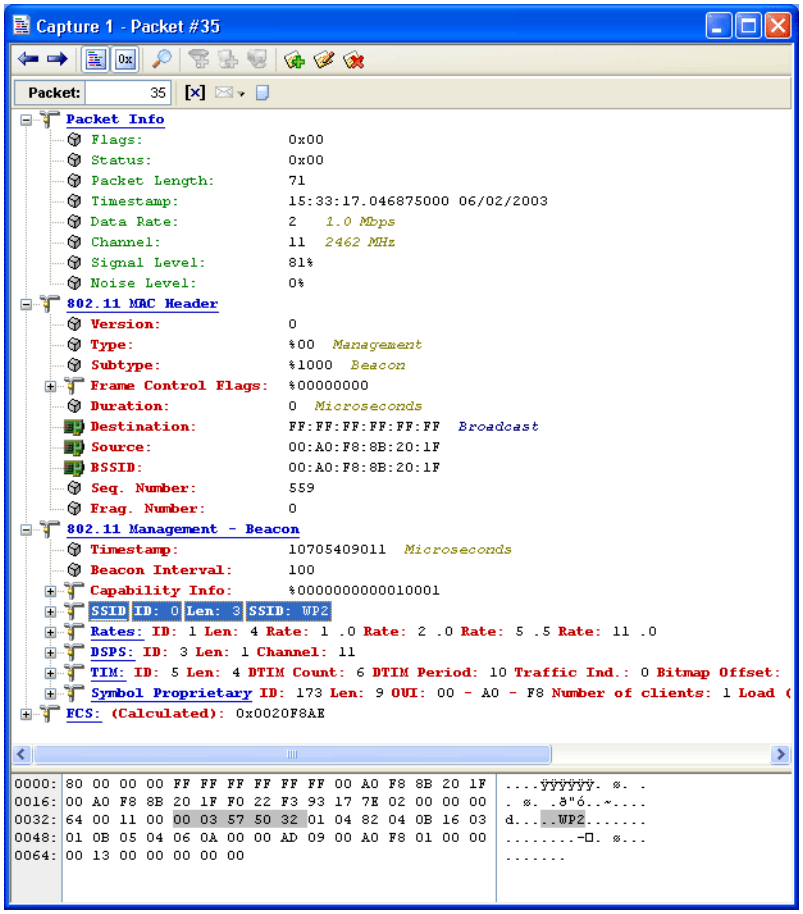
AiroPeek also ships with a security audit template, which you can use as is or extend or modify to meet particular requirements. The template makes use of special filters, alarms, and pre-configured capture sessions to create a basic WLAN security monitoring system. The security audit template scans network traffic in the background, looking for indications of a security breach. When it finds one, it captures the packets that meet its criteria and sends a notification, keeping you informed of suspicious activity on your wireless LAN.

For more on wireless security, please see WildPackets' tutorials on Security Audits and Rogue Access Points.

Analyzing higher level network protocols

Managing a network is more than just managing Ethernet or the WLAN. It also means making sure all the resources users expect to access over the network remain available. This means troubleshooting the network protocols that support these resources. When WLANs are used to extend and enhance wired networks, there is no reason to expect the behavior of higher level protocols on these mobile clients will be any more or less prone to problems than on their wired equivalents.

