The new IEEE 802.11ac standard is truly exciting as it breaks the gigabit barrier. This latest WLAN technology enables enterprise organizations to deploy new applications and better support mobile users with improved business operations, productivity, and growth. This white paper outlines the 802.11ac market and technology, and describes best practices for troubleshooting large and small enterprise deployments.
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

Table of Contents

Introduction .......................................................................................................3
802.11ac Overview ...........................................................................................3
802.11ac Technical Description ........................................................................4
802.11ac Deployment in the Enterprise............................................................5
WLAN Network Monitoring and Troubleshooting for 802.11ac networks ....... 6
WildPackets solutions for 802.11ac ...............................................................12
Summary and Conclusion .............................................................................. 13

Table of Figures

Figure 1. The evolution of 802.11 data rates .................................................... 3
Figure 2. Comparison of 802.11ac to 802.11n.................................................. 4
Figure 3. Aggregate 802.11ac Capacity for Typical Deployment Scenarios..... 8
Figure 4. Example Screenshot .......................................................................10
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

Introduction

802.11ac takes a big step forward with unprecedented performance, capacity, reliability, and RF efficiency. With this WLAN advance comes noteworthy deployment and optimization challenges. The traditional techniques of WLAN data capture and troubleshooting will not keep up with the very high throughput of 802.11ac. For network managers planning 802.11ac pilots and migration, this white paper recommends options and best practices to assure optimal network operation.

802.11ac Overview

It’s hard to believe that the IEEE ratified the first 802.11 standard over 15 years ago. According to ABI research, over 5 billion Wi-Fi enabled devices had shipped by the end of 2012. We have seen 802.11 evolve from 2 Mbps standard to an aggregate capacity of up to 7 Gbps with 802.11ac. This is a remarkable evolution in WLAN technology for consumers and businesses alike.

Why is 802.11ac a big deal? Simply stated - it’s fast - the first wireless LAN standard to break the gigabit barrier.

<table>
<thead>
<tr>
<th>Year</th>
<th>Data Rate</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1991</td>
<td>1-2 Mbps</td>
<td></td>
</tr>
<tr>
<td>1997</td>
<td>802.11b</td>
<td>550%</td>
</tr>
<tr>
<td>1999</td>
<td>802.11g/a</td>
<td>490%</td>
</tr>
<tr>
<td>2003</td>
<td>802.11n</td>
<td>833%</td>
</tr>
<tr>
<td>2009</td>
<td>300/450/600 Mbps</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>433/866/1300+ Mbps</td>
<td>288% (vs 450) (to 6.93 Gbps)</td>
</tr>
</tbody>
</table>

Figure 1. The evolution of 802.11 data rates

In addition to notable performance advances, there are a number of other enhancements over previous 802.11 standards:

- Significant range improvements with better performance at any range with fewer dead spots
- Standardized beam-forming supports reliable connections for media streaming
- Wider channel bandwidths for more efficient spectrum utilization
- Support for up to 8 spatial streams enabling more throughput per device
- Multi-user MIMO (MU-MIMO) that allows 802.11ac nodes to transmit data to multiple clients simultaneously, increasing WLAN efficiency
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

<table>
<thead>
<tr>
<th>Specification</th>
<th>802.11n</th>
<th>802.11ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>2.4 GHz and 5 GHz</td>
<td>5 GHz only</td>
</tr>
<tr>
<td>Channel Widths</td>
<td>20 and 40 MHz</td>
<td>20, 40, and 80 MHz (160 MHz optional)</td>
</tr>
<tr>
<td>Spatial Streams</td>
<td>Up to 4</td>
<td>Up to 4 per client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Up to 8 total</td>
</tr>
<tr>
<td>Multi-user MIMO</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Single Stream (1x1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Stream (1x1)</td>
<td>150 Mbps</td>
<td>433 Mbps</td>
</tr>
<tr>
<td>Max Client Data Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Three Stream (3x3:3)</td>
<td>433 Mbps</td>
<td>1.3 Gbps</td>
</tr>
<tr>
<td>Max Client Data Rate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Not surprisingly, these enhancements introduce new WLAN deployment and monitoring challenges. With 802.11ac operating only in the 5 GHz band, these challenges take on a different scope than 802.11n. The 5 GHz band is clearly under-utilized, and has fewer sources of interference, making this choice a wise one for 802.11ac.

Since interoperability is only required with 802.11a and 802.11n devices in the 5 GHz band, 802.11ac enables investment protection and eases the process of network migration. However, the slower transmission rates of legacy devices will likely impact the overall benefit of 802.11ac in non-greenfield deployments.

