TOP 5 ROLES OF WI-FI FOR THE ENTERPRISE

In the early days of Wi-Fi, organizations relied on wireless technology primarily for basic connectivity and email. But as the volume of wireless devices connected to enterprise networks has increased and the workforce has grown increasingly mobile, things have changed significantly. Many existing Wi-Fi networks were not designed to accommodate the rapid increase in connected devices, nor were they up to the task of supporting the types of robust applications being used on today's mobile devices. To meet this challenge head-on, many enterprises are seeking to evolve their Wi-Fi networks for the modern age.

The mobile era has brought about new architectures, advanced access point technologies and simpler management tools that are drastically improving Wi-Fi reliability and performance. Now is the time for enterprises to rethink wireless networking and the significant role it plays in today's expanding mobile enterprise. Let's take a look at the five new roles Wi-Fi can play in the enterprise as it goes beyond the basics to support even the most strategic applications and business objectives.

1. SUPPORTING PERFORMANCE-INTENSIVE APPLICATIONS

Users need significant bandwidth for enterprise applications such as video conferencing, large file sharing and video streaming. Since bandwidth is not unlimited on Wi-Fi networks, quality of service becomes critical. Businesses need the ability to prioritize traffic on the network based on a variety of factors. For example, priorities may be assigned by user type (employees vs. guests), application (enterprise resource planning vs. collaboration platforms) or device type (smartphones vs. medical devices). Advances in software offer enterprises that level of control so they can prioritize access based on business need and available bandwidth, and easily adjust as needed. Similar innovations in software help optimize the performance of each access point to ensure seamless Wi-Fi coverage.

The mobile era has brought about new architectures, advanced access point technologies and simpler management tools that are drastically improving Wi-Fi reliability and performance.

Certain software designed for Wi-Fi networks also enables analysis of user patterns and performance requirements so businesses can tailor their Wi-Fi networks to deliver the appropriate level of bandwidth to their most critical and data-intensive applications. For example, enterprises can better determine if they need to increase the number of access points to accommodate more users, or switch to the

5 GHz band (IEEE 802.11ac) from the more common (and crowded) 2.4 GHz band to free up bandwidth.

With improved reliability and control of Wi-Fi networks, employees need not be restricted to the wired network when using performance-intensive applications. This untethered freedom can drive operational excellence and increase productivity as employees can do more than ever before, whenever needed, wherever they are.

2. EMPOWERING A MOBILE FIRST WORKFORCE

The old way of making the network available—wired connections for PCs in offices and Wi-Fi only in conference rooms or public spaces, for example—doesn't cut it anymore. Wi-Fi is now the "go to" network for employees no matter where they are, and they expect to have access to the same information, applications and resources with the same performance and reliability as they would when plugged in. By leveraging the advances brought about by the latest standards and protocols, enterprises can give their employees the freedom and flexibility they demand.

In addition, advances in wireless management tools bring better visibility into the network for the IT team. With this insight, IT can make informed decisions in real time, creating an adaptable network that can keep up with today's dynamic business. For example, adaptive radio management enables access points to put out a stronger signal if/when a nearby access point has failed to temporarily fill in the gap in coverage while the access point issue is resolved. Enhanced visibility can also come from integrating wireless management tools with applications like Microsoft Skype, which can leverage specific information about the Skype calls, such as audio or video quality, to see correlations between problem devices, access points and coverage areas.

With the enhanced insight, the Wi-Fi network is able to deliver the speed, quality and reliability needed for a positive end-user experience. As such, enterprises are able to build an environment that fosters increased productivity for mobile workers.

3. EMBRACING IOT

The Internet of Things (IoT) is having a profound effect on the demands and expectations of wireless networks. Businesses are connecting more IoT devices to the network than ever before, such as sensors for lighting and energy management, cameras for security and environmental controls for heating and air conditioning. As innovation spawns more and more connected things, businesses require a robust and reliable Wi-Fi solution to ensure everything that is connected to the network is performing as needed. With the explosion of IoT, the role of the access point becomes crucial in order to deliver the scale and seamlessness these devices require.

