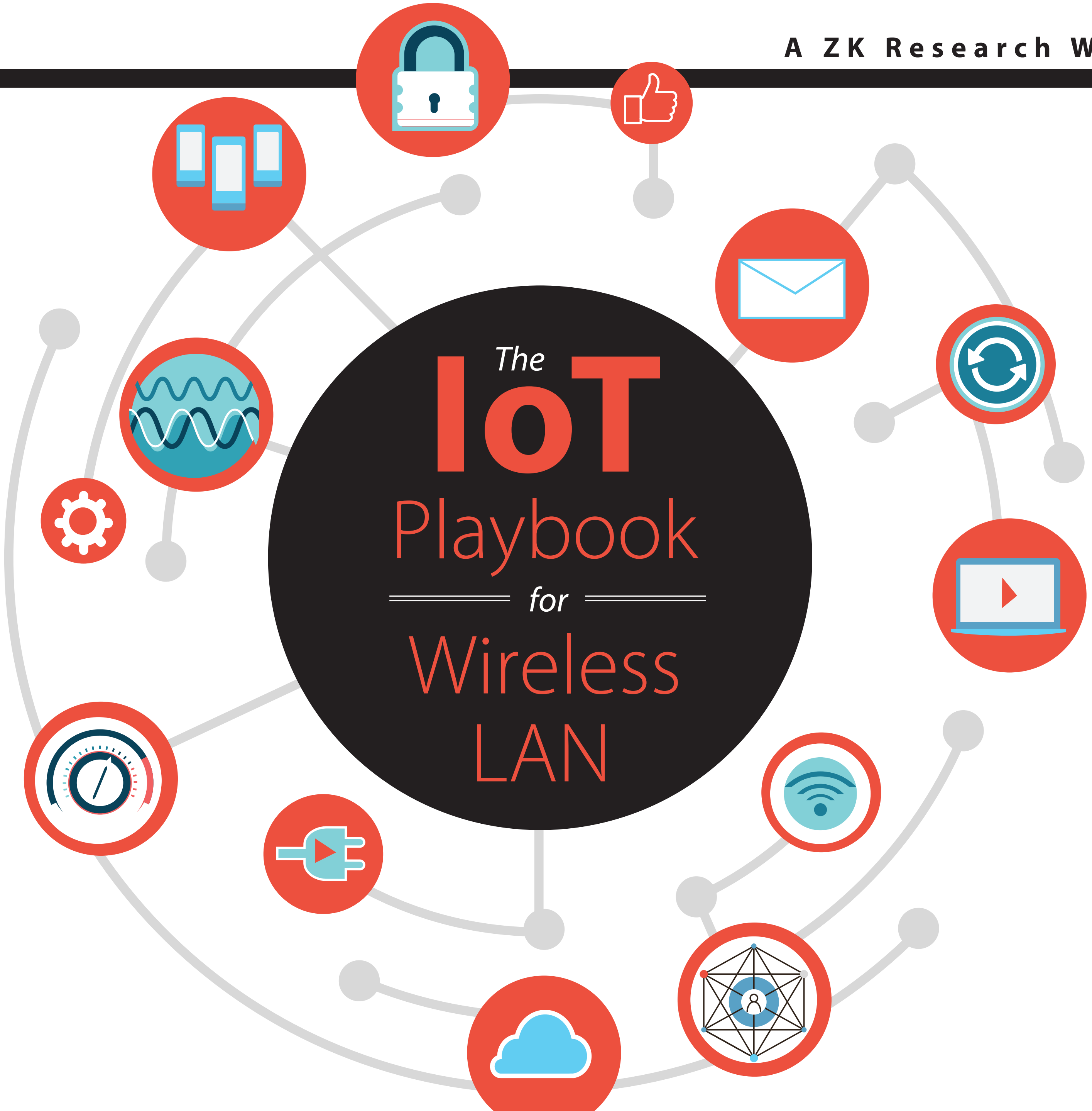
謀
RESEARCH

A ZK Research Whitepaper

November 2015

The IoT Playbook for Wireless LAN



Introduction: The Era of the Internet of Things Has Arrived

The phrase "perfect storm" is used to describe a situation where a number of large forces come together to create a singular, massive force. The technology industry had its own perfect storm in the early 1990s, when several trends converged to create the most significant change of our lifetime.

Low-cost PCs, the evolution of the browser, graphical user interfaces, home broadband and massive network buildouts gave birth to the Internet era. This perfect storm was so powerful that it created an entirely new economic model. Organizations that quickly found a way to capitalize on the Internet found themselves in an industry leadership position, while the rest struggled—and many of them did not survive. The Internet has forever changed the way we work, entertain ourselves and educate.

