DATASHEET

OmniPeek for Wireless
Gigabit Wireless Requires Gigabit Wi-Fi Analysis

New Technologies Require New Solutions

Wi-Fi networks are everywhere and the number of connected devices is growing exponentially. A quick Google search will turn up numbers like billions of connected devices, and with the Internet of Things driving connectivity, these estimates could be low.

At the same time we are seeing another Wi-Fi revolution regarding the speed and capacity of Wi-Fi networks. With the introduction of 802.11ac, Wi-Fi is now at gigabit speeds, and as new phases of 802.11ac equipment are introduced data rates could reach as high as 6.93Gbps.

Users of Wi-Fi are thrilled, but this rapid expansion of Wi-Fi is causing serious difficulties for those with the responsibility of managing wireless local area networks (WLANs). The solutions and methodologies that worked with b/g networks at 54Mbps are simply outdated and cannot be made to adapt to today's Wi-Fi technology. New solutions and methodologies are needed.

OmniPeek for Wireless – Performance, Ease-of-use, Flexibility

WildPackets' OmniPeek Wi-Fi analysis solution addresses the needs of today's WLANs. It is specifically designed to capture data from high-speed networks, fully capable of handling even the fastest 802.11ac network configurations. Its award-winning UI simplifies WLAN analysis, enabling network engineers to find problems fast. Flexible data capture and storage solutions allow users to work with OmniPeek in the way that best suits them – whether portable, distributed, or remote. For mission-critical applications, wireless forensics can be used to capture and store wireless data for detailed, post-capture, analysis and verification.

OmniPeek provides the most advanced Wi-Fi analysis technology available anywhere:

- The first to support data capture and analysis of 802.11ac traffic
- The only to support 802.11n 3-stream (450Mbps) portable analysis
- The most comprehensive for voice-over-wireless (VoFi) analysis
- The only to support remote data capture from commercial enterprise APs
- The best for distributed networks with remote 24x7 real-time analysis
- The only to support packet capture from non-technical users
- The most cost-effective by supporting both wireless and wired network analysis in the same solution
- The most comprehensive with an industry-leading UI that simplifies root cause analysis

Flexible Data Collection for High-Speed Networks

Portable Analysis

Portable analysis has been the approach of choice for WLAN network analysis for years. OmniPeek WLAN analysis software and USB supported WLAN adapters can be placed in sniffer mode to capture packets from multiple channels simultaneously. This solution is used by field engineers and IT consultants where portability is a key requirement.

Remote Analysis

As WLANs become more numerous, the networks are often across the campus or across the country. Remote analysis eliminates the need to travel to a hotspot for troubleshooting. Remote Analysis uses existing WLAN infrastructure assets to capture data and forward it over the wired network to your desktop. This approach is very useful for all those times the problem isn't near you.

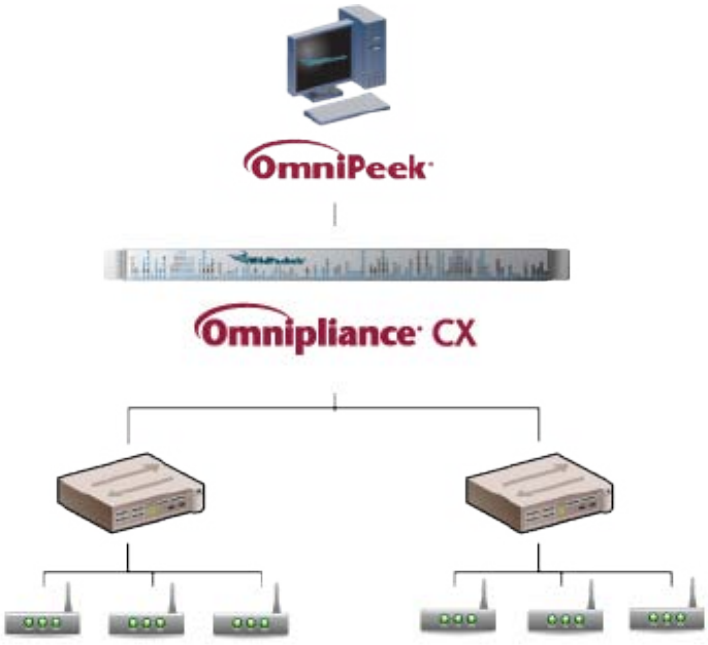
"Abandon all doubt that 802.11ac is replacing 802.11n – today. Except in very limited or unbelievably-cost-constrained situations, I can't see further installations of .11n making any sense."

Craig Mathias,
The Farpoint Group
December 2013

"WildPackets saves Houston Methodist countless hours of post deployment labor. Houston Methodist can quickly pinpoint a Wi-Fi client problem and work with the Wi-Fi vendor for a quick resolution before deployment"

Distributed WLAN Analysis

Distributed WLAN analysis uses deployed APs to capture data and Omnipliances deployed at the WLAN controller to analyze and store data. The Wi-Fi analysis is performed locally at the Omnipliance and provides ongoing 24x7 analysis. This approach is preferred for environments with high Wi-Fi data volumes like enterpises, schools, and universities.



Wireless Forensics

Distributed WLAN analysis allows you to record Wi-Fi traffic 24x7 to an Omnipliance. WLAN issues can then be analyzed both in real-time or post-incident, also known as Wireless Forensics. With wireless forensics, you can accelerate your response to service degradation and outages, increasing uptime while reducing IT labor costs. Wireless forensics is useful in mission-critical environments like financial services, healthcare, retail and warehouses.

OmniPeek for Wireless Advantages

Capture wireless data from anywhere, with almost anything

Wireless networks are highly distributed. It is now virtually impossible to be where the problem is being reported. You need to be able to capture data remotely, with whatever is available. And you need to capture data from the most up-to-date WLAN equipment, including 802.11ac 3-stream and 4-stream. OmniPeek provides the support you need. No other product offers this level of flexibility.

"802.11ac is fast, and OmniPeek is up to the challenge. Designed for use on both wired and wireless networks, OmniPeek is built for speed. It has been used to analyze 1 and 10G networks by over 6,000 customers."

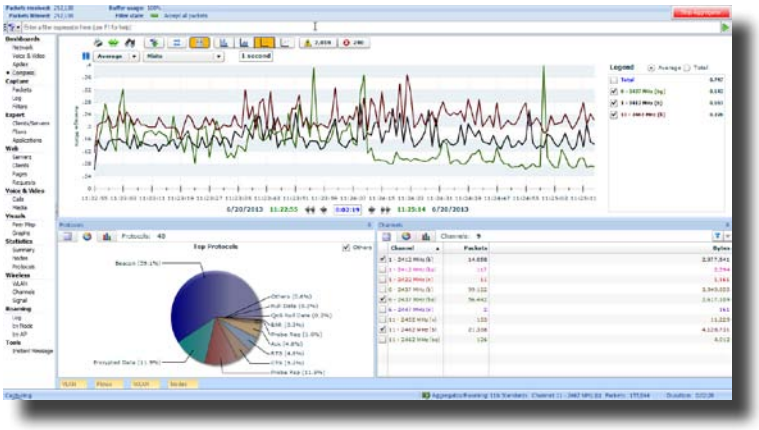
See who's connected to which APs

Before initiating any analysis, you need to get the lay of the land. The WLAN view in OmniPeek does just that, showing you which networks are available, which APs are servicing those networks, and which clients are connected to which APs, along with all of the associated configuration details (bands, channels, security, signal, noise, data rates, etc.).

Detailed analysis for any situation

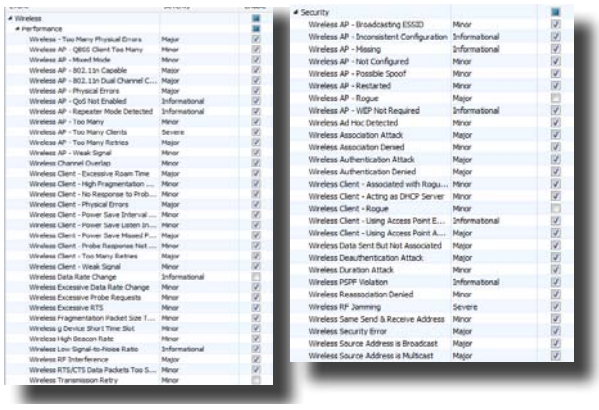
With the most complete analysis capability of any WLAN analysis solution, OmniPeek is capable of determining the root cause of any issue on your WLAN. From simple issues, like poor or no connectivity from an AP, to complex issues like intermittent dropped connections on specific BYOD device models, OmniPeek can address it all.

Multi-channel analysis – visibility into all Wi-Fi traffic



Most WLANs operate on multiple channels – that's how we keep APs from interfering with each other. Analysis solutions that scan through the channels do not provide the level of detail needed for analysis and troubleshooting. Your WLAN analysis solution must be able to capture data on multiple channels simultaneously, without dropping any data. OmniPeek does exactly that.

Expert Events – alerts to WLAN issues



What good is a WLAN network analysis solution if you have to sit in front of it all day long? A truly effective solution runs 24x7, performing analysis for you, and leaving you free to do other things. When problems begin to surface you're immediately notified so you can take quick action. OmniPeek provides over 50 wireless-specific Expert analytical functions, which constantly monitor and analyze your WLAN for you.

Roaming analysis – analyze real-world quality of experience

Wireless networks are designed for mobility. As users we take that for granted every day. As analysts, we know it implies a wide range of problems that are never encountered on wired networks. Once users connect to a WLAN, roaming is typically the number one issue that impacts the user experience. Handoffs from AP to AP take time, and although 802.11 standards and improvements have been introduced over time, these handoffs can cause significant issues for users, from poor voice over Wi-Fi (VoFi) quality to dropped VPN connections. OmniPeek continuously analyzes the WLAN and identifies and logs all roaming activity, whether from AP to AP, channel to channel, or both. It reports roam time for clients and APs, and provides a "single-click" drill down for detailed, millisecond visibility of the roaming activity.

Filters – see only the data of interest

Network analyzers capture a great deal of data quickly. OmniPeek is of course designed to handle that, but when it comes to analyzing the data a smaller data set is much easier to manage, especially when you know what you're looking for. With OmniPeek you can apply filters before starting a capture, which limits the data collected, or on-the-fly, filtering out data simply for visualization, but leaving all the collected data in tact just in case you need to apply a different filter to find what you're looking for. OmniPeek provides over 100 built-in filters, half of which are wireless-specific. Custom filters are extremely easy to create using the GUI filter builder, or they can be created using the BPF filter bar for quick, on-the-fly access.

Manage BYOD with rogue detection

With the rapid adoption of BYOD, keeping track of friend or foe on your WLAN can be a real chore. OmniPeek makes it easy with simple device classification that is session independent. Once you classify a device it is stored in the OmniPeek Name Table so it will always be recognized and categorized in the same way. Devices can be identified as Trusted, Known, or Unknown. Trusted devices are typically those under your control. Known devices include things like neighboring APs – you know they're there, but not under your control. Unknown devices should be investigated – these are possible rogue devices.

About WildPackets

WildPackets, Inc., founded in 1990, develops network and application analysis solutions that enable organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets has more than 6,000 customers, and its products are sold in over 60 countries in all industrial sectors. Customers include Safeway, Boeing, Siemens, AT&T, Motorola and over 80% of the Fortune 1000. For more information, please visit www.wildpackets.com.

WildPackets

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597

T (925) 937 3200
F (925) 937 3211
www.wildpackets.com