Network World and Robin Layland present

The 2014 Wi-Fi Challenge

Guide to Understanding and Choosing a Wi-Fi Solution for Today's Mobile Worlds

2014

What It Takes for Wi-Fi to Conquer the Mobile Revolution

Key Issues to Consider

Robin Layland
Principal Analyst
Layland Consulting

We are in the midst of a mobile revolution. People are carrying multiple mobile devices. Initially, we started making calls, surfing the web and receiving texts and emails. Now, the revolution is being driven into overdrive by apps. Apps allow us to do an even wider range of tasks, consuming significantly more bandwidth as they send and receive larger amounts of data. All this creates more demand on the Wi-Fi network.

Added to the mix is the Internet of Everything. Increasingly, equipment comes with Wi-Fi. Devices in your house and office generate traffic on their status. Hospital devices and equipment send their results directly to the nurse or doctor. If anyone needs to locate the equipment, it self-reports where it is and if it is busy. All this information sharing generates traffic over the network and increases the number of connections.

The revolution goes beyond just creating more traffic. It also includes what enterprises can learn from mobile devices. Businesses can gain an understanding of what their employees, visitors and customers are doing. For example, tracking mobile devices allows a stadium to understand the flow of people looking for a concession stand. Such knowledge enables stadium personnel to reengineer signs and flows if too many people turn in one direction and cause a backup at the concession stand. They can even send messages telling you which direction is best and how long the wait is. This new understanding of behavior, combined with mobility-provided big data analytics, has opened up new business possibilities and improved user experiences.

What this all means is more data and connections with the expectation of high reliability and good service. If the flow of data from Wi-Fi enabled devices is slow, productivity and customer experience suffers. It also means a network need to be designed for more than just moving data; it also needs to be design to capture location information and data for analytics too.

Wi-Fi is the critical infrastructure in today's networks. What does a solution need to meet the challenges of today's mobile world? Here are just some of the factors you should consider when selecting the right Wi-Fi solution:

Right Architecture: With all the data and connections created by the mobile revolution, you need the right wireless architecture. The critical issue is where the intelligence and decisions on forward traffic and the route are made. The debate revolves around whether you are using a controller or controller-less solution. The controller approach has the intelligence located in servers or in the cloud. The controller-less solution places the intelligence in the Access Point. As in any debate, there are two sides, and each has advantages and disadvantages. The key is to understand what the vendor is saying and why they have taken that position.

Management: A global understanding of what is happening is critical. A solution needs to provide an intuitive view of the network and quickly allow you to troubleshoot any problems. Other issues include how it integrates with your existing management solution and whether the

Wi-Fi vendor provides a solution that can cover other parts of your network. Another factor to consider is where does the management reside? On your equipment? Or does the vendor provide a Cloud solution? Management is a personalized issue; there is no right solution for everyone, so it's best to listen to the vendor's case and try it out.

Scalability: As Wi-Fi traffic grows the number of Access Points or radios increases. Ask the vendor how they scale their solution. Get them to explain how they provide a high-density design and what it takes to grow those locations. Vendors have different solutions for building a high-density network from adding Access Points to increasing the number of radios per Access Point. They may use spectrum optimization techniques and have different ways to manage RF interference. Additionally, new features such as beamforming, a method of focusing RF energy directly toward clients to increase signal strength, may be used. Have the vendor explain how it solves the high-density design problem and how its solution can lessen the need to change your current site design.

.
Deployment: With the explosion of mobile devices and the Internet of Everything, there is a good chance the network you put in today will need to grow or be adjusted. It is important that a solution is easy and fast to deploy and cost effective. Understand what it takes to add new Access Points and locations or increase the capacity of existing Access Points. Ask about what it takes, not just at headquarters, but at remote locations with no technical support. The goal should be plug-and-play so you don't have to send staff out to the location.

BYOD: Increasingly, companies are allowing employees to Bring Your Own Device (BYOD). BYOD presents unique challenges. You want to make it easy for an employee to connect and access the resources they need, but not make it so easy that your security can be breached. Does the vendor have a good solution for on-boarding and registering devices that is easy to use? Can it monitor the device? Do management, quality of service (QoS) and security solutions have the ability to differentiate between a user's personal device and work device and traffic?

Internet of Everything: The Internet of Everything (IoE) is just a more complicated version of BYOD. With BYOD, an employee is able to deal with some complexity. With IoE you need to address many of the same concerns as with BYOD, but with limited intelligence on the other end. Understand how the vendor can protect your network, and make it so that Wi-Fi enabled equipment can easily connect without needing a lot of handholding from IT.

Location-Based Services: Location-based services have the potential to increase sales, lead to a better customer and employee experience and provide valuable information on what is happening. All Access Points have the potential to provide location data. That does not make them all equal. First, it's important to understand how much accuracy you need. Better accuracy comes with a cost, such as requiring more Access Points and radios. It may also require a solution that has Bluetooth and other short-range wireless technology built-in. Have the vendor explain how they handle location-based services and provide analytics to understand the data. It is best to do this in the context of your business. Also understand that a network layout may be great for handling your traffic load, but not good at determining locations. For example, having all the Access Points in a straight line results in poor accuracy, but could handle all your traffic needs. Have the vendor explain what is the best design mix for your situation.

