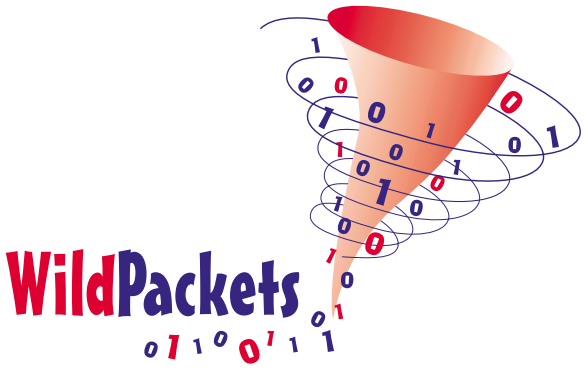
WildPackets' Guide to Wireless LAN Analysis



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. Developing countries, with more sophisticated network and internet access than ever before, have surged ahead in the utilization of wireless networks so that even the most remote parts of the globe have coverage undreamed of only a few years ago. Though deployment of wireless LANs in the United States has lagged behind the rest of the world, the domestic market is now quickly coming up to speed.

It is therefore of critical importance for the corporate network manager to understand not only how the wireless revolution is taking place, but how this technological paradigm shift will affect the day to day monitoring and management of network data.

This paper provides a brief overview of wireless networks and the 802.11b standard in particular, followed by a discussion of troubleshooting and network maintenance problems and the types of monitoring and analysis required to resolve them.

Introduction to wireless networking

The market for wireless communications has grown rapidly since the introduction of 802.11b wireless local area networking (WLAN) standards, which offer performance more nearly comparable to Ethernet. Business organizations value the simplicity and scalability of WLANs, and the relative ease of integrating wireless access and the ability to roam with their existing network resources such as servers, printers, and Internet connections. WLANs support user demand for seamless connectivity, flexibility and mobility.

As their price/performance and reliability continue to improve, WLANs are poised to become a common part of most business networks. In some cases, WLAN technology may make up the entire network. Cahners In-Stat Group predicts the Enterprise segment of the WLAN market will grow from $771 million in 1999 to nearly $2.2 billion in 2004 (Wireless LAN Market Analysis, January 2000).

The increasing need for wireless LAN analysis

While the obvious benefits of wireless LANs gain new converts, the network administration requirements for this relatively unfamiliar technology may not be as widely understood. Sometimes referred to as "wireless Ethernet," the IEEE 802.11 standards are in fact a completely distinct set of technologies with their own peculiar strengths and weaknesses. 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 more familiar wired network. In addition, WLANs are very often integrated with new or existing Ethernet networks. Naturally, diagnostic and troubleshooting requirements for TCP/IP, IPX and other higher level protocols and services do not stop at the end of the wire.

Wireless networking presents some unique challenges for the network administrator 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 802.11b standard

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 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 to explore alternate implementations of 802.11.

Working Group A explored the 5.0 GHz band, hoping 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, may keep their 802.11a standard from reaching wide distribution before 2002 or 2003 despite its promise of high performance.

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

The 802.11b WLAN protocol specifies the lowest layer of the OSI network model (physical) and a part of the next higher layer (data link). In addition, the protocol specifies the use of the 802.2 protocol for the logical link control (LLC) portion of the data link layer. In this same OSI conceptual 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.