Enterprises must have the right technology in place for IoT devices to communicate securely and efficiently. For example, a wireless sensor must be configured properly to ensure it can be identified and connected to the best access point to achieve optimal performance. A mobile device management (MDM) platform may be required to authenticate the sensor to maintain adequate security levels. And an access point controller may be responsible to prevent IoT congestion from interfering with business-critical application traffic.

More connected devices means more opportunity to create safer, more comfortable and eco-friendly environments. However, without the right technology and expertise, adding IoT sensors into the Wi-Fi mix has the potential to disrupt important business operations.

4. LEVERAGING ANALYTICS

Aside from the employee flexibility and productivity benefits that Wi-Fi has come to offer, it has also become a mechanism in which enterprises gather data and information to gain actionable insights across the business. The data on device types, user groups and applications offers intelligence that creates opportunities to improve practices, tailor customer experiences and capitalize on new trends. For example, a business can use location-based data to promote a sale or offer a coupon to nearby consumers. Alternatively, a grocery store may offer an in-store shopper an app that keeps a running total of the items placed in his or her shopping cart.

But as with any opportunity, there comes a challenge. While the Wi-Fi network is gathering volumes of data, it is not all going to be valuable. The challenge becomes filtering, aggregating and analyzing the information so that it can be valuable and ultimately actionable. Fortunately, as Wi-Fi technology has improved over the years, so, too have the tools that can analyze the data traversing the networks. Many of the solutions on the market today offer simple reports and even visual dashboards so decision makers can have a snapshot of the data that matters.

5. REIMAGINING SECURITY

While Wi-Fi in the enterprise can bring about significant advantages, it doesn't come without risk. By enabling an ecosystem of wirelessly connected devices that access business-critical information, it expands the threat surface for enterprises. The perimeter now extends beyond the office building and beyond the edge of the traditional wired network. In itself, the Wi-Fi network is actually part of the security solution because it authorizes access to the network and governs which users can access information and resources. But it is also part of the problem.

Looking at the risk/reward ratio, the benefits of Wi-Fi far outweigh the risks it poses to enterprise security. That is due in large part to the emergence of authentication and network access control (NAC) technology. NAC enables businesses to take three key steps to build a secure network:

1. **Identify devices.** Retaining information on the number of devices and types, connections to and from, and operating systems used provides the foundation of visibility. Continuous insight into the enterprise-wide device landscape and potential device security corruption, as well as which elements come and go, gives you the visibility required over time.
2. **Enforce security policies.** Implement policies that provide proper user and device access, regardless of user, device type or location. This provides an expected user experience. Organizations must adapt to today's evolving devices and their use—whether the device is a smartphone, surveillance camera, tablet, mobile scanner, etc.
3. **Protect resources.** Dynamic policy controls and real-time threat remediation that extends to third-party systems is the third piece to the puzzle. Organizations must plan for existing and unforeseen challenges. Being prepared for unusual network behavior at 3 AM requires a unified approach that can block traffic and change the status of a device's connection. And it's not realistic to rely on IT and help desk staff to manually intervene whenever a user decides to work remotely or buy a new smartphone. Network access control is no longer just for performing assessments on known devices before access.

The trick is finding the ideal mix of capabilities and security levels that best suits a given situation and business need. Some key considerations that effect which security solutions to implement include:

- Federal and state and regulations
- Industry-specific compliance obligations
- The use of personally identifiable information (PII)
- Campus and remote office locations

These and other factors are critical to the evaluation, selection and implementation of the right NAC technologies.

THE BIG PICTURE

The time has come for Wi-Fi to elevate its value in the enterprise. As its role expands beyond basic connectivity and evolves to include critical implications for productivity, security and analytics, new requirements are placed on the Wi-Fi network. Fortunately, new technologies are emerging to help.

The emergence of robust access points, advanced management tools, intelligent analytical platforms, and network access control solutions is giving Wi-Fi a much needed boost as a business-critical platform.

If you're looking to upgrade your Wi-Fi network to meet today's mobile demands, or have recently embarked on an upgrade project but you're still not getting the type of performance or scalability you expected, now is the time to reevaluate. Let the WEI team assist you in analyzing your wireless networking strategy to achieve optimal performance, and power your enterprise forward.

TALK TO WEI TODAY

How is your wireless network performing? Is it time for a network refresh? Contact WEI for a wireless networking assessment today.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.