Access Points: Access Points are built using many different chips and parts. The truth is that some of the chips and parts are the same or come from a small number of suppliers. This does not mean all Access Points are the same. Each enterprise-grade vendor adds its own special chips and parts to the mix. This customization could increase security, enhance throughput or

provide better analytics, management or location-based services. It is important to understand how such differentiation helps you or if it even matters.

802.11ac: 802.11ac is a reality, but unlike the past version of Wi-Fi, AC is designed to evolve. The first phase of AC does not have all the planned features. This is not a vendor failing, but part of the AC plan. When you select a solution, you need to understand if future features are important. If they are, you need to have the vendor explain how they will evolve their solutions and your installed base of Access Points.

Security: I have security last on this list, but it is really one of the most important issues. Having good security is a critical part of any BYOD and IoE solution. Security is best with a layered approach. Have the vendor explain how they provide important security functions such as firewalling, access control, IPS and authentication. Understand how each element fits into your overall security framework. Solutions need to reflect an understanding of the various types of traffic generated by apps and applications, even sub-applications within a large application such as Facebook. You may want to have different QoS, security and bandwidth usage for each. Just because you can differentiate doesn't mean you should. There is a cost in both time and management, plus it puts a burden on the equipment. Ask yourself if you need to apply policies at a granular level, and then ask the vendor how their solution meets your needs.

My Challenge to the Industry

The 2014 Wi-Fi Challenge serves as a kind of "cheat sheet" you can use to understand what the respective vendors are focusing on and get an idea of their strengths. It will help you learn specifically what the leading enterprise-class vendors are doing to meet the challenges of BYOD, IoE, security and the mobile revolution.

I have challenged them to articulate to you, within the following pages, the specific value propositions that make them the right company for you. Instead of asking them to address all the issues mentioned in this article, I requested that they concentrate on where they excel and stand out in the industry compared with their competition. Don't assume just because they didn't address an issue that they don't have a good solution. If they say something that interests you, call them in and ask them to address all your issues.

This document is just one part of The 2014 Wi-Fi Challenge. There are additional papers on Wi-FI and three webcasts focusing on:
- The why and how of location-based services
- The impact of the Internet of Everything on your Wi-Fi network
- Is a cloud-based Wi-Fi solution right for your enterprise?

You can find the webcast and additional resources by going to the Network World site, selecting the "Resources / White Paper" tab at the top of the page, and then selecting the "Solution Center" category under the "Resource Type" pull-down, or by clicking on this **link**.

Scale Beyond The Crowd

IdentiFi Wireless From Extreme

Mike Leibovitz
Director of Mobility and Applications
Extreme Networks

As time proceeds, the universal challenge of scale continues to get bigger. Each day more users, devices and applications are consuming more bandwidth no matter the type of business you are in. Just a few years ago the main consideration for Wi-Fi deployment was providing basic connectivity. This has changed with the advent of smartphones, tablets, BYOD and mobile life; soon enough the Internet of Things (IoT) will proliferate even more Wi-Fi consuming devices onto your network. Growth in mobile device use is explosive, along with growth in the expectation of people using your network. It is therefore more critical, now, than ever before to consider the future of your Wi-Fi network and how it will scale.

The solution for scale is not appropriately addressed by throwing more Access Points (APs) into an environment. Often overlooked, the single biggest source of interference found in most Wi-Fi networks today is the Wi-Fi network itself. That's right. Too many APs will likely result in self-created interference. This scenario is as bad as it gets as there's no way to solve it other than powering down, or turning off APs you've paid for. Few can afford making this costly mistake.

Designing a network for scale demands much more than just randomly deploying a few APs on the ceiling.

Let's investigate the critical elements delivered by IdentiFi Wireless from Extreme Networks that delivers the scale your future requires.

Purpose Built Access Points
Not all Wi-Fi solutions are created equal. IdentiFi access points are purpose-built to meet the need of scale while supplying the security, reliability, and availability you've come to expect from enterprise grade Wi-Fi. IdentiFi AP radios, CPU, memory and antennas have been designed to operate at full power, run cooler and provide the cleanest signal of any access point available today.