802.11ac Technical Description

The 802.11ac standard extends the significant advances made in 802.11n to deliver this next generation rise in WLAN speed and capacity. To achieve these advances, a number of enhancements have been implemented in both the MAC and Physical Layer. The key improvements include:

- Wider channels – 80 and optional 160 MHz channel widths were added to the 802.11n 20 and 40 MHz options. Wider channels provide increased bandwidth for 802.11 RF transmissions, resulting in greater overall data rates. In general, a doubling of the channel width results in a doubling of the data rate. Channelization is straightforward in that congruent sub-channels are grouped into pairs for 80 and 160 MHz operation. For example two adjacent 40 MHz sub-channels are grouped to make one 80 MHz channel. There is also an “80+80” option, allowing data to be sent simultaneously over two non-adjacent 80 MHz channels. Channel usage is negotiated per client device, enabling 802.11a, 802.11n, and 802.11ac clients to coexist, with each operating at their respective bandwidth and data rate capabilities.

Farpoint Group predicts that critical mass usage of 802.11ac BYOD client devices will occur in 2014 and 802.11ac access point infrastructure in 2015.
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

• Improved modulation increases data transfer efficacy and renders higher data rates. Expansion of 802.11n OFDM (Orthogonal frequency-division multiplexing) and adding 256 QAM (quadrature amplitude modulation) enables more bits to be encoded in the same channel size.

• Up to eight spatial streams (doubling that of 11n) also contribute to an increased aggregate data rate. MIMO (Multi-input, Multi-output) allows multiple data streams to be sent simultaneously, maximizing reliable throughput. As an example, with a single-stream 802.11ac client operating in an 80 MHz channel, the maximum theoretical data rate is 433 Mbps while a 2-stream client operating in an 80 MHz channel can achieve an 867 Mbps theoretical data rate.

• Beamforming, which is optional in 802.11n is now specified in 802.11ac, enabling interoperability in a multi-vendor WLAN environment. Beamforming enables an AP with multiple antennas to better aim its signal transmission toward an 802.11 receiver. This is ideal for clients that don’t move around much, like a video receiver or a set-top box. Beamforming allows the power in an RF signal to be increased in the path between the AP and the client, enabling better range and greater signal reliability. This is in contrast to a standard 802.11 transmission with sends the signal in all directions (omnidirectional), diluting the power in the signal much more rapidly with distance.

• MIMO was first introduced in the 802.11n standard, and enables an AP to transmit multiple data streams to a single client device, significantly increasing the overall data rate to that single client. With MU-MIMO, APs will be able to transmit streams to multiple clients simultaneously – a first in wireless LANs. A great use case is simultaneous streaming of a single video to multiple clients. In addition to enabling a much higher aggregate data rate, it also increases the reliability of communications for latency-sensitive applications like VoIP and video.

• As previously noted, 802.11ac operates exclusively in the 5 GHz band. Since most 802.11n deployments historically have been in the 2.4 GHz band, backward compatibility issues are likely to be small when 802.11ac is added to the mix. There are clear advantages to 5 GHz operation. The most obvious is that the performance gains in 802.11ac come in part from wider channel usage and the ability to access adjacent channels. The 2.4 GHz band is simply too limited in terms of available spectrum and channels. In addition, the 5 GHz band has seen limited usage so far, making 802.11ac Greenfield deployments a possibility. And the 5 GHz band is less prone to interference from non-802.11 devices.

There are mission critical requirements that will drive 802.11ac usage in the enterprise. These include bandwidth hungry, uptime dependent, and latency sensitive applications including:

• HD video and video conferencing
• Voice over Wi-Fi (VoFi)
• Medical imaging portability
• Campus-wide IPTV, video streaming
• Wired network expansion/replacement
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

802.11ac Deployment in the Enterprise

Let's take a look at primary use cases in enterprise organizations. Typically, 802.11ac will be additive to an existing network, and not a “rip-and-replace” of 802.11n APs and clients. Certainly for the next several years support for legacy 2.4 GHz and 5 GHz devices will be required. Likely early enterprise deployment scenarios include:

- As an overlay of existing networks for targeted applications: One example is power-user “hot spots” that benefit from increased performance – such as locations were medical imaging or live video streaming applications are in use. Areas with high density and high demand WLANs such as lecture halls, conference rooms, and dormitories benefit from increased 802.11ac throughput, increased channel width, and more spatial streams. An overlay network enables gradual, well-managed migration from 802.11n and earlier 802.11 technologies.
- In Greenfield deployments where it is more cost effective to go completely wireless: The performance and availability of an 802.11ac WLAN does not quite match that of a wired network, but it certainly provides the necessary throughput for just about any application and any user. The mobility and cost savings of deploying a wireless only network may outweigh any additional benefits of installing both a wired and wireless network.
- Pilot networks: Most enterprises are already planning and deploying 802.11ac networks for proof of concept, knowing that future WLAN upgrades or expansions will be based on this new standard.