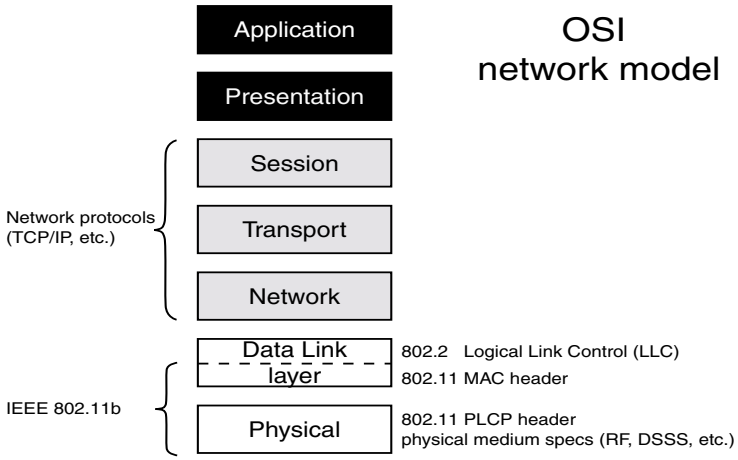


Figure 1 802.11 and the 0SI Model

Radio frequencies and channels

The most striking differences between WLANs and the more familiar 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, 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 signal power, distance and interference from intervening objects or other signals.

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 a pre-determined set of codes, such that each small modulation of the radio wave carries the greatest possible information. The term Direct Sequence Spread Spectrum in DSSS refers to one particular approach to packing more data into a given piece of RF spectrum -- more data in the channel.

The FCC in the United States and other bodies internationally control the use of RF spectrum and limit the output power of devices. The 802.11b WLAN standard attempts 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 802.11b WLAN transmissions to fairly short effective ranges, measured in hundreds of yards. In addition, the nature of radio waves and of spectrum spreading technology means that 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 signal. To overcome signal degradation problems, 802.11b 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 in 802.11b WLANs is 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps.

The 2.4 GHz band (2.40 GHz to 2.45 GHz) in US implementations is divided into 11 usable channels. To limit interference, any particular 802.11b WLAN network will use less than half of these in operation. All network hardware is built to be able to listen or transmit on any one of these channels, but both sender and receiver must be on the same channel in order to communicate directly.

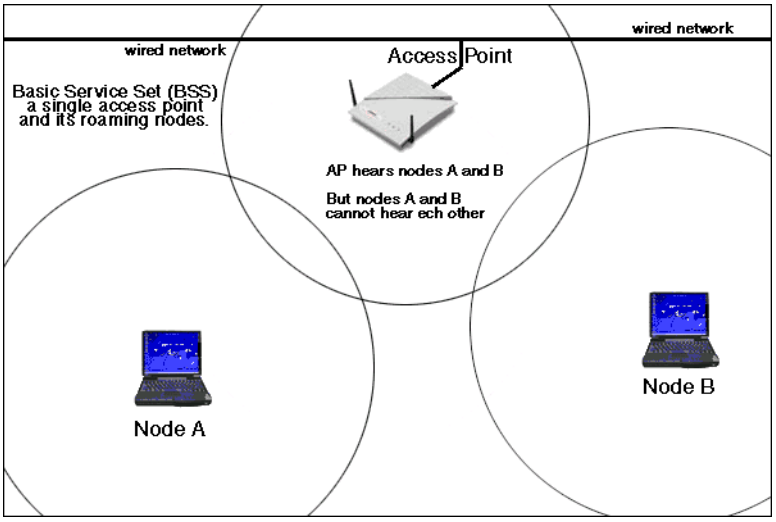


Figure 2 Basic Service Set (BSS), showing the hidden node problem.

Collision avoidance and media access

One of the most significant differences between Ethernet and 802.11b 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. 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.

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 where 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, 802.11b 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.

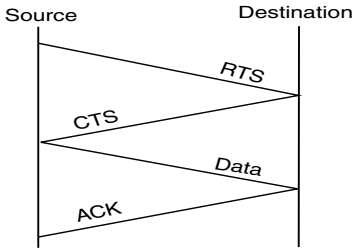


Figure 3 A Four-Way Handshake ensures collision avoidance in 802.11b networks.

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.

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.

