



Getting the Most from Your Wireless Network

WHITE PAPER

Network disruptions are no longer minor inconveniences; they have become business disruptions with financial and sometimes even legal consequences. Network engineers need to quickly visualize global network performance and analyze root cause failures as quickly as possible to keep wireless networks and wireless VoIP on mobile devices running smoothly. This white paper outlines best practices in monitoring, analyzing, and troubleshooting wireless networks using the WildPackets® OmniPeek™ Wireless Solutions.

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.wildpackets.com

Getting the Most from Your Wireless Network

Introduction.....	3
Planning and Designing a WLAN.....	3
Develop Your Baseline.....	3
Test Your Initial Layout.....	4
Managing a WLAN.....	5
Managing Signals.....	5
Managing Users.....	5
Administering a WLAN.....	6
Securing the WLAN.....	6
Troubleshooting a WLAN: Analyzing Higher-Level Network Protocols.....	8
Leveraging Existing Assets with AP Capture Adapters.....	10
Multi-Channel Analysis.....	10
Roaming Latency Analysis.....	10
Conclusion.....	11
Wireless Abbreviations and Terms.....	12
WildPackets Distributed Analysis Solutions.....	13
Learning More.....	13
About WildPackets, Inc.	13

Getting the Most from Your Wireless Network

Introduction

Wireless networks require the same kinds of analytical and diagnostic tools as any other LAN to maintain, optimize, and secure network functions with one notable exception. In a LAN environment, all signals are conducted over a fixed, well-defined and “electrically stable” network of cables. This is in stark contrast to wireless networks, where signals are transmitted using Radio Frequency (RF) technology. Radio frequency waves propagate outwardly in all directions from their source, and are very sensitive to disruption and interference. The quality of the transmitted signal varies over time and space—even if the source and destination remain fixed. The path between the source and destination also has a very significant impact on the quality of the resulting communication. Open propagation of data means that anyone can receive the data, even those not “connected” to the network, making security a far bigger issue for WLANs. The use of unlicensed spectrum by 802.11 also increases its vulnerability to interference, as it must share its available bandwidth with non-802.11 devices, including Bluetooth, cordless telephones, and microwave ovens.

Fortunately, the 802.11 WLAN standard offers more data for monitoring and analysis than any of the other members of the 802 family of protocols. WildPackets® provides a wide range of products that take advantage of this, enabling the creation of highly flexible, cost-effective wireless network analysis solutions. Also, new technologies are being developed to simplify the identification and mitigation of interference sources by analyzing the 802.11 physical layer—the actual RF environment that is the transmission network. This white paper describes four broad areas in which the WildPackets wireless network analysis solutions can be of particular use: network planning, management, administration, and troubleshooting.

Planning and Designing a WLAN

One of the advantages of 802.11 WLANs is their ability to dynamically adjust to changing conditions and to configure themselves to make the best use of available bandwidth. These capabilities work best, however, when the problems they address are kept within limits. To do this, you must understand the limits of the RF environment in the areas where wireless is to be deployed. This is best accomplished by assessing the area to get a quantifiable baseline of your environment.

Develop Your Baseline

When developing your baseline, it is imperative to assess two specific areas: 1) interference sources from non-802.11 devices and 2) signals from existing 802.11 equipment.

Interference sources are often ignored when planning a WLAN deployment, yet this information is critical in designing wireless access point (AP) placement, spacing, and channel selection. For example, where interference is high, 802.11 WLAN nodes will continue to increase fragmentation, simplify spectrum spreading techniques, and decrease transmission rates in an attempt to best use the available bandwidth. In addition, physical layer interference increases retransmissions, especially when they occur despite high fragmentation. While some network applications may show no ill effects from a given source of interference, 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.

Getting the Most from Your Wireless Network

Using OmniPeek, you can quickly determine the state of your network. Possible sources of interference can be examined, their effect on network performance assessed, and proper Access Point (AP) placement, power and channel allocation can be determined. This will result in a WLAN that consistently delivers the throughput that you and your users expect.

Test Your Initial Layout

Once the environment is understood and an initial layout is determined, it's time to test it out. OmniPeek can be used to both verify the pre-deployment baseline measurements, and to measure the actual performance of your WLAN design.