Regardless of the scenario, the deployment of 802.11ac changes the game when it comes to WLAN planning, performance assessment, network administration, and troubleshooting. Up until now WLAN analysis and troubleshooting has primarily relied on portable solutions based on USB adapters for “over-the-air” packet capture and analysis. With 802.11ac, this technique is less effective. We will address the reasons for this later in this paper.

WLAN Network Monitoring and Troubleshooting for 802.11ac Networks

WLAN performance assessment allows the network administrator to measure overall network health. Tuning for optimal performance requires that monitoring tools be capable of capturing the wireless transmissions between communicating devices. This means these tools must have a measuring point in the vicinity of the wireless signals. This is typically done with a packet-based network monitoring and analysis solution, which “sniffs” every packet within range of the measuring device, generally capturing data within a few hundred feet. This enables the compilation of overall WLAN statistics in order to analyze specific characteristics per client, such as encryption state, authentication method, data rate, signal and noise statistics, and retransmission rates.

WLAN monitoring must also include continuous security audits. This goes beyond simply deploying standard encryption and authentication mechanisms. Compliance to security policies and intrusion protection from rogue devices and network attacks must continually be monitored. Many WLAN analysis solutions provide automated network monitoring for common security issues and policy violations.

The challenge of WLAN troubleshooting is capturing the wireless packets over the air. To accomplish this, key practices include placing portable analysis systems within range of the wireless signals, or leveraging existing wireless assets, such as deployed APs.
“802.11ac is clearly the trend for the future. While upgrades will take some time, the Farpoint Group believes that it is important to begin preparing the organizational network for the arrival of this new technology. Properly planned and executed, this transition can be easy for network operations staff and smooth and transparent for users.”

Craig Mathias, Farpoint Group, April 2013

Since 802.11ac is evolutionary, the basic tenets of WLAN monitoring and troubleshooting don’t change. However, with significant capacity improvements, including more clients per AP and higher data rates, methodologies that have worked well up to now, will not be as effective for 802.11ac.

The Challenges of 802.11ac Troubleshooting

There are a number of challenges in analysis of high performance WLANs.

Network Data Capture at the Point of Failure

First, given the pervasive deployments of WLANs, it is becoming less likely that a network engineer can always be in the vicinity of a problem. As stated earlier, troubleshooting a WLAN requires that data be captured within a few hundred feet of the problem – there is no way around this – it’s a matter of physics! As WLANs become more widespread, network engineers must plan for remote solutions to capture data when problems arise.

Network Analysis at gigabit speeds

The availability of high performance network analysis solutions is also a critical issue. With the first phase of 802.11ac, AP data rates already perform up to 1.3 Gbps. This means that the analysis software for WLANs must have the same performance capability as that of gigabit Ethernet LANs. Most WLAN analysis software was originally designed to handle only one-tenth the data rates of 802.11ac. So care must be exercised to ensure that the analysis software can handle the 802.11ac data rates.

USB is not up to the task

In addition to network analysis platforms, USB bus speeds and WLAN USB adapters are simply not up to the task of 802.11ac packet capture. Most laptops in use for WLAN analysis have USB v2.0 ports. USB 2.0 has a maximum theoretical speed of 480 Mbps, and a practical limit of 280 Mbps. This is clearly slower than the current data rate of 1.3 Gbps, and falls far short of the rates that will be achieved with 802.11ac Phase 2. Even “Super Speed” USB v3.0, with its effective throughput of 3.2 Gbps, will barely make the grade for most 802.11ac performance scenarios, as depicted in Figure 3. This means that even if both the 802.11ac USB adapter and the laptop support USB 3.0, there are still 802.11ac scenarios that cannot be fully analyzed.
Best Practices for Monitoring and Troubleshooting 802.11ac Networks