Although part of this work can be done by capturing traffic from the wired network alone, some problems will yield more quickly to analysis of wireless-originated traffic captured before it enters the DS. To determine whether access points are making errors in their bridging, or if packets are being malformed at the client source, you must be able to see the packets as they come from the client node.



```
Packet: 35
Packet Info
    Flags:                      0x00
    Status:                     0x00
    Packet Length:              71
    Timestamp:                  15:33:17.046875000 06/02/2003
    Data Rate:                  2    1.0 Mbps
    Channel:                    11   2462 MHz
    Signal Level:               81%
    Noise Level:                0%
802.11 MAC Header
    Version:                    0
    Type:                       %00   Management
    Subtype:                    %1000   Beacon
    Frame Control Flags:        %00000000
    Duration:                   0  Microseconds
    Destination:                FF:FF:FF:FF:FF:FF   Broadcast
    Source:                     00:A0:F8:8B:20:1F
    BSSID:                      00:A0:F8:8B:20:1F
    Seq. Number:                559
    Frag. Number:               0
802.11 Management - Beacon
    Timestamp:                  10705409011   Microseconds
    Beacon Interval:            100
    Capability Info:            %0000000000010001
    SSID ID: 0 Len: 3 SSID: WP2
    Rates: ID: 1 Len: 4 Rate: 1 .0 Rate: 2 .0 Rate: 5 .5 Rate: 11 .0
    DSPS: ID: 3 Len: 1 Channel: 11
    TIM: ID: 5 Len: 4 DTIM Count: 6 DTIM Period: 10 Traffic Ind.: 0 Bitmap Offset:
    Symbol Proprietary ID: 173 Len: 9 OUI: 00 - A0 - F8 Number of clients: 1 Load (
FCS: (Calculated): 0x0020F8AE

0000: 80 00 00 00 FF FF FF FF FF FF 00 A0 F8 8B 20 1F   ....ÿÿÿÿÿÿ. ø.  .
0016: 00 A0 F8 8B 20 1F F0 22 F3 93 17 7E 02 00 00 00   . ø. .ð"ó..~....
0032: 64 00 11 00 00 03 57 50 32 01 04 82 04 0B 16 03   d.....WP2.......
0048: 01 0B 05 04 06 0A 00 00 AD 09 00 A0 F8 01 00 00   ........-□. ø...
0064: 00 13 00 00 00 00 00                              .......
```

Figure 12 Decode of a wireless packet

In an all-wireless environment, the only way to troubleshoot higher level protocols like IPX and TCP/IP protocols is to capture the packets off the air. In smaller satellite offices in particular, this all-wireless solution is increasingly common. It offers quick set up and can cover areas that would be awkward to serve with wiring, such as non-contiguous office spaces on the same floor. The only wired part of such networks may be the connection from the DSL modem, through the router to the access point.

The actual troubleshooting of these higher level protocols is no different on a wired or a wireless LAN, provided the network analysis software can read the packets fully. If WEP is enabled, the protocol analyzer must be able to act like any other node on the wireless network and decode the packet payloads using the shared keys.The ability to use WEP in the same way as all other nodes on the network must be built into the analyzer.

Roaming and wireless analysis

The 802.11 WLAN standards leave much of the detailed functioning of the DS to others. This was a conscious decision on the designers' part, as they wanted a standard entirely independent of any other existing network standards.

As a practical matter, an overwhelming majority of 802.11 WLANs using ESS topologies are connected to Ethernet LANs and make heavy use of TCP/IP. These users, at least, would probably have favored a bit more interconnection, even at the cost of some independence. The IEEE 802.11f working group is preparing a set of standards for communications between access points, to address this and related issues.

In the meantime, WLAN vendors have stepped into the gap, offering proprietary methods to facilitate roaming between nodes in an ESS. Third party software is also available to cache and proxy for roaming nodes at the TCP/IP layer. While no packet analyzer is likely to recognize all -- or perhaps any -- of these proprietary approaches out of the box, some packet analyzers can be taught to recognize and decode new packet types. Others can be taught how to capture and filter packets based on particular values or strings found at specific locations within packets. Either of these approaches would deliver the ability to diagnose and troubleshoot a wider variety of performance problems found in proprietary enhancements to roaming.

Conclusion

The demand for wireless networks is strong and increasing. The technology continues to evolve rapidly. Improvements in throughput, reliability, security, and system interoperability will only add to this demand. Both the security of the new WLANs and their performance depend on active, informed network management. Effective network management requires the right tools. WildPackets' AiroPeek, AiroPeek NX and RFGrabber are feature-rich, easy-to-use wireless tools designed expressly for 802.11 WLANs.