OmniPeek is used to assess overall throughput and signal strength at key locations in your network, and to troubleshoot both the wireless *and* wired side of your network, simultaneously, should problems be identified. The ability to troubleshoot both the wired and wireless side of the network simultaneously is critical, and this is illustrated in Figure 1. The wireless side of the network is shown on the left, the wired side on the right. Using the dual capture and compare features of OmniPeek, ongoing problems with packet retransmission on the wireless side of the network are clearly demonstrated.

OmniPeek can also be used to test the interaction of clients and APs in multi-AP deployments. 802.11 WLAN Basic Service Sets (BSS) and Extended Service Sets (ESS) have the ability to dynamically configure themselves, associating and reassociating roaming nodes, first with one AP and then with another. The physical location and RF channel used by each AP should be optimized.

These choices can either lead to smooth network functioning or to unexpected problems.

To help evaluate your overall network topology and its performance, OmniPeek can capture data from multiple APs on multiple channels simultaneously, giving you a complete picture of overall network behavior. Roaming, or the reassignment of clients from one AP to another AP, typically on a different channel, can be easily identified and the latency caused by the transfer can be accurately measured using multi-channel analysis.

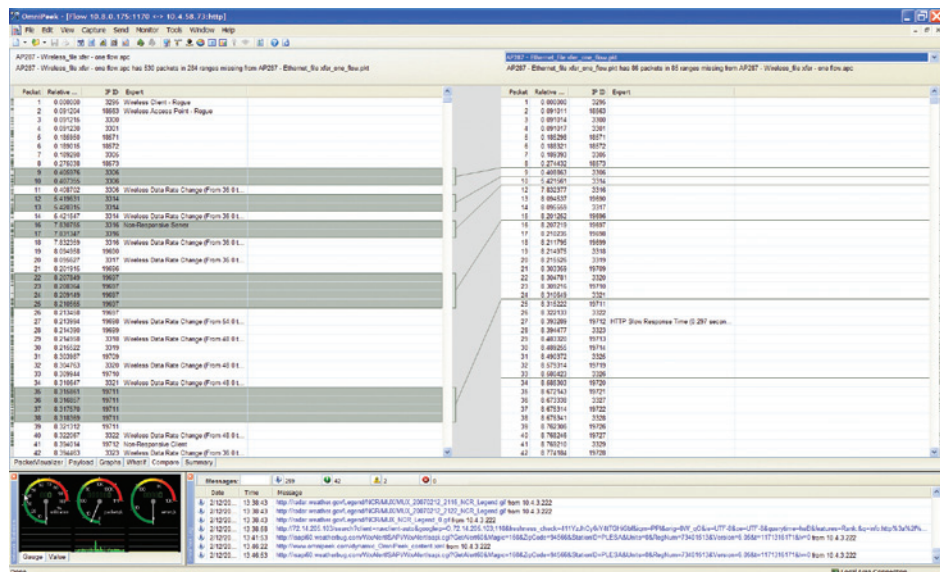


Figure 1. The dual capture and compare feature allows simultaneous wired and wireless analysis.

Getting the Most from Your Wireless Network

Performing a site survey with OmniPeek 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 APs, or perhaps moving one or more to a new location. The effects of each change can quickly be monitored with OmniPeek.

Managing a WLAN

Managing Signals

Management of your WLAN begins with simple “dashboard” views that you can use to quickly assess the overall health of your network. OmniPeek provides 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 as shown in Figure 2.

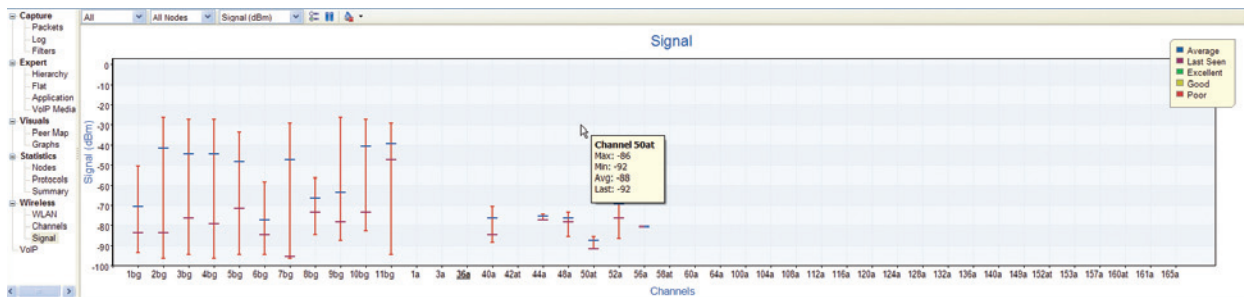


Figure 2. Detailed graphical display of reported signal strength for each WLAN channel.