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Typical Client Form Factor</th>
<th>PHY Link Rate</th>
<th>Aggregate Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-antenna AP, 1-antenna STA, 80MHz</td>
<td>Handheld</td>
<td>433 Mbit/s</td>
<td>433 Mbit/s</td>
</tr>
<tr>
<td>2-antenna AP, 1-antenna STA, 80MHz</td>
<td>Tablet, Laptop</td>
<td>867 Mbit/s</td>
<td>867 Mbit/s</td>
</tr>
<tr>
<td>1-antenna AP, 1-antenna STA, 160MHz</td>
<td>Handheld</td>
<td>867 Mbit/s</td>
<td>867 Mbit/s</td>
</tr>
<tr>
<td>2-antenna AP, 2-antenna STA, 160MHz</td>
<td>Tablet, Laptop</td>
<td>1.73 Gbit/s</td>
<td>1.73 Gbit/s</td>
</tr>
<tr>
<td>4-antenna AP, 4 1-antenna STAs, 160MHz (MU-MIMO)</td>
<td>Handheld</td>
<td>867 Mbit/s to each STA</td>
<td>3.47 Gbit/s</td>
</tr>
<tr>
<td>8-antenna AP, 160MHz (MU-MIMO)</td>
<td>Digital TV, Set-top Box, Tablet, Laptop, PC, Handheld</td>
<td>3.47 Gbit/s to 4-antenna STA</td>
<td>6.93 Gbit/s</td>
</tr>
<tr>
<td>-- 1 4-antenna STA</td>
<td></td>
<td>1.73 Gbit/s to 2-antenna STA</td>
<td></td>
</tr>
<tr>
<td>-- 1 2-antenna STA</td>
<td></td>
<td>867 Mbit/s to each 1-antenna STA</td>
<td></td>
</tr>
<tr>
<td>-- 2 1-antenna STAs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-antenna AP, 4 2-antenna STAs, 160MHz (MU-MIMO)</td>
<td>Digital TV, Tablet, Laptop, PC</td>
<td>1.73 Gbit/s to each STA</td>
<td>6.93 Gbit/s</td>
</tr>
</tbody>
</table>

Figure 3. Aggregate 802.11ac Capacity for Typical Deployment Scenarios

Capture support for 3- or 4-stream packets

Perhaps the most significant USB limitation is that even the most capable adapters support only 802.11ac 2-stream transmission and reception. This translates to a maximum 867 Mbps throughput. Such a device will only capture 1- and 2-stream packets. Any 3- or 4-stream packets on the WLAN will simply be ignored. Because the USB adapter is not able to capture these packets, they cannot be monitored or analyzed for troubleshooting. Clearly, this not acceptable for an analysis solution that you trust to report on everything about your WLAN environment. And it is unlikely that 3- and 4-stream USB WLAN adapters will ever come to market. The primary use case for a USB WLAN adapter is to add 802.11 networking support to a device that currently does not have it. As technology advances, 802.11 networking is being built into every device imaginable, eliminating the need for USB WLAN adapters.

The Solution: Using an 802.11ac AP as a Packet Capture Device

Undoubtedly new methods must be employed for capturing data to plan, analyze, and troubleshoot 802.11ac networks. The trend for data capture will rapidly migrate to leveraging APs already deployed in the network, versus relying on portable analysis with USB WLAN capture devices. Using an 802.11ac AP as a packet capture device has significant advantages:

- The APs are already part of the network and inherently have the capacity to capture whatever traffic is on your WLAN.
- APs are located exactly where you need them to capture 802.11 packets, eliminating the need for additional sensors or “overlay” networks for monitoring.
- Capturing directly from APs allows for remote analysis – anywhere and anytime – eliminating the need to travel to locations simply to capture wireless traces.
• When designed with appropriate overlap, one or several APs can be used as a sensor, or in promiscuous mode, without disrupting WLAN operation. Plus when not in sensor mode, the AP simply increases the overall coverage and performance of the WLAN.

Access points for data capture can be utilized in one of two ways:

• Directly connected to a laptop running a network analyzer such as WildPackets' OmniPeek via the AP and laptop Ethernet ports. This provides portable analysis capability without the limitations of a USB WLAN adapter.
• Remotely connected, to collect data from APs that are installed as part of the WLAN.

For either approach, there are two different, but similar, connection methods:

• Using an AP that supports RemotePcap (Remote Packet Capture). RemotePcap is an open source AP feature included with the Pcap library, commonly used in enterprise APs.
• Using an AP with custom remote adapter software specifically designed to tunnel packets between an AP and specific WLAN analysis software.