Extreme Networks has taken great care to minimize potential performance bottlenecks as described below:

- 802.11ac on 802.3af PoE: All of the performance you need, full 3x3:3 802.11ac gigabit Wi-Fi at an industry leading 802.3af power budget running at less than 12watts!
- Radio: State of the art radio chipsets providing reliable and high performance RF using: Dynamic Radio Management to optimize channel and power plans, Flexible Client Access ensuring optimal airtime use in a mixed mode wireless client environments, Band Steering ensuring dual band clients use the high capacity and less interference prone 5GHz band, and Spectrum analysis with avoidance to identify and address RF interference issues.
- CPU: We utilize an energy efficient and powerful dual core CPU to ensure extremely fast processing of data packets. Additionally, we take advantage of a dedicated network processor

(NPU) to offload frame processing to the hardware boosting packet-processing performance by up to 25%. In addition, we also support hardware-based encryption to maximize our backplane capacity for end-to-end encryption.

- Wired side of the AP: We have designed the software and hardware to support 1.75Gbps overall throughput with Ethernet port processing of 75,000 packets per second of performance with mixed packet sizes. Finally, IdentiFi supports dual Ethernet port for link aggregation and redundancy for added wired capacity and service continuity during wired-link failures.
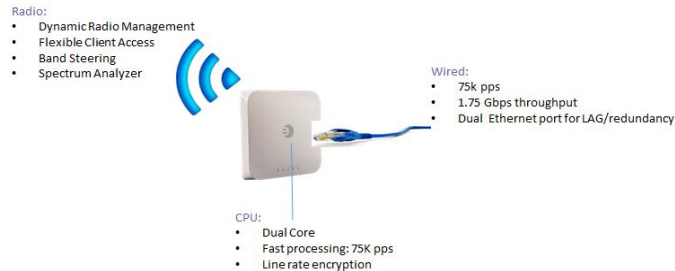
Flexible WLAN Architecture

A flexible and adaptable architecture is a key element to provide the scale you will need tomorrow. You simply cannot afford to be locked-into a single WLAN architecture – Wireless LAN is not one size fit all – It must offer the agility to adjust to your requirements in the future. The IdentiFi architectural approach improves overall wireless network performance, reducing the management complexities associated with multiple SSIDs and provides a cleaner RF environment all leading to greater scale.

Extreme Networks IdentiFi Adapt architecture offers three key benefits when designing Wi-Fi networks for scale:

- Simultaneously support for centralized and distributed traffic forwarding architectures within a single SSID based on user-role, device type, application, and location.
- Contains multicast traffic independent of SSID or VLAN infrastructure including noisy protocols such as Bonjour in an easy way while eliminating the bottleneck "gateways" approach.
- Integrates 3rd Party Applications through Extreme Networks SDN solution that provides limitless integrations including Mobile Device Management (MDM), firewall, virtual hypervisor, unified communications, and more.

Context Based Access Controls

Contextual based access control is a critical element required for your growing network needs. In order to scale, your network must adapt and be programmable with a single click. Onboarding new users, new devices and applications are found in most current BYOD solutions. Tomorrow's world will require a new framework for BYOD to support "browser-less" IoT devices inclusive of passive onboarding and provisioning solutions. Extreme Networks Mobile IAM™ is specifically designed for the need; don't assume that every other onboarding solution will meet the need as not all solutions are built with your tomorrow in mind.

Working in concert with Extreme's onboarding process, IdentiFi™ Wireless provisions contextual role-based policies at the AP. These policies provide security, QoS priority, rate limiting, and traffic forwarding modes that are implemented based on the user's context (who you are, where you are, what device and application is being used). Each policy provides very granular control over what each user has access to. The policy is not tied to a VLAN; it is associated with the context of that user and will follow that user as they roam throughout your network. Extreme's onboarding and provisioning framework provides

guaranteed application delivery while supplying excellent Quality of Experience for every user on your network.

Unified Management and Analytic Measurements

Automation, orchestration and provisioning are key elements driving your network to scale in the future. As demand continues to grow, a centralized management and analytics solution encompassing your entire wired and wireless infrastructure becomes mandatory. It is the only way to assure excellent experiences are being delivered to all users, all of the time.

Extreme Networks
NetSight™ unifies wired and wireless network management capabilities under one web-based control interface. This powerful and intuitive tool enables both managers and technical staff to be more efficient in their monitoring, reporting, analysis, troubleshooting and problem solving tasks.

Extreme Network Purview™ is a network powered application analytics and network optimization solution that captures and analyzes context-based application traffic that delivers meaningful intelligence.

Network powered analytics is an essential requirement to answer a simple question: "How can you measure the experience of each individual user on your network?" As your network scales and grows this question becomes more difficult to answer. In the end delivering user experience remains the reason you deployed a Wi-Fi network in the first place! You must be able to measure success.

The Sum Of The Parts

Extreme Networks is the only proven stadium class Wi-Fi solution on the market. Solving connectivity for 70,000 NFL fans is no simple feat – it requires a complete end-to-end approach. The IdentiFi Wireless, and Extreme Networks product line is offered and delivered to customers in every business type and every vertical. Our customers find success one AP at a time and are not forced to add more APs to scale their network. When you combine all things Extreme Networks does right you reveal a solution that scales beyond the crowd.

For more information about Extreme Networks IdentiFi Wireless solutions described here, please visit www.extremenetworks.com