Today, the world sits on the precipice of another perfect storm—the coming of age of the Internet of Things (IoT)—as billions of previously unconnected devices become connected to the Internet (Exhibit 1). As was the case with the Internet, there is no single driving force but rather a number of trends that have come together to enable the IoT to shift from a vision to reality. The following forces are ushering in the IoT era:

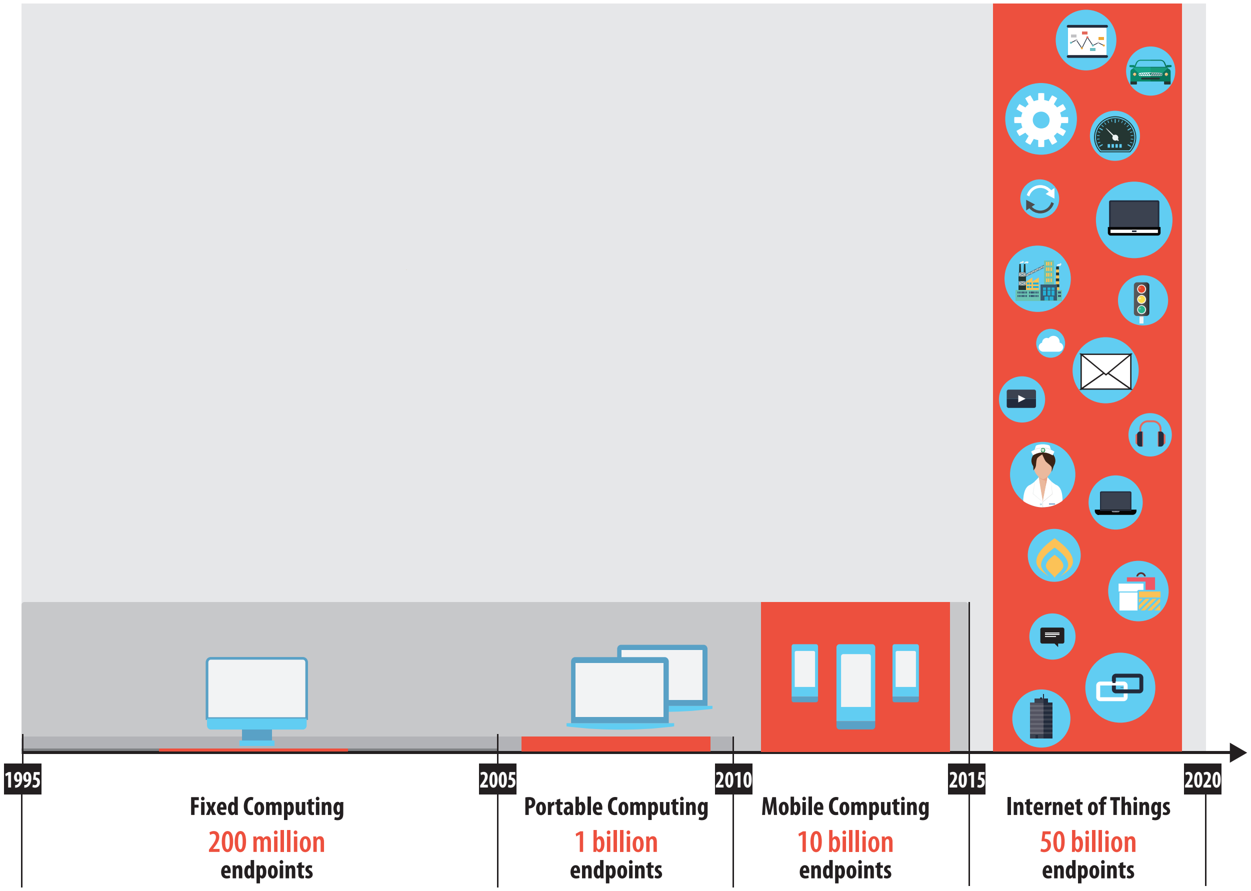
Low-cost sensors: Five years ago, the sensors that were used to connect a device to the Internet cost as much as $15 to $20. This made it cost prohibitive to network-enable most endpoints, limiting the adoption of IoT to verticals such as oil and gas and manufacturing. Today,

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice to help his clients in the current business climate as well as long-term strategic advice. He delivers research and advice to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

the cost of a sensor is as low as $1, and ZK Research predicts it will fall to less than 20 cents within five years. That price point will enable almost anything from coffee cups to wearable

Exhibit 1: More Than 50 Billion Devices Will Be Connected by 2020



Source: ZK Research, 2015

The explosion of connected devices will generate an unprecedented amount of data.

technology to airplanes to be outfitted with a sensor.