In either scenario the AP must be configured (typically via the AP wireless controller) for use in promiscuous, or “sniffing” mode. Depending on the access point manufacturer and model, it will either be able operate as both a sniffer and an AP or as a sniffer only.

Remote Packet Capture (RemotePcap)

RemotePcap is an industry standard that enables interaction with one or more APs to capture WLAN packets for analysis. These captured packets are then forwarded over the wired network to a system running WLAN analysis software. While remotePcap is generally available in enterprise-grade APs, the feature typically doesn’t show up in marketing materials.

RemotePcap operates in two different modes:

• Passive Mode operation is the default method. Here, the user directs the network analyzer to connect to an AP that supports RemotePcap (via the RemotePcap daemon). Once the connection is established, the AP sends a list of supported RemotePcap interfaces back to the analyzer. The user then chooses which interfaces to use and manually starts the capture.
• In Active Mode the AP running the RemotePcap daemon initiates the connection to the network analyzer. The analyzer sends the appropriate commands to the daemon to automatically start the capture. This mode is useful in cases where the remote daemon is behind a firewall and cannot receive connections from the external world. The daemon can be configured to establish a connection to a given host, which is set up to wait for that connection.

The main advantages with using RemotePcap are that it is a defacto standard - no custom software is required, and all supported devices will operate in a consistent manner. However, the challenge is in discovering which APs support RemotePcap. The best way to do this is to contact the manufacturer directly.
Custom Remote Adapters

Custom Remote Adapters are essentially software “shims”, developed by either enterprise AP manufacturers or WLAN analysis software providers. They use a proprietary tunnel to send packets directly from an AP to a WLAN analyzer such as WildPackets OmniPeek. The custom remote adapter allows the AP to look like it is physically connected to the analyzer, even though it is located remotely. With a custom remote adapter both the AP (or WLAN controller) and the network analyzer must be connected to the same wired network. Leading enterprise vendors such as Cisco, Aruba, and Meru Networks have developed custom remote adapters for WildPackets OmniPeek.

This method of remote packet capture has significant advantages. AP packet streams are not necessarily standard which creates the potential for complex configuration and software tweaking. A custom remote adapter provides not only a tunnel to send the packets but it is also designed to handle the translation between the network analyzer and the AP. With OmniPeek, for example, set-up and use is simple and straightforward. On the AP side, the user changes the AP to sniffer mode, sets the channel that the AP will use to capture packets, and specifies the IP address to which the AP should forward the packets. The IP address is for the computer running the WLAN analysis software. At this point, packets are already flowing. The user then configures the appropriate remote adapter via the analysis software GUI and starts a capture. This software then immediately begins processing and analyzing the packet flow from the AP(s).
Access Point Capture and Wi-Fi Analysis - Rules for the Road

Using APs for packet capture does not require a separate overlay network for monitoring, significantly reducing the overall capital expenditure for WLAN monitoring and analysis. When done correctly, it provides the most cost-effective and flexible remote WLAN analysis system. Here are some WLAN design factors that should be considered for AP-based remote packet capture:

- **Additional AP coverage**
  When using APs as packet capture devices, the wireless network must have sufficient AP overlap. Typically, overlapping coverage is already a part of any well-designed WLAN deployment. This allows WLAN clients to maintain adequate data rates and performance, even when roaming. Since remote AP packet capture could take certain APs offline while in sniffer mode, additional overlap should be factored into the design to compensate for one or more APs being unavailable for client access.

- **Dedicated APs for packet capture**
  It's a good idea to designate certain APs as sniffer-only devices so that they are dedicated to data capture 24/7. This simplifies the AP coverage design since this approach will eliminate the need to take APs offline. This is especially important for wireless forensics, which is used to continuously capture, store, and analyze data. Forensics is well suited for high-throughput networks, or WLAN analysis systems that are capturing packets from a large number of APs simultaneously. It provides a complete recording of all WLAN traffic; so any and all problems are captured and recorded as they happen. This eliminates the time consuming task of reproducing complex, intermittent problems that are common with wireless networks. Network forensics also provides a complete history of WLAN activity for transaction verification in mission-critical deployments, such as financial applications.

- **Not every problem on the WLAN is a wireless problem**
  Wired analysis must be part of the total monitoring and troubleshooting solution. Problems are just as likely to occur on the wired side of the connection, especially for authentication issues when using WPA2 Enterprise, or for application-layer issues. Using a single solution that can perform both wired and wireless analysis enables seamless comparisons of traffic from both sides of the AP, and reduces the learning curve for network analysts.