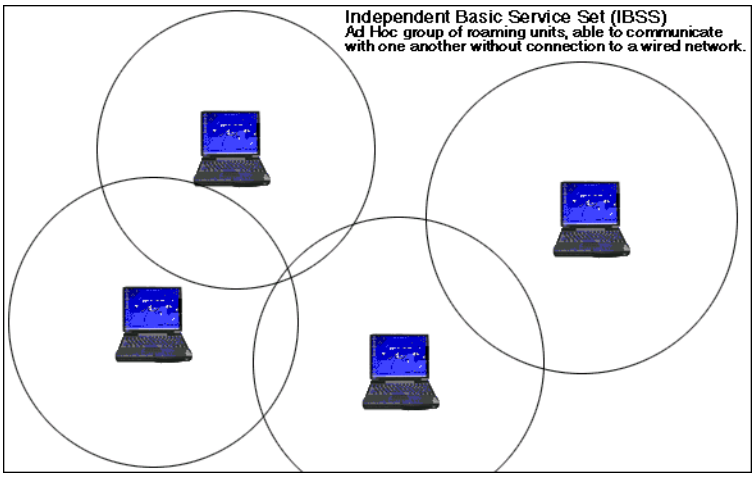


Figure 4 An IBSS or “Ad Hoc” Network.

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.

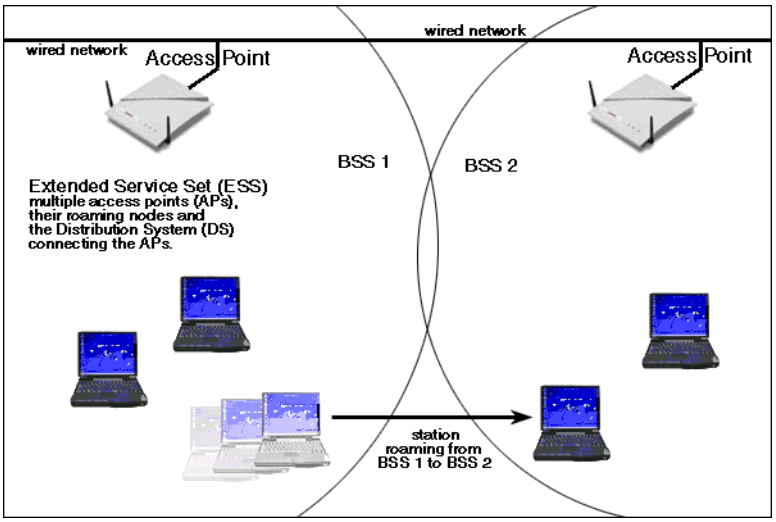


Figure 5 Extended Service Set (ESS) supports roaming from one cell to another.

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. In 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 distribution system or DS.

- **Note**: To meet the needs of mobile radio communications, the 802.11b WLAN standard must be tolerant of connections being dropped and reestablished. The standard attempts to ensure minimum disruption to data delivery, and provides 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 standard 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.

Authentication and privacy

Authentication restricts the ability to send and receive on the network. Privacy ensures that eavesdroppers cannot read network traffic.

Authentication can be open or based on knowledge of a shared key. In either case, authentication is the first step for a device attempting to connect to an 802.11b 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 key, then a device must prove it knows this shared key in order to be authenticated.

WEP (Wired Equivalent Privacy) is a data encryption technique supported as an option in the 802.11b WLAN protocol. The technique uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. The 802.11b WLAN network headers themselves are not encrypted.

The designers’ purpose in supporting this feature was to give a wireless network, with its inherent vulnerability to eavesdropping, a level of security similar to that enjoyed by a wired network operating without encryption. Eavesdropping on a wired network, they reasoned, requires a physical network tap or a suite of sophisticated radio listening devices. Eavesdropping on a radio network requires only a device capable of listening on the same channel or frequency. Since all 802.11b WLAN network adapters are capable of listening on any of the usable channels, eavesdropping is almost a certainty, given a large enough number of devices in circulation.

The original WEP specification called for 64 bit key length encryption (often referred to as "40-bit" with respect to the user-defined key). In part, this was an explicit effort to make commercial implementations of the protocol exportable from the U.S. in an era when only the very weakest encryption technologies were granted export licenses. The standard’s support for such a weak encryption method also underlines the design function of encryption in this protocol, however. It is intended to stop casual eavesdropping, not to stop a concerted attack. Several vendors now support 128-bit key lengths. This significantly increases the barriers to attack, but even at 128-bit key lengths, WEP is still

the door to an office, not a bank vault. Any of these levels of encryption serves the primary purpose of WEP quite well.