Cloud and edge computing: The explosion of connected devices will generate an unprecedented amount of data. This data needs to be analyzed quickly so businesses can move faster to better serve customers and workers or take advantage of market trends. Although much of the data will be analyzed in a centralized public or public cloud resource, it may be necessary to process the data at the edge of a network. For example, retailers may want to analyze customer data in real time to push a promotion. The growth of the cloud is well under way, and edge computing resources are starting to gain momentum—both are required for IoT to be successful.

Internet Protocol (IP) as the de facto standard: Although the concept of IoT is still fairly new, many businesses have been connecting operational technology (OT) such as medical devices and factory equipment for years. However, these machine-to-machine (M2M) connections were made with a variety of proprietary or closed protocols that did not interoperate with each other. Today, almost all IoT connections are made with IP, enabling potentially tens of billions of devices to be connected to a common network. Another important factor regarding IP is that the last version, IPv6, overcomes the addressing limitations of IPv4 by enabling an almost infinite number of devices to be assigned a unique IP address.

The maturation of big data/analytic platforms: IoT is about more than just connecting traditionally unconnected devices. Although doing so is certainly important, it only creates the foundation for IoT. For IoT to thrive, organizations must capture the massive amounts of data made available and analyze that information to make more intelligent decisions and even automate certain processes.

In addition to the above forces, another one is undergoing its own technological shift: Wireless LAN is the final missing piece of the IoT puzzle. Historically, many early adopters of IoT-connected devices such as factory equipment used proprietary wireless connectivity methods. Today, WiFi has become nearly ubiquitous, enabling almost any device to connect.

Not all WLAN solutions are equal.

However, not all WiFi solutions are created equal, and there are many factors to consider. IoT can be a killer of the WiFi network if not deployed correctly. Complicating the problem is the fact that the wireless LAN industry has been evolving rapidly over the past few years and has seen the 802.11ac Wave 1 and Wave 2 specifications come to market, leaving organizations wondering where to start. This paper investigates the changes in the WiFi market and provides advice to help deploying organizations make the right decision regarding this critical enabler of IoT.

Section II: Wireless LAN Is the Foundation for the Internet of Things

The rise of IoT will have a profound impact on the business wireless network. Historically, most organizations considered the wireless network to be an addition to the wired network. The wired network was known as the predictable, reliable and secure network, while the wireless network was used more for convenience and mobility. Users would often have to choose between connecting to the wired network for high-bandwidth or mission-critical applications and connecting to the wireless network to enjoy all the benefits of being mobile.