AiroPeek

AiroPeek™ is a comprehensive wireless network analyzer for IEEE 802.11 wireless LANs, designed to identify and solve wireless network anomalies. Features include:

- Full 802.11 WLAN protocol decodes
- Multi-NIC support
- Display of data rate, channel, and signal strength for each packet
- SSID tree of nodes
- Alarms, triggers, and notifications, all user-definable
- Security Audit template with pre-defined security audit filters

- Scan/surf by channel(s), ESSID or BSSID
- VoIP analysis tools

AiroPeek NX

AiroPeek NX™ brings the power of Expert Analysis to AiroPeek. This real-time expert analyzer has all the features of AiroPeek standard plus an advanced set of expert troubleshooting and diagnostic capabilities. The following features are unique to AiroPeek NX:

- Expert Analysis of over 100 aspects of network performance in real time, including VoIP expert diagnoses and 27 exclusively wireless problem events
- Designation of nodes as Trusted, Known, Unknown identifies rogue access points
- Description, Possible Causes, and Possible Remedies in the Expert ProblemFinder Settings window
- Peer Map of a continuously updated graphical view of traffic between pairs of network nodes, showing volume, protocol, node address, and node type

AiroPeek NX won eWeek Magazine Analyst's Choice Award in April 2002, Network Computing Editor's Choice Award in May 2002, and was selected as a Finalist for the Network Computing Well-Connected Award in April 2003.

AiroPeek and AiroPeek NX support a variety of 802.11a, 802.11b, and 802.11g wireless LAN adapters. Please see the support pages on our website at http://www.wildpackets.com/support for the most current listing of adapters and system requirements.

Enterprise customers who have standardized on WildPackets' network management solutions and training include Motorola, Lucent Technologies and Cisco Systems.

RFGrabber Probe

The RFGrabber Probe™ is a separately purchased hardware device that acts like a "listen-only" access point, allowing you to capture and monitor WLAN traffic in a remote location and stream the results to AiroPeek via TCP/IP over your wired network. You can connect to any network accessible RFGrabber Probe just as you would to any other network adapter. For more information on distributed wireless solutions, please see WildPackets' paper, "Remote Analysis of a Wireless LAN Environment."

For further information on these products, contact sales@wildpackets.com.

Wireless Terms

Access Point Provides connectivity between wireless and wired networks.

Ad Hoc Network Peer-to-Peer network of roaming units not connected to a wired network.

Base Station Access Point.

BSS Basic Service Set. Wireless network utilizing only one access point to connect to a wired network.

Cell The area within range of and serviced by a particular base station or access point.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

CSMA/CD Carrier Sense Multiple Access with Collision Detection.

CTS Clear To Send.

DHCP Dynamic Host Configuration Protocol, used to dynamically assign IP addresses to devices as they come online.

DS Distribution System. Multiple access points and the wired network connecting them.

DSSS Direct Sequence Spread Spectrum.

ESS Extended Service Set. A wireless network utilizing more than one access point.

Frame A packet of network data, framed by the header and end delimiter.

FHSS Frequency Hopping Spread Spectrum.

IBSS Independent Basic Service Set or Ad Hoc Network.

IEEE The Institute of Electrical and Electronics Engineers

Infrastructure Wireless network topology utilizing access points to connect to a wired network.

LLC Logical Link Control.

MAC Media Access Control.

NIC Network Interface Card.

OFDM Orthogonal Frequency Division Multiplexing.

Roaming Traveling from the range of one access point to another.

RF Radio Frequency

RTS Request To Send.

WEP Wired Equivalent Privacy.

WLAN Wireless Local Area Network.

WildPackets Professional Services

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

WildPackets Academy

WildPackets Academy provides 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 Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The (T.E.N.) Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

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

Live Online Quick Start Program

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

About WildPackets, Inc.

Since 1990, WildPackets has built affordable and easy to use network analysis tools. Our customers rely on WildPackets tools to help them design, maintain, troubleshoot, and optimize their networks. For information about our company, its products and partners, please see our website at www.wildpackets.com. See the WildPackets Academy site, www.wildpackets.com/services, for information on courses and Professional Services offerings. WildPackets' Network Analysis Expert (NAX) Certification Program details can be found at www.nax2000.com.

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
925-937-3200
www.wildpackets.com