Because WEP encrypts all the data above the 802.11b WLAN layers, it can prevent network analysis tools from decoding higher level network protocols, and so prevent accurate troubleshooting of problems with TCP/IP, IPX, NetBEUI and so forth. To overcome this limitation, network analysis tools should allow users to specify the WEP shared key set for their network so they can decode the network data contained in 802.11b WLAN packets in the same way that every other station on the user's network does.

❖ **Note**: Although it is possible to implement WEP with open authentication, this is strongly discouraged as it leaves the door open for intruders to collect enough information to compromise the security of WEP.

Packet structure and packet types

Like the rest of the 802 family of LAN protocols, 802.11b 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 an 802.11b WLAN data packet and the information they provide for network analysis. The second section describes the management and control packets, their functions and the part 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 802.11b WLAN networks. This added complexity is reflected in the long physical layer convergence protocol (PLCP) headers as well as the data-rich MAC header.

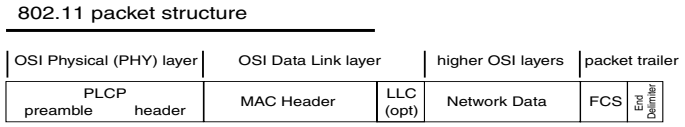


Figure 6 802.11b WLAN data packet structure

Because 802.11b 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.

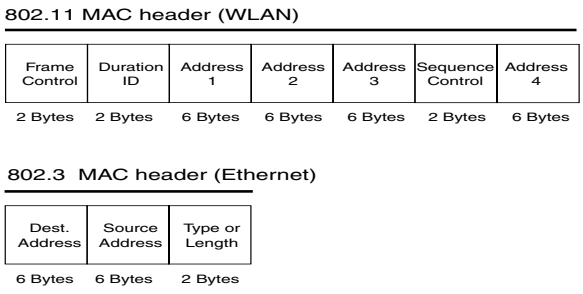


Figure 7 Comparison of MAC headers: 802.11b WLAN to 802.3 Ethernet

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. Instead, Table 1 below presents a list of the types of information 802.11b WLAN data packet headers convey. The table also shows the types of information carried in management and control packets.

Table 1 Protocol functions in 802.11b WLANs

Info Type	Usage
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.
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, but 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	These are 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 802.11b WLAN protocol supports rapid adjustment to changing conditions, always seeking the best throughput.
channel	the channel used for this transmission.
data rate	the data rate used to transmit this packet.

Table 1 Protocol functions in 802.11b WLANs (Continued)

Info Type	Usage
fragmentation	802.11b 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	These are control packets used in the four way handshake in support of collision avoidance.
version	The version of the 802.11 protocol used in constructing the packet.
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.

Table 1 Protocol functions in 802.11b WLANs (Continued)

Info Type	Usage
Routing	Again, many fields are related to routing traffic, but the following are most directly related:
addresses	There are four address fields in 802.11b 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 BSS ID. Which of the address fields shows what address 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 format is 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 1, along with the related information found in data packet headers.

Wireless packet 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 802.11b WLAN standard offers even more data to packet analysis than any of the other members of the 802 family of protocols. After a brief note about the kinds of information available to packet analysis, this section describes four broad areas in which protocol analyzers can be of particular use in network troubleshooting and administration.

A note on packet analysis and RF monitoring

Network administrators accustomed to Ethernet may be daunted at first by the unfamiliarity of RF technology. They may wonder if they need RF detection and monitoring devices more than their traditional network analysis tools. It is true that WLANs pose unique problems. It is also true that some understanding of, for example, RF signal propagation will be useful -- particularly in the initial deployment of larger ESS networks.

That being said, however, the need for specialized hardware to support an 802.11b WLAN is no greater than the need for similar equipment in support of the wiring plant of an Ethernet network, and perhaps even less. The reason for this lies in the specification of the protocol itself, and in the design of the network hardware. Nearly all of the parameters of physical network performance are available directly or indirectly in the packet headers and network management packets themselves. All that is required for most troubleshooting and maintenance tasks is a good network analysis program able to read, collect and display the data it finds on the network in a clear and meaningful way.

Configuration and traffic management

One of the advantages of 802.11b 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.

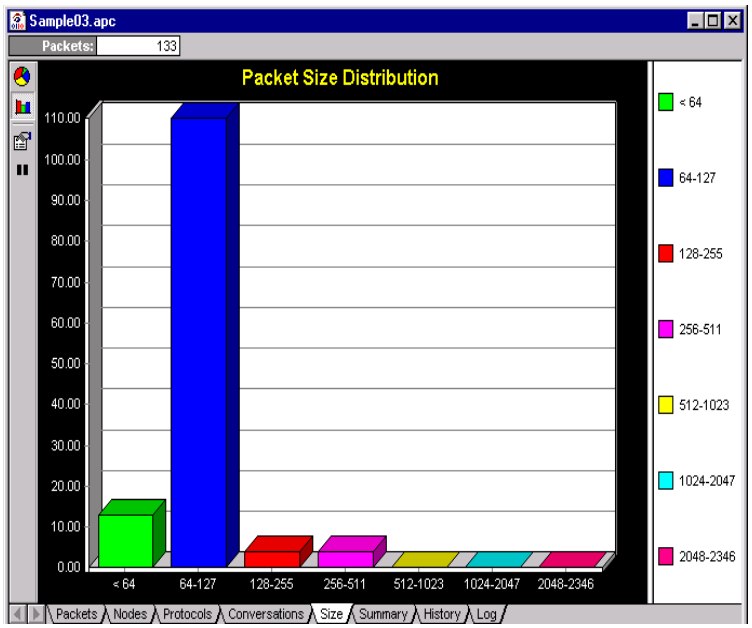


Figure 8 An unusual predominance of small packets may indicate interference

For example, where interference is high, 802.11b 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 802.11b 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.

802.11b 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.

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.

Identifying potential security problems

Security is a particular concern in wireless networks. Although 128-bit shared key encryption makes WEP secure against casual intrusion, it does not stop eavesdropping. Instead, it seeks to keep eavesdroppers from finding anything of use. The weak link in the security of WLANs is not the encryption scheme (particularly not at 128-bit levels) but user authentication. An authenticated user can gain all the information they need to compromise even 128-bit encryption. Given enough computing power, eavesdropping plus the information gathered as an authenticated user will allow any determined attacker to crack WEP.

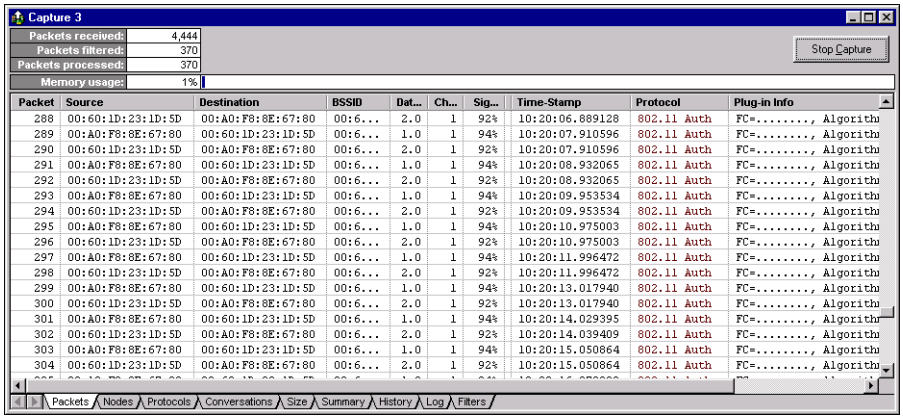


Figure 9 Focusing on authentication requests to guard against intrusion

Packet analyzers cannot detect eavesdroppers. They can detect failed authentication attempts, however. If a packet analyzer has a filtered or triggered start capture system, such an analyzer can be set to scan continuously for failed authentication attempts, capturing all the traffic exchanged in these attempts and making it possible to identify the potential attacker.

In a similar way, packet analyzers with sophisticated filtering can be set to watch for WEP encrypted traffic to or from any MAC address which is NOT a known user of the system.

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 much 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.

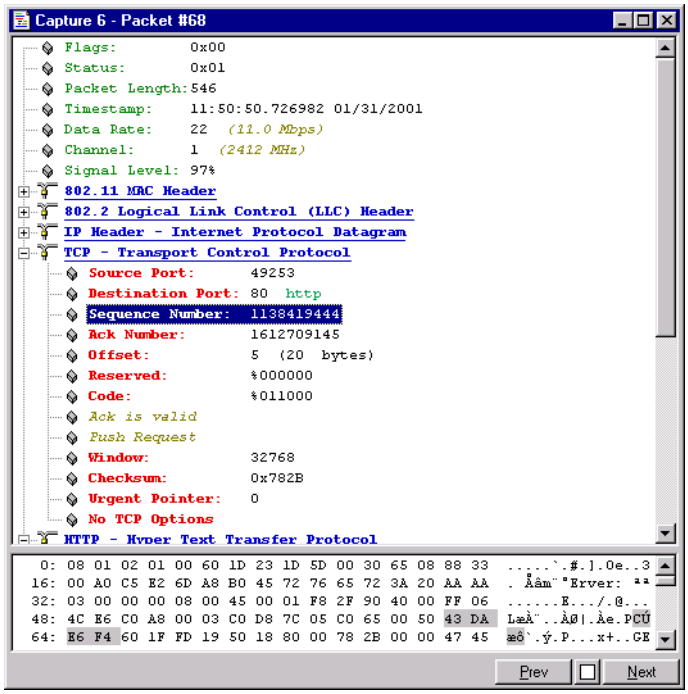


Figure 10 Troubleshooting an HTTP session requires the ability to read packet data

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.

Theoretically, of course, WEP is only an option and could be temporarily disabled. In practice, it is both unlikely and inadvisable that any WLAN should operate without WEP. Nor is it particularly simple to turn this function on and off at will. 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 802.11b WLAN standard leaves much of the detailed functioning of what it calls the DS (distribution system) to others. This was a conscious decision on the designers' part, as they were most concerned to make their standard entirely independent of any other existing network standards.

As a practical matter, an overwhelming majority of 802.11b 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.

WLAN vendors have stepped into the gap to offer proprietary methods of facilitating 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 in transitioning nodes from one BSS to another.

Conclusion

The competitive advantage of wireless networks is evident in the flexibility, mobility, and interoperability of WLANs standing alone or in conjunction with existing conventional networks. As corporate operations increasingly rely on wireless networks for effective and real-time communication, the ability to analyze and troubleshoot network problems in the wireless environment becomes critical to the management of network resources. WildPackets' AiroPeek Protocol Analyzer is specifically designed to meet the challenges of network management in the wireless environment.

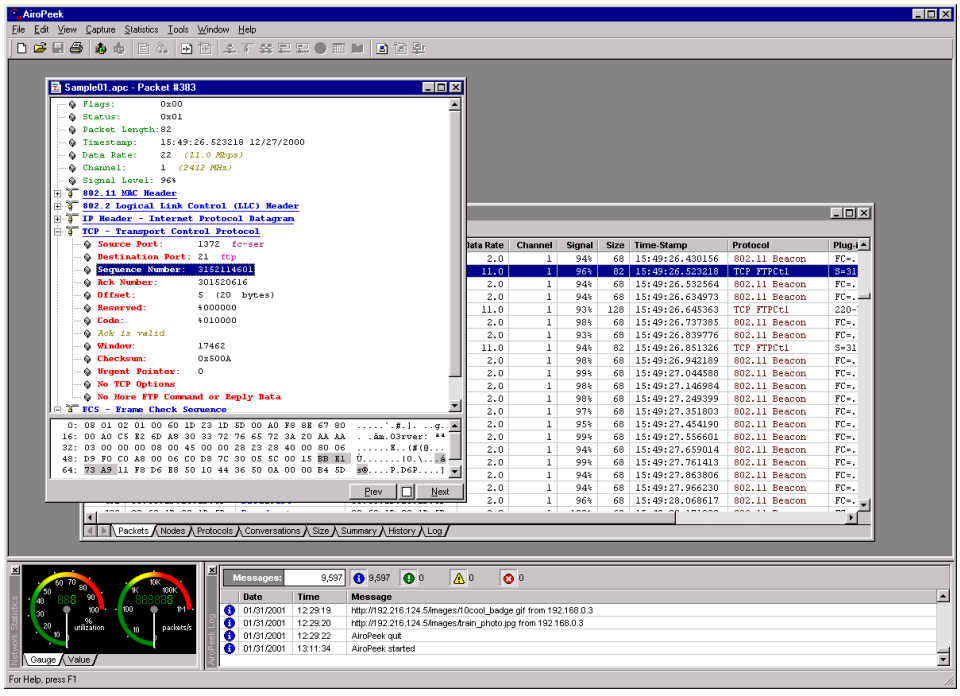


Figure 11 AiroPeek network analysis tools for 802.11b WLANs

AiroPeek protocol analyzer

AiroPeek is a comprehensive packet analyzer based on the IEEE 802.11b protocol standard for wireless communications, supporting all standard higher level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX. AiroPeek capabilities include:.

- Packet capture: direct, full, filtered, triggered, alarmed, or any combination.
- Shows data rate, channel, and signal strength for each packet.
- Full 802.11b WLAN protocol decodes.
- Support for WEP decryption (with user-supplied key sets).
- Continuous monitoring of network statistics in real-time.
- Channel selection by SSID and channel scanning
- Statistical analysis: for all traffic and for specific sets of captured packets.
- Filters, standard and user-defined, including use of logical AND, OR, and NOT.
- Name table, caches found names, substitute user-defined or card vendor names.
- Customized output of packet data, as lists or decodes.
- Alarms, triggers, and notifications, all user definable.
- Customized output of statistics (HTML, XML, text).

AiroPeek v1.1 currently supports Cisco, 3Com, Symbol, Nortel, and Intel wireless LAN adapters.

System Requirements: AiroPeek is a Windows-based tool that operates under Win 98/NT/2000/ME. AiroPeek v1.1 requires the installation of a custom NDIS driver.

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

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.

Roaming Traveling from the range of one access point to another, the ability to do so.

RF Radio Frequency

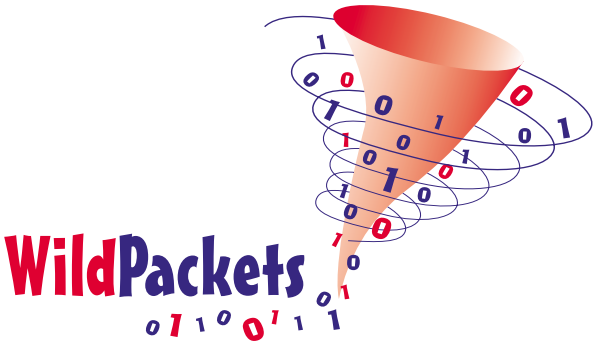
RTS Request To Send.

WEP Wired Equivalent Privacy.

WLAN Wireless Local Area Network.

About WildPackets, Inc.

WildPackets, Inc., formerly known as AG Group, is a network software and professional services organization that develops high performance tools to deliver real-time, strategic information about an organization's network and Internet presence, and provides network and packet analysis training, consulting and support services for IT Professionals at all levels.



WildPackets, Inc.
2540 Camino Diablo
Walnut Creek, CA 94596
(925) 937-7900
http://www.wildpackets.com