- **Portable analysis isn’t dead - but know the limitations**
  Using a portable device for WLAN analysis and troubleshooting is definitely still a viable option, however users need to be very aware of the limitations. As discussed above, capturing 802.11ac data with USB WLAN adapters will not always provide adequate results. Most USB WLAN adapters are limited to 2-stream 802.11ac operation (867 Mbps), so any traffic that exceeds this data rate will simply be invisible to an analysis session. This approach is still feasible in cases where the analysis is limited just to clients that operate under 867 Mbps. However if the problem being investigated is not well characterized, you will need to see all of the WLAN traffic, and a USB based solution will not meet your needs.
• WLAN analysis software must be powerful

Don’t forget that the demands on WLAN analysis software are also much greater with 802.11ac. Many WLAN analysis systems were originally designed to handle 802.11b/g data rates – nothing in excess of 54Mbps. Processing packets in real time at 1.3 Gbps or greater is a much different story. Be sure that your WLAN network analysis software meets the demands of multi-gigabit real-time packet processing. Systems that are designed for both wired and wireless analysis are much more likely to be capable of meeting these demands.

WildPackets Solutions for 802.11ac

WildPackets has a long history of being first to market with industry leading WLAN analysis and troubleshooting, supporting the new 802.11 standards. Consequently, it is not surprising we are ready for 802.11ac today.

802.11ac Solution Specifics

The WildPackets OmniPeek Network Analyzer gives network engineers real-time visibility and analysis into every part of the wired and wireless network from a single interface. WildPackets solution uniquely enables the capability to capture and analyze 802.11ac WLAN traffic with the most flexible deployment options. The OmniPeek platform provides 802.11ac data capture directly from supported APs and USB adapters.

The OmniPeek Wi-Fi analyzer solution has been updated to include the ability to decode, analyze, and display all new 802.11ac elements. This includes reporting of MCS (Modulation Coding Scheme) values for each packet, the number of spatial streams, and the bandwidth used for each packet transmission. OmniPeek supports capture and analysis for all new 802.11ac bandwidths, while enabling users to simultaneously analyze multiple channels so every bit of data is captured regardless of the number of channels deployed.

We leverage strong partnerships with leading WLAN vendors such as Cisco, Aruba, Meru Networks, Aerohive, and Ruckus Wireless, to ensure that WLAN traffic can be reliably captured for detailed analysis. OmniPeek also includes new 802.11ac custom remote adapters supporting Cisco, Aruba, and Meru; with more to come as AP vendors release 802.11ac access points. Each vendor solution is tested in our labs, to provide integration compatibility and operational assurance. In addition, OmniPeek expands built-in RemotePcap support, as new APs are identified and tested. For a current listing of supported APs: http://www.wildpackets.com/wireless/wireless_partners

WildPackets WLAN Analysis Solution Advantages:

The WildPackets OmniPeek Solution is the first to support data capture and analysis of 802.11ac traffic delivering significant system value:

- Exclusive support for:
  - Data capture via inexpensive, commercially available devices
  - Remote data capture that’s leverages the current network of deployed enterprise APs
  - Improved productivity with packet capture that can be performed by non-technical users
• Comprehensive voice-over-wireless (VoFi) analysis
• Optimal support for distributed networks with remote 24x7 real-time analysis
• Effortless and comprehensive troubleshooting with the industry-leading user interface
• A cost-effective solution that supports simultaneous wireless and wired network analysis
• Investment protection you can count on with WildPackets' history of early support for new 802.11 standards and vendor hardware

Summary and Conclusion

Wireless LANs have become pervasive and mission critical in enterprise organizations, large and small. The sheer performance and capacity of 802.11ac will continue this trend as it approaches Ethernet speeds. This, in combination with the exponential growth of smart phones, hybrids, and tablets accelerates the need for network reliability and uptime. In addition, 802.11ac introduces new challenges in WLAN analysis and troubleshooting. Network analysis solutions, such as WildPackets' OmniPeek, cost effectively address these challenges, while continuing to protect your network investments.

More Resources About 802.11ac Network Analysis

You'll find white papers, case study, videos, and other resources about Monitoring and Troubleshooting 802.11ac Networks here: http://www.wildpackets.com/wireless/wireless

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 market sectors. Customers include Boeing, Chrysler, Motorola, Nationwide, and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP).

To learn more about WildPackets solutions, please visit www.wildpackets.com, or contact WildPackets Sales: sales@wildpackets.com or (925) 937-3200