

Remote Analysis of a Wireless LAN Environment

Executive Summary

This white paper describes the background, challenges, and solutions to understanding, and effectively implementing, a distributed wireless LAN management system. This paper also presents guidelines for remotely managing, monitoring, and troubleshooting the WLAN environment.

March 2003



Contents

Perspective	1
Local WLAN Analysis Functions in a Remote Environment	1
RF Signal Analysis	1
Assessment of Protocol Behavior	3
Security Monitoring	3
Capacity Planning	3
Advantages of Remote WLAN Monitoring and Analysis	3
Types of Remote Analysis Devices	4
RMON Agents and Wireless Monitoring	4
Remote-Access Protocol Analysis	5
Vendor-Proprietary Probes	5
Determining the Placement of a Remote Device	6
Application of the RFGrabber Probe	7

Remote Analysis of a Wireless LAN Environment

With 802.11 wireless access becoming more widely deployed, it is increasingly important to be able to monitor, manage, and troubleshoot a geographically distributed WLAN environment from a central location. This paper presents the background, challenges, and solutions to successfully implementing a distributed wireless LAN management system.

Perspective

Unlike the classic wired Ethernet LAN environment, wireless analysis requires a focus on issues surrounding the physics of the transmission medium. Radio frequency (RF) engineering is an area of study that is often outside the core competency of the network support staff responsible for WLAN management. Consequently, it cannot be emphasized enough that appropriate training and study must be undertaken to become familiar with the concepts relating to RF signal transmission. It is only by understanding how a WLAN network operates that informed decisions can be made regarding the implementation of a system to monitor, manage, or troubleshoot the environment.

Local WLAN Analysis Functions in a Remote Environment

There are four key aspects to WLAN analysis and monitoring:

1. RF signal analysis
2. Assessment of protocol behavior
3. Security monitoring
4. Capacity planning

Understanding each aspect as it relates to stand-alone (local) analysis is the basis for understanding how to distribute the functionality to geographically remote locations. The key concept to keep in mind as you read through the discussion of these analysis aspects is that, in a distributed environment, the point of RF reception (by the analysis tool) doesn't move. That is, locally we could think about an engineer walking around with an analyzer, seeing packets as they are received when standing next to the client machine, or next to the access point, or somewhere in between. In a distributed environment, however, the analysis tool is installed in a fixed location and is accessed remotely. This will present some challenges to the remote analyst, since they won't have the capability of moving from location to location.

RF Signal Analysis

Assessing the RF signal strength in a wireless network is often thought of as being part of the site survey process. The aspects of RF analysis related to a site survey are not accessible to a remote engineer accessing an on-site, fixed-location tool. Only the RF environment seen by the fixed-location tool will be analyzed. There are two approaches to remote RF signal analysis.

Access Point Monitoring

In the first case, a single analysis tool is placed close to the remote access point. We'll call this "Access Point Monitoring." In this case, the analyzer sees an RF environment that is consistent with the environment seen by the access point. Client stations that are outside the range of the access point are outside the reception range of the analyzer. Using this approach allows the most accurate analysis of client problems related to the access point being monitored.

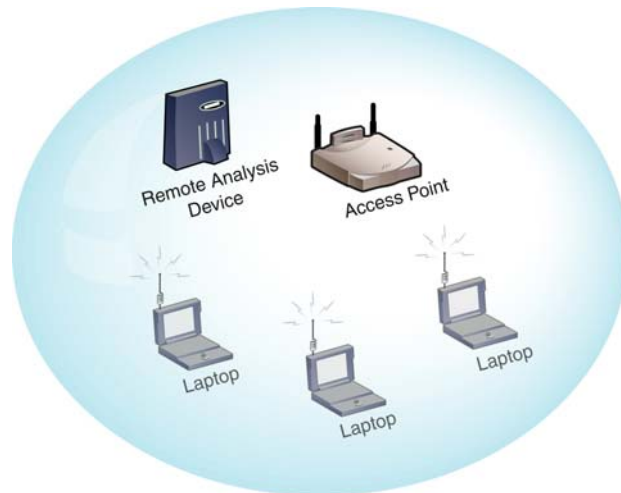


Figure 1 Access Point Monitoring

Environmental Monitoring

A second approach involves placing three analyzers in a triangle surrounding an access point and at a distance where the signal from the access point has fallen to roughly 50% signal strength. In this way, the client's RF environment is being monitored, as opposed to the environment being seen solely by the access point. We'll call this approach "Environmental Monitoring." Using this approach allows the most accurate analysis of RF and security issues.

Using Environmental Monitoring allows the remote engineer to see not only the immediate WLAN environment, but also lets him/her see stations that are outside the range of the access point, perhaps casually, or perhaps "war driving" (looking for available WLAN's to penetrate). In addition, Environmental Monitoring allows an analysis of client behavior as the client both enters and leaves the wireless service set. Access Point Monitoring can't see the station once it's moved outside the range of the access point; Environmental Monitoring can. In general, Environmental Monitoring is the more useful of the two methods, but it does require a larger investment in analysis equipment.

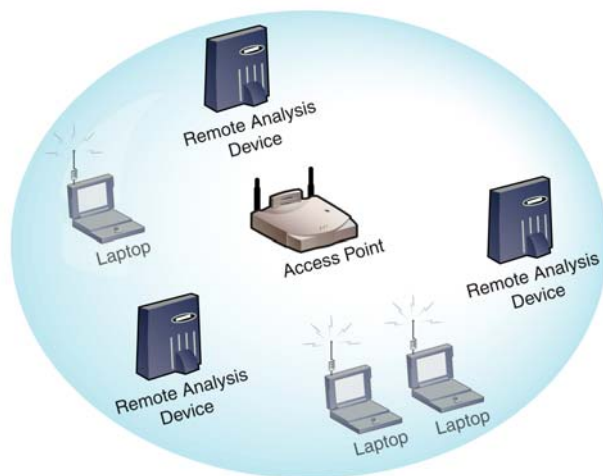


Figure 2 Environmental Monitoring

Assessment of Protocol Behavior

Whether the network being examined is based on TCP/IP, AppleTalk, Novell NetWare, or some other protocol environment, there are specific behaviors that are expected from the upper layer protocols. The operation of DHCP, DNS, WINS, NBP, NDS, and the file transfer behavior of SMB, AFP, or NCP remains the same on the wired and wireless network segments, as do the behaviors of all of the classic wired protocols.

In the wireless environment, there are two possible scenarios to consider relative to analysis of classic, wired protocol behavior as it manifests itself in the wireless infrastructure. The WLAN may or may not be using an encryption mechanism. If no encryption is being used in the classic corporate environment, then the first troubleshooting problem has been solved already. That is, encryption should be used! Encryption may be as simple as 802.11 WEP or as sophisticated as Cisco's LEAP, standard 802.1x EAP, or other authentication/encryption schemes. If WEP is in use, one must simply provide the WEP key to the analysis tool and perform analysis on the unencrypted packets. With mechanisms (such as LEAP) where the key changes or where analyzer decryption is otherwise not possible, you won't be able to perform upper layer protocol analysis on the traffic.

Not being able to analyze upper layer traffic on the WLAN is not significant with respect to the 802.11-specific aspects of monitoring, analysis, and troubleshooting. All of the 802.11 behavior remains unencrypted and the client association, disassociation, and reassociation mechanisms are fully visible. Moreover, the establishment of LEAP/EAP authentication is transmitted using unencrypted packets. It can be determined whether or not a client is having a problem accessing the WLAN, and whether or not the client is properly authorized to perform such access attempts.

Security Monitoring

The wireless NIC card addressed in a WLAN are always visible in an analyzer trace file. Consequently, the presence of an unauthorized device, based on its MAC address, can always be determined. Moreover, the utilization of the WLAN network is reported on an address-by-address basis, so it can be determined who the most active communicators are, even if their traffic is encrypted. Since access points always transmit beacon packets, the presence of a rogue (unauthorized) access point can also be determined.

Capacity Planning

As the number of devices present in a WLAN increases, the potential for performance degradation increases. Access points provide a single point of access to the wired Ethernet, so all of the stations in the WLAN must compete for bandwidth between the access point and the rest of the wired network. As more and more stations participate in the WLAN, the contention between them becomes visible as an increase in CRC errors and a reduction in the speed used by each station (11, 5, 2, or 1 Mbit/sec). Monitoring the wireless environment gives the network manager an opportunity to detect growth in usage before it impacts the end-user community.

Advantages of Remote WLAN Monitoring and Analysis

Monitoring and analyzing remote WLAN sites provides the same basic set of capabilities that are available with local analysis, but without having to physically go to the remote site. Whether it's on another floor of the building or across the country, having a remote analysis device standing ready to capture a problem situation or to simply monitor statistical trends at a remote site saves time and money.

Much of the traffic that originates on the wireless LAN, and (in some cases) all of the traffic going to the clients on the wireless LAN crosses the wired Ethernet. Simply capturing the Ethernet traffic (from, for example, a mirrored Ethernet switch port) doesn't provide a true picture of the behavior taking place on the wireless portion of the network. It's not sufficient to simply evaluate wireless clients on the basis of their presence on the wired Ethernet.

For example, consider a situation in which multi-path reflections were causing packet loss that affected only those clients located in the north-east corner of a building, and only on the fourth floor. Using the client utility that came with the 802.11 NIC would show a relatively noise-free environment (since, in the absence of packet transmission, there was nothing going on in the RF spectrum). Moreover, the client utility would show that received packets (those that were received successfully) had reasonably high signal strength. The 802.11 NIC's client utility is not intended to serve as an analyzer but rather, as a way to ascertain proper operation of the installed NIC. In this case, the NIC is working properly and it's able to send and receive packets in a suitable environment.

The problem would not be evident on the wired side either. The result of the problem might show up as long interpacket delays, but the actual packet-level behavior would not manifest itself on the wired Ethernet. Consider a situation in which the client had just received some TCP data and was now trying to send a TCP ACK. Because of WLAN issues like multi-path reflections, hidden node problems, RF denial of service attacks, or congestion, the ACK packet is not received by the access point. The client's 802.11 stack retries the transmission multiple times (setting the Retry bit in each subsequent packet) until the access point sends its 802.11 Ack back to the client.

None of these behaviors are visible with an 802.11 client utility, nor are they visible on the wired Ethernet. You need to be monitoring and analyzing the wireless network itself.

Of course, Murphy's Law says that by the time you ride the elevator up to the fourth floor the problem has gone away, so using your portable protocol analyzer is of no use in isolating and describing an intermittent anomaly. In the RF environment, the presence of momentary problems is much more prevalent than in the wired Ethernet. When you're in your car, for example, a distant radio station may be received with your favorite song loud and clear, only to fade into static a short distance down the road, and then spring back to full volume a moment later. The RF environment is impacted by a number of factors that can be explained to us by the physicists, but our challenge is to quickly isolate and describe their impact on the WLAN clients. This is why you need remote WLAN analysis capabilities in a geographically distributed network.

Types of Remote Analysis Devices

There are, fundamentally, three types of remote WLAN analysis designs that could be considered:

1. RMON-enabled probes
2. Remote-access protocol analyzers
3. Vendor-proprietary probes

RMON Agents and Wireless Monitoring

The Remote Monitoring (RMON) data structure is defined by the Internet RFC's for both Ethernet and the now generally obsolete Token-Ring network architectures. There is no RMON standard for 802.11 wireless networking. Consequently, although it is technically feasible to imagine the creation of a wireless RMON agent, no such device currently exists. Moreover, any use of Ethernet RMON standards to implement a wireless monitoring agent

would, by virtue of the absence of a legitimate wireless RMON standard, be a vendor-proprietary product.

Remote-Access Protocol Analysis

There are several vendors in the marketplace that offer a wireless protocol analyzer. WildPackets' AiroPeek NX is an example of a full-featured wireless analyzer. Unlike an RMON device (using Ethernet RMON as a point of reference), a protocol analyzer will provide not only statistics, but will allow analysis of packet-level communication as well. Expert system technology can automatically detect various problems in the 802.11 environment. Because a full-featured protocol analyzer is designed to utilize the capabilities of a high-speed, Pentium-based computer with a large memory space, it's possible to troubleshoot conversations that are extracted from the network traffic and (in the case of AiroPeek NX) perform expert system analysis at the same time that full packet decodes are studied.

When considering deploying a protocol analyzer as a remote analysis device, it's important to select a tool that allows the connection of an external antenna. This is because it's unlikely that a notebook computer (running the analyzer software) can be mounted on the ceiling next to an access point! You'll need to extend the analyzer's antenna to fix it in position near the access point (for Access Point Monitoring) or to multiple locations (for Environmental Monitoring). Moreover, the analyzer will have to have the capability of acquiring data from multiple sources simultaneously (or else you're going to need a lot of notebook computers!).

Having installed your analyzer and its antennae, you'll now simply access the notebook computer remotely using either an off-the-shelf solution (Windows Terminal Services, Timbuktu, PCAnywhere, etc.) or a vendor-proprietary solution. In some cases, vendors offer customized hardware in place of a simple notebook computer. A decision must be made as to whether you'll use the analyzer vendor as your hardware source, or whether you'll depend on your normal PC-hardware supplier for repairs.

The disadvantage of using a standard analysis tool as a remote WLAN analysis device is, fundamentally, the potential cost of deploying multiple computers to multiple locations. Of course, reasonable placement of a notebook or other stand-alone analyzer is often compromised by the need to use an external antenna for proper coverage. Moreover, when comparing trace files or statistics reports taken from multiple locations, the time stamps will always vary from one analyzer to the next, even if the tools are synchronized with systems like Network Time Protocol. This is because a time synchronization protocol is impacted by propagation delays to the various devices it's trying to coordinate, coupled by the fact that the software clocks in PC platforms are not designed to provide absolute accuracy or consistency.

Vendor-Proprietary Probes

In the marketplace, there are external probe devices that can be placed in remote locations (in much the same way as placing an access point) and connected back to a centrally placed wireless protocol analyzer using standard cabling. WildPackets' RFGrabber is an example of this type of probe. The probe uses Ethernet and UDP to carry data from a remote location (the various floors of a building, for example) back to the central protocol analyzer (AiroPeek NX). The probes can be placed for either Access Point Monitoring or Environmental Monitoring, and are each separately wired back to the central analyzer. Because the probes are separately addressed as IP devices, the wiring infrastructure used to bring probe data back to the analyzer can utilize standard hubs or switches exactly like the user's Ethernet. The analyzer itself can send SNMP traps to an umbrella management system when problems are detected.

This approach requires a separate wiring system to connect the probes to the analyzer. This can be overcome by connecting the probes directly to the user's Ethernet. However, there are two fundamental considerations in this situation. First, since data in the WLAN often originates on the user's Ethernet, the probe will increase the load on that Ethernet as it sends the WLAN data back to the analyzer. Over a 100% increase in Ethernet load could, in theory, be observed. The reason for this is that two types of traffic may be sent back from the probe to the analyzer. First, in a situation where all wireless users were employing services on the Ethernet, each Ethernet packet transmitted onto the WLAN would be encapsulated in UDP by the probe and sent back across the user's Ethernet to the analyzer. In addition, the 802.11 MAC traffic would also be sent back to the analyzer. This traffic load can be minimized by the use of probe filtering. It is, therefore, necessary that any wireless probe be capable of selectively sending traffic back to the analyzer.

WildPackets' RFGrabber does include on-probe filtering. These filtering capabilities ensure that the traffic that is gathered is the traffic that is necessary for efficient identification and remedy of wireless network problems. For example, when monitoring an access point, you can capture only the data traffic. RFGrabber contains filters for management, control, and data traffic.

A second issue that arises when the probe is attached to the user's Ethernet is the fact that the IP address of the probe must be consistent with the subnet (perhaps through DHCP assignment) and that address must somehow be known to the analyzer (so that the probe can be contacted). This is a network management issue and demands careful use of manually assigned IP addresses (for the probes) and appropriate administrative systems to get these addresses configured into the analyzer. To make this process easier, the RFGrabber Analysis Module supports a scanning feature that automatically identifies RFGrabber Probes that are distributed on the same subnet. Once identified, the probes can be easily configured through the RFGrabber Analysis Module.

In conclusion, probes are an ideal way to implement monitoring and analysis to locations within a building or at other remote sites. They should be wired back directly to the analyzer and only if direct connection is not feasible should they be attached to the user's Ethernet.

Determining the Placement of a Remote Device

When we consider the placement of a remote "device" we're actually talking about the placement of the receiver antenna on the monitoring device. In the case of a notebook computer or other device with an internal (or PCMCIA-type) 802.11 card, this is the device itself. When using probes or remote antennae, the location of the analyzer itself is not important; only the location of the probe antenna is of concern.

If Access Point Monitoring is to be used, there is no need to perform a site survey to determine antenna placement. Simply put a monitoring antenna near each access point. The monitoring antenna should be at least 5-feet (1.5 Meters) from the access point to avoid overpowering the monitoring probe.

If Environmental Monitoring is to be used, then it will be necessary to determine the transmission range of a typical access point. To accomplish this, it will first be necessary to determine a value that we can call "wall penetration" for the WLAN being monitored. This is done using a portable analyzer on-site prior to the full-scale deployment of the final system. Quite simply, it's a matter of walking around and determining how many walls can be penetrated by the signal (the beacon packets) coming from an access point. What's being assessed here (indirectly) is the type of wall construction used in the building. Perhaps this is a relatively new office building with drywall on aluminum studs. In an old building in the heart of a city, you may find plaster on lath. Some buildings may use cinderblock construction. It could be the case that you're surveying an open area with no walls. In that

case, you're simply measuring the distance from the access point at which the signal level falls off.

The goal of surveying a site is to determine the wall penetration value and distance at which the signal strength falls to roughly 20% (-90dBm). This will determine the radius of a circle that you're going to use to draw a coverage map of your site.

Consider this process for a corporate campus with 15, 4-story buildings. This could be an office park, hospital, or other site where the buildings were constructed at the same time. In all probability the wall (and floor) construction is the same for all the buildings. In this case, it's only necessary to survey one floor of one building to obtain the radius for 20% signal strength.

Place three remote monitoring probes 120-degrees apart (in a triangular configuration) with the access point at the center as shown in the following diagram.

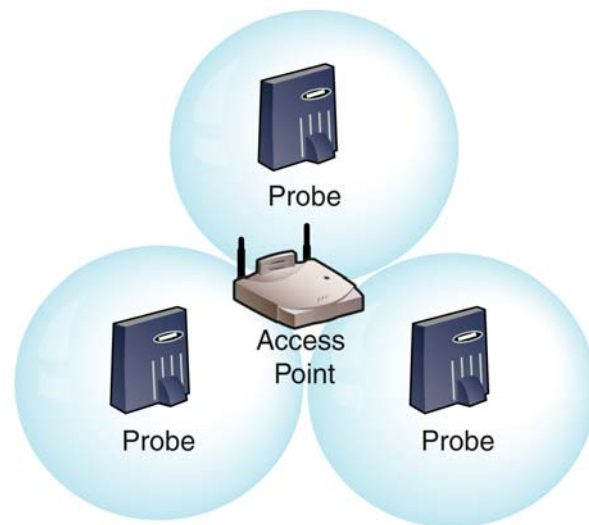


Figure 3 Access Point Range

You can see (above) that there may be some areas that are not monitored but are, nonetheless, in range of the access point. For more complete coverage, four, or even five probes could be used.

Application of the RFGrabber Probe

The WildPackets RFGrabber remote monitoring and analysis probe is ideally suited to become part of a geographically distributed wireless LAN management system. A single AiroPeek NX analyzer can support multiple RFGrabber probes at the same time. The RFGrabber probes are connected to AiroPeek NX using standard Ethernet cable and infrastructure equipment.

Consider the design of an RFGrabber/AiroPeek NX implementation to monitor and analyze the 802.11 LAN environment in a six-story building. There are four access points on each floor and we've decided to use Access Point Monitoring. An RFGrabber probe is installed near each access point.

On each floor, the four RFGrabber probes are Ethernet-cabled back to a dedicated hub in the wiring closet. This hub will be part of the monitoring Ethernet and is not connected to the

user's Ethernet. These hubs, on each floor, are all wired separately to the computer room on the first floor. The hubs, of course, can't simply be "daisy-chained" one to another since this would violate the repeater rules for 802.3 Ethernet. In the computer room, the six hubs come together into a single core hub. The Ethernet NIC in AiroPeek NX that's intended for RFGripper attachment is then plugged into the core hub.

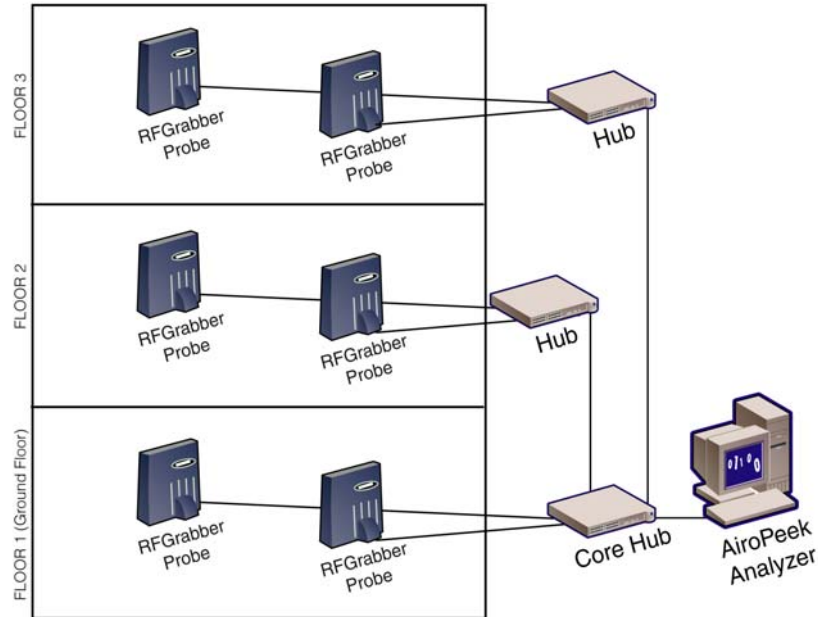


Figure 4 Building Wired with RFGripper Probes

To differentiate between standard client services (web, email, etc.) that would use the AiroPeek NX's host computer's standard TCP/IP client NIC (a separate Ethernet NIC) and the NIC that will communicate with the RFGripper probes, it's simply a matter of configuring the RFGripper probes onto a private, non-routed subnet (like network 10.0.0.0). The AiroPeek NX host will know that packets for network 10.0.0.0 go to one Ethernet NIC while other packets go to the standard Windows client NIC.

Now, from within AiroPeek NX, you can specify multiple RFGripper probes that are to be monitored or used for packet capture. In this way, network managers are able to monitor, manage, and troubleshoot a geographically distributed WLAN environment from a central location.

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/services. 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.

WildPackets, a privately-held corporation, was founded in 1990 with a mission to create software-based tools to simplify the complex tasks associated with maintaining, troubleshooting, and optimizing evolving computer networks. WildPackets' patented, core "Peek" technology is the development base for EtherPeek™, TokenPeek™, AiroPeek™, and the NX™ family of expert packet analyzers. All are recognized as the analysis tools of choice for small, medium, and large enterprise customers, allowing IT Professionals to easily maximize network productivity. Information on WildPackets, WildPackets Academy, Professional Services, products, and partners is available at www.wildpackets.com.

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