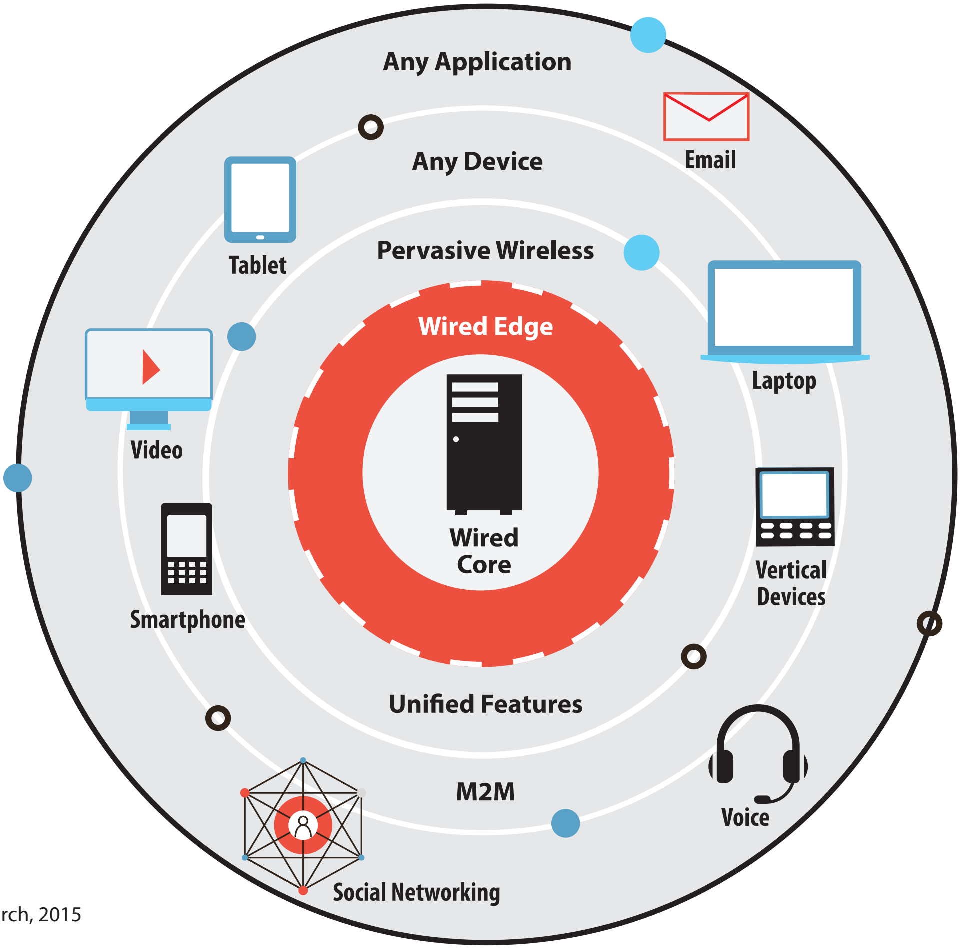
Although not ideal, this model was sufficient for more than a decade, as most organizations had well-defined processes that were augmented with mobility. Today, business processes have flipped. Many companies now think "mobile first"—meaning workers must have access to all applications on any device no matter where in the organization the employees are located (Exhibit 2). With respect to IoT, a mobile-first strategy is mandatory, as many non-traditional IT devices will be connected to the data network via a wireless connection. Examples of WiFi-enabled IoT endpoints are medical devices, manufacturing equipment, industrial infrastructure and even cargo containers.

A mobile-first strategy is mandatory.

This shift to a mobile-first strategy means the wireless network needs to perform exactly like the wired network. If it does not, at best, worker productivity will be reduced. However, in some verticals where processes are uniquely mobile, the lack of a quality wireless network can have significant consequences. Consider a hospital setting, where alarms on patient monitors are sent to a mobile device carried by clinicians. If the wireless network doesn't perform well, clinicians may be alerted to patient alarms late or not at all—putting the patients' safety at risk. Not all IoT processes are a matter of life and death, as they are in healthcare—but the more mobile and connected organizations become, the more they will rely on the WiFi network.

In addition to performance, wireless needs to offer higher and more consistent throughput to handle bandwidth-intensive or real-time applications. Also, security must be integrated into the solution to ensure regulatory requirements are being met and the data being transmitted over the wireless network is secured to protect workers and organizations. However, there are

Exhibit 2: Businesses Are Now Predominantly Mobile



Source: ZK Research, 2015

some stark differences between wireless and wired technology, including the following:

Interference challenges: Because wired connectivity is isolated to the cable, it is very rare for external forces to create interference on the data transmission. However, that isn't the case with wireless. Interference can be created by a number of sources such as the following:

> Physical barriers like metal, concrete and mirrors

> Frequency interference from microwaves, cordless phones and other access points (APs)

> Other factors including power lines and even some Bluetooth devices

Client dependency: The quality of transmission between a wireless access point and a client is dependent on both elements. Although an AP may be capable of handling certain speeds, those speeds cannot be achieved unless the client has the same speed capability. For example, 802.11ac has been referred to as "gigabit WiFi," but the devices involved in the transmission must also be 802.11ac endpoints to achieve the maximum possible speed.

Density of access points: With a wired network, a user simply needs to plug in the Ethernet cable to his or her computer, and this will generally result in a quality connection. With wireless, if a user is in motion, a quality connection could be established but the signal may degrade as the worker moves away from the AP. If the density of APs is sparse, there may be gaps in coverage. However, if there are too many APs, interference could be generated, which could also degrade the signal quality.

The challenge for IT departments is providing the same level of performance and reliability through the wireless network as workers have become accustomed to with wired connectivity. The vision for IoT calls for billions of new devices to be connected to a common network. Some devices will be connected over a wired network, but wireless connections will account for a significant portion of IoT connectivity. Based on interviews with early adopters of IoT, ZK Research estimates that at least two-thirds of IoT devices will be connected via WiFi. Businesses will only have success with IoT if the wired network and the wireless network are comparable with respect to performance, security and reliability.

ZK Research estimates that at least two-thirds of IoT devices will be connected via WiFi.