Managing Users

Wireless networks are made up of one or more radio cells, centered on 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 Distribution System (DS)) at the top, then individual BSSs (individual APs and their clients), then the individual client nodes or stations (STAs).

In OmniPeek, the 802.11 view of Node Statistics displays the wireless devices on your network in just such a hierarchical tree, as shown in Figure 3. Individual devices are identified by their ESSID, BSSID, or MAC address as appropriate. An ESSID identifies a group of APs. This is the identifier sent out as “SSID” from the AP. The BSSID is the specific identifier of the AP, naming its MAC address. 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. Trust values can also be assigned to each node, allowing you to quickly distinguish friend from potential foe.

Getting the Most from Your Wireless Network

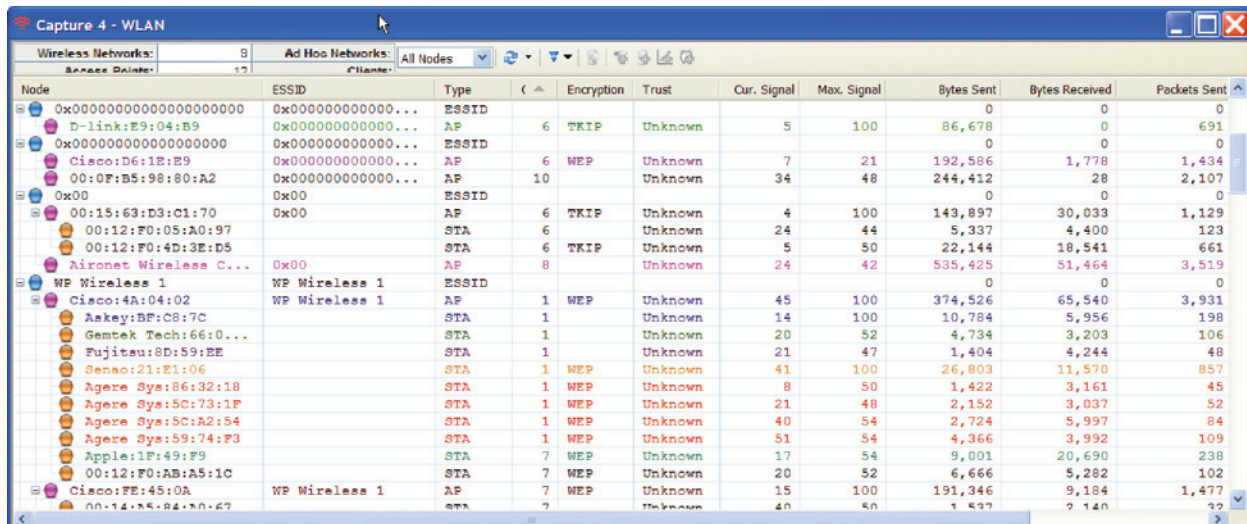


Figure 3. Hierarchical tree view of a WLAN

In addition to a hierarchical view of network users, OmniPeek can also be used to represent the network as it is physically deployed. By importing a floor plan into the OmniPeek Peer Map view and dragging APs to their physical location, the Peer Map can be used to give you a more intuitive view of the WLAN layout. This is illustrated in Figure 4.

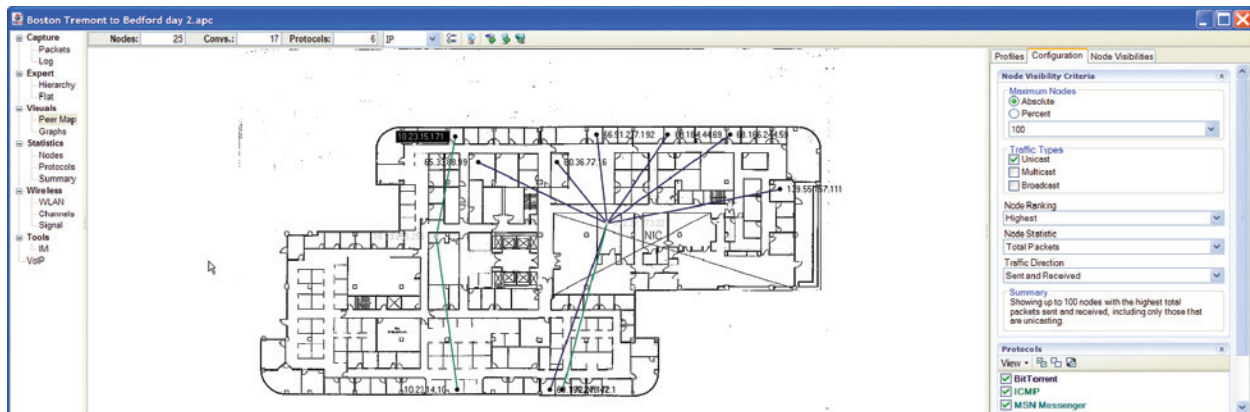


Figure 4. A physical representation of the OmniPeek Peer Map.

Administering a WLAN

Securing the WLAN

Because WLANs use radio transmissions, they are inherently more difficult to secure than wired LANs. Simple encryption and authentication techniques such as WEP prevent outsiders from casually or inadvertently browsing your WLAN traffic, but they cannot stop a deliberate attack. WPA, and particularly WPA2 is quite secure today, and meets the need of the most demanding security officer. Even the best passive defenses, however, must be paired with an active defense in order to really work.

Getting the Most from Your Wireless Network

1) Attempted breaches must be identified and stopped.

2) Networks must be monitored to ensure that security policies are followed.

OmniPeek can be used to monitor compliance with security policies, and to identify, intercept, log, and analyze unauthorized attempts to access the network. It can automatically respond to security threats in a variety of ways, making it ideal both for monitoring and for more focused analysis.

Expert, real-time analysis of all traffic on the network identifies anomalies and sub-optimal performance. OmniPeek provides 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
- Adherence with common wireless network policies

Figure 5 shows an example of the Expert ProblemFinder Settings.

With OmniPeek, 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 APs, as shown in Figure 5. 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 AP in a neighboring office. Nodes classified as *Unknown* (the default) can be quickly identified.

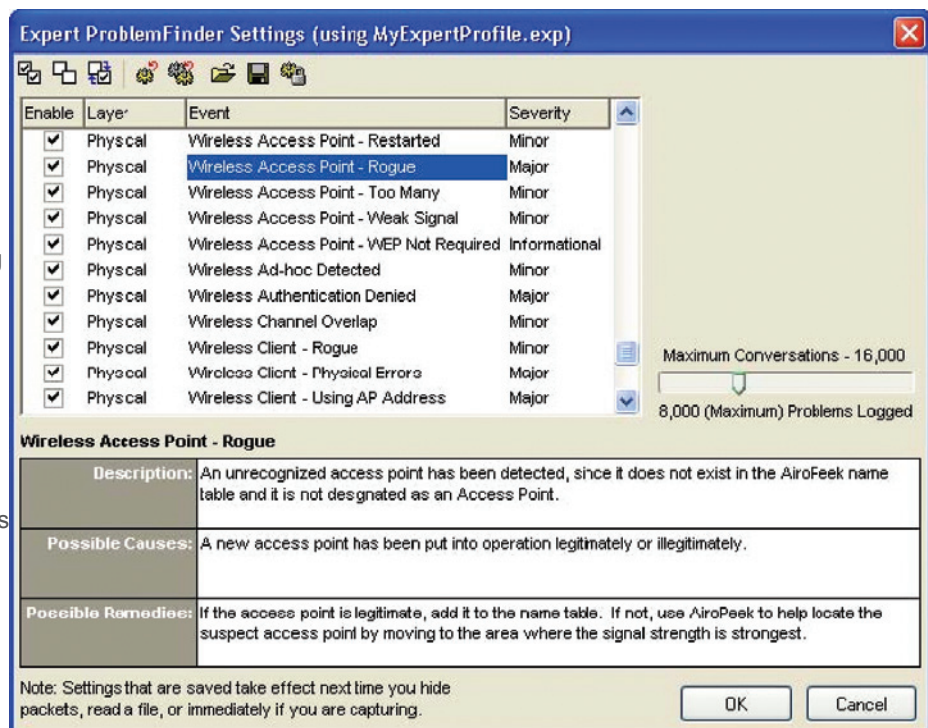


Figure 5. Wireless Expert Events in OmniPeek.

Getting the Most from Your Wireless Network

OmniPeek also includes a security audit template, which you can use as is or modify to meet particular requirements. The template makes use of special filters, alarms, and pre-configured capture sessions to create a 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 traffic that meets its criteria and sends a notification, keeping you informed of suspicious activity on your wireless LAN.

Event	Severity	Ena...	
VoIP		<input type="checkbox"/>	
Wireless		<input checked="" type="checkbox"/>	
Network Policy		<input checked="" type="checkbox"/>	
Network Policy Violation - Vendor ID	Minor	<input checked="" type="checkbox"/>	
Network Policy Violation - Channel	Minor	<input checked="" type="checkbox"/>	
Network Policy Violation - ESSID	Severe	<input checked="" type="checkbox"/>	
Network Policy Violation - WLAN Encryption	Minor	<input checked="" type="checkbox"/>	
Network Policy Violation - WLAN Authentication	Minor	<input checked="" type="checkbox"/>	
Client/Server		<input type="checkbox"/>	
Application		<input type="checkbox"/>	
Session		<input type="checkbox"/>	
Transport		<input type="checkbox"/>	
Network		<input type="checkbox"/>	
Data Link		<input type="checkbox"/>	
Physical		<input type="checkbox"/>	

Figure 6. Wireless Network Policies in OmniPeek.

Security issues are not always malicious. Even with well-established security policies in place, well-intentioned users can be inadvertently violating these policies due to misconfigured security settings or simply an overall lack of knowledge of wireless security. With OmniPeek, security policies established around common operating procedures like those illustrated in Figure 6 can be monitored in real time, providing instantaneous alerts when a single client is in violation of the policy.

Troubleshooting a WLAN: 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 are more easily resolved if wireless-originated traffic is captured and analyzed before it enters the DS. To determine whether APs 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, as shown in Figure 7.

Getting the Most from Your Wireless Network

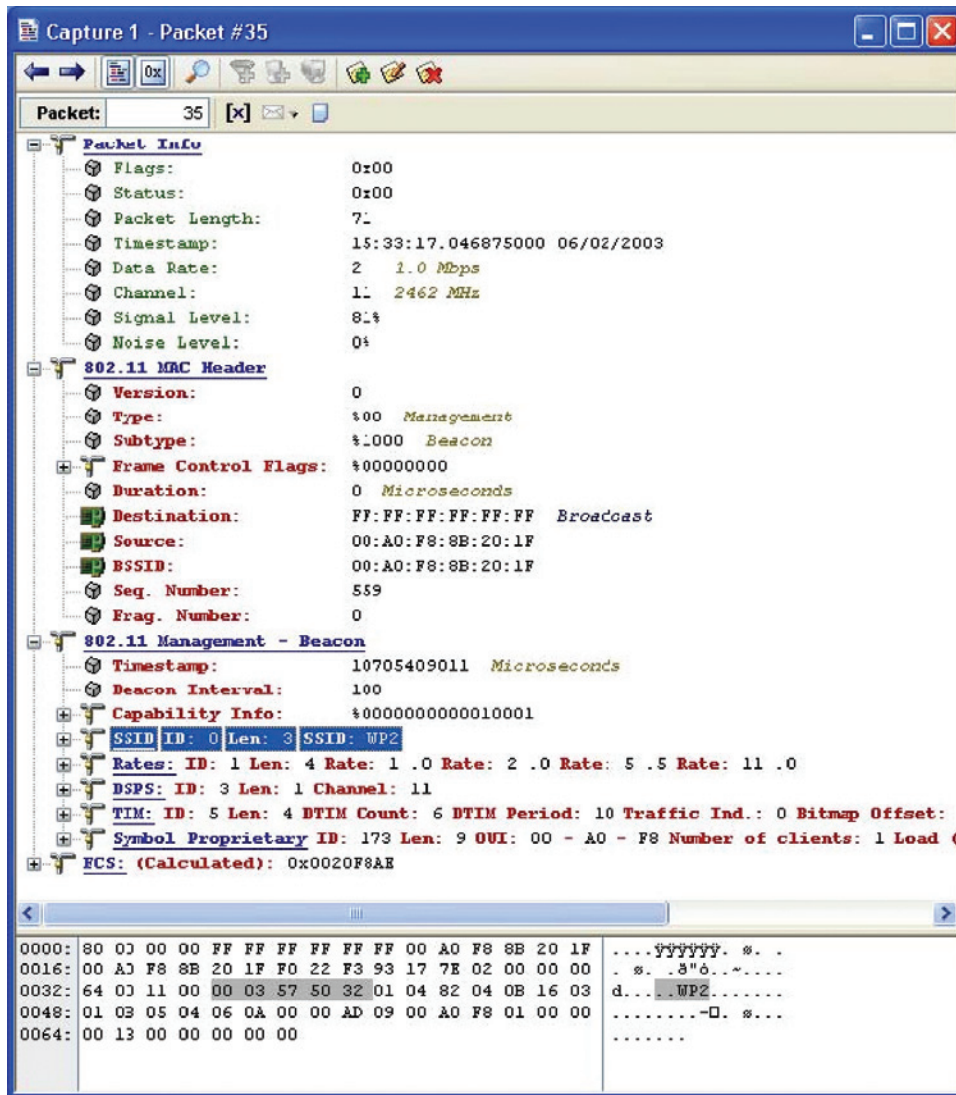


Figure 7. Partial Example of a detailed OmniPeek packet decode.

In an all-wireless environment, the only way to troubleshoot higher-level protocols like TCP/IP is to capture the packets off the air. In smaller satellite offices in particular, this all-wireless solution is increasingly common. It offers quick setup 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 AP.

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 security 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 security in the same way as all other nodes on the network must be built into the analyzer.

Getting the Most from Your Wireless Network

Leveraging Existing Assets with AP Capture Adapters

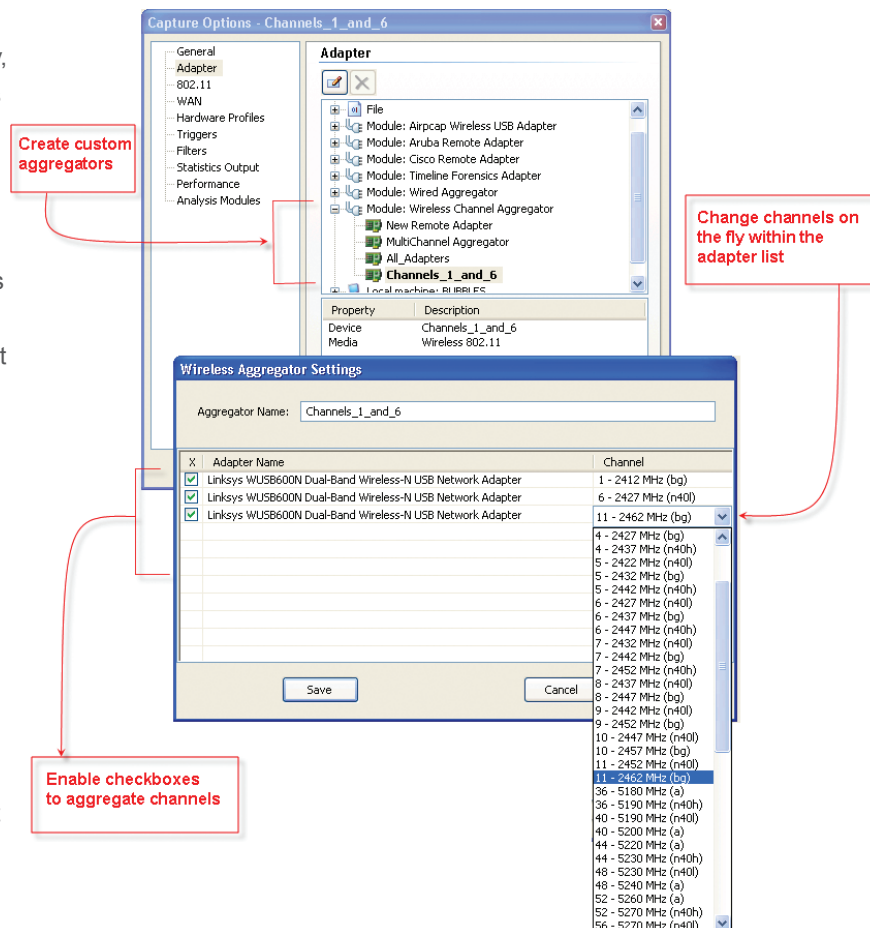
One of the most significant issues that exists in WLAN troubleshooting today is access to the network packets at the source of the trouble. Overlay networks, a deployment of wireless sensors that can monitor all wireless traffic from existing APs, is an effective but very costly means of having instantaneous access to wireless packets. A far more attractive solution is to capture packets using the existing wireless network—after all, the hardware is designed to both transmit and receive. With WildPackets AP Capture Adapters, the wireless network can be employed to do just that. An AP Capture Adapter allows existing APs to be put into a “listen-only” mode, and directs them to forward all of the packets they receive to OmniPeek over the wired network. No additional hardware, or expense, is required to implement this solution. Access to information for troubleshooting from any location on the network is only a few clicks away.

Multi-Channel Analysis

The WildPackets Wireless Channel Aggregator extends OmniPeek with powerful features specific to the capture and analysis of wireless traffic across multiple channels. It captures wireless packets from multiple channels simultaneously (without scanning), measures vital statistics on each channel separately, and calculates the latency of devices roaming between APs. The Wireless Channel Aggregator can capture and aggregate packets from any heterogeneous wireless capture device that supports the WildPackets API, making it a very cost-effective solution for performing multi-segment analysis, as seen in Figure 8.

Roaming Latency Analysis

Roaming latency is the amount of time it takes for a wireless device to move from one AP to another. This is also known as re-association. WildPackets Roaming Latency Analysis measures this type of latency by calculating the amount of time between the last known data packet for a device on one AP, and the first data packet seen for that device on another AP.



Getting the Most from Your Wireless Network

One example of roaming latency is wireless VoIP on mobile devices. More than a few hundred millisecond delay between packets leads to unacceptable quality and even dropped calls. Delays and dropped calls can occur when mobile wireless devices, such as laptops or phones, roam from one channel to another. Until recently, solutions were only able to scan one channel at a time in a round-robin fashion leaving as much as 90% of wireless data unmonitored at any one period, making analyzing the data for troubleshooting and optimization almost impossible. The issues are connection-disconnection problems, less signal strength, dropped transmissions either on the phone in VoIP Wi-Fi environments or with laptops.

The latest extensions to OmniPeek now offer real-time multi-channel capture, aggregation and analysis of wireless networks to pinpoint the root cause of these issues and keep wireless networks running smoothly, as seen in Figure 9.

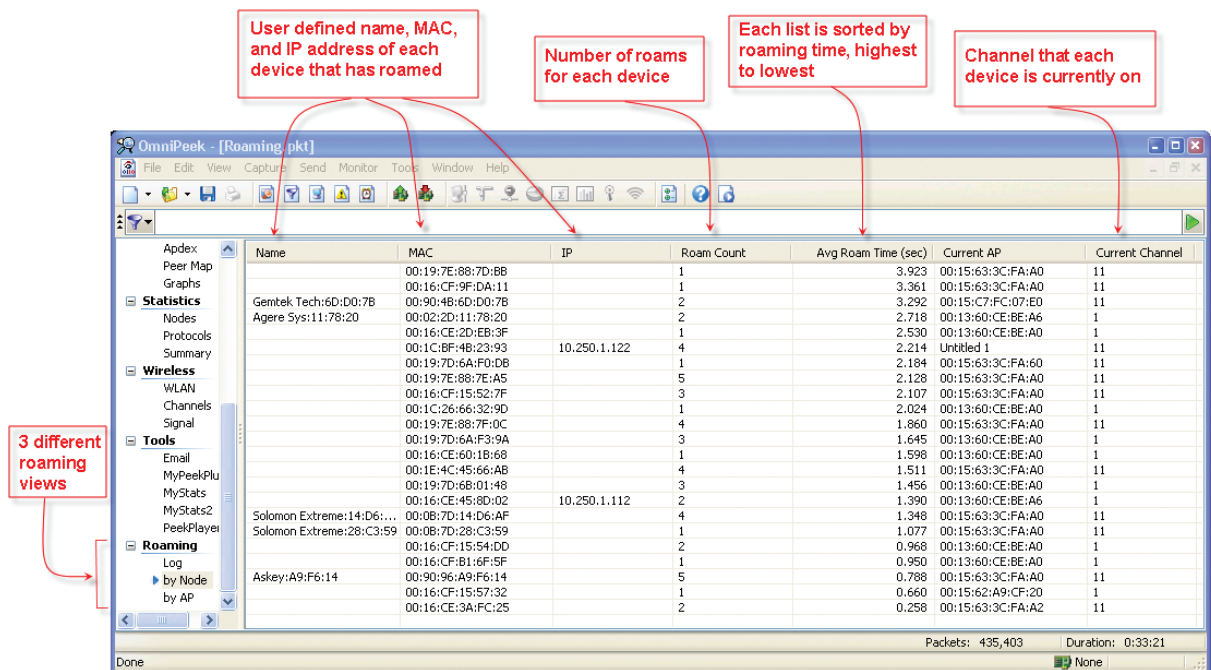


Figure 9. Roaming Latency group of tabs in the “by Node” view.

Conclusion

In every industry, real-time network monitoring and rapid troubleshooting have become mission-critical. Network disruptions are now business disruptions, with financial and sometimes even legal consequences. IT departments are working full-time to manage data centers, provision new applications, and respond to help desk requests. More than ever, you need solutions to monitor and troubleshoot problems wherever they are occurring on the network, quickly and efficiently, so that business and other essential IT operations are not disrupted.

Whether viewing network activity for application usage, protocol distribution, node activity or the network packets themselves, or leveraging built-in Expert network analysis, WildPackets Distributed Analysis Solutions enable you to visualize global network performance and analyze root cause failures more quickly and effectively than any other solution.

Getting the Most from Your Wireless Network

Wireless Abbreviations and 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

AES - Advanced Encryption Standard

Base Station - Access Point

BSS - (Basic Service Set) Wireless network utilizing only one access point to connect to a wired network

CBC-MAC - Cipher Block Chaining Message Authentication Code

CCK - Complimentary Code Keying

CCMP - CTR (Counter mode) with CBC-MAC Protocol

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

DCF - Distributed Coordination Function

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

EAPOL - EAP (Extensible Authentication Protocol) over LAN

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

FCS - Frame Check Sequence

FHSS - Frequency Hopping Spread Spectrum

GTK - Group Temporal Key

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

MIMO - Multiple Input, Multiple Output

NIC - Network Interface Card

OFDM - Orthogonal Frequency Division Multiplexing

PBCC - Packet Binary Convolutional Coding

PCF - Point Coordination Function

PMK - Pair-wise Master Key

PPM - Pulse Position Modulation

PSK - Pre-Shared Key

PTK - Pair-Wise Transient Key

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

RF - Radio Frequency

RTS - Request To Send

Getting the Most from Your Wireless Network

WEP - Wired Equivalent Privacy

WFA - Wi-Fi Alliance, an industry organization specializing in interoperability and promotion of 802.11 WLAN equipment

WLAN - Wireless Local Area Network

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access, version 2

WildPackets Distributed Analysis Solutions

WildPackets gives network engineers real-time visibility into every part of the network—simultaneously from a single interface—including 10/100, Gigabit, 10 Gigabit (10G) Ethernet, 802.11 wireless, and VoIP.

Using OmniPeek's local capture capabilities, centralized console, distributed OmniEngine intelligent software probes, Omnipliance and TimeLine network recorders, and Expert Analysis, engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

WildPackets Distributed Analysis Solutions:

- Monitor entire enterprise networks, including network segments at remote offices
- Provide real-time analysis of mission-critical network services
- Secure diagnostic communications so analysis never compromises security
- Optimize diagnostic communications to minimize impact on networks using Intelligent Data Transport™
- Are flexible, scalable, and extensible to grow with network needs
- Monitor and troubleshoot Voice and Video over IP applications without having to invest in stand-alone tools or special hardware
- Analyze application performance in the context of overall network activity

Learning More

- "Introduction to Wireless Networking" is the first in a three part series. It covers wireless network architecture, topologies and security issues.
- "Getting the Most from Your Wireless Network" is the second in a three part series. It outlines best practices in monitoring, analyzing, and troubleshooting wireless networks.
- "Finding and Fixing VoIP Call Quality Issues" is the third in a three part series. It examines a specific use case and identifies factors that lead to poor VoIP call quality and presents best practices for keeping quality of service high.

All of these white papers and more can be found at www.wildpackets.com under the "Downloads" section.

About WildPackets, Inc.

WildPackets develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize and secure their wired and wireless networks. WildPackets products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Motorola, Nationwide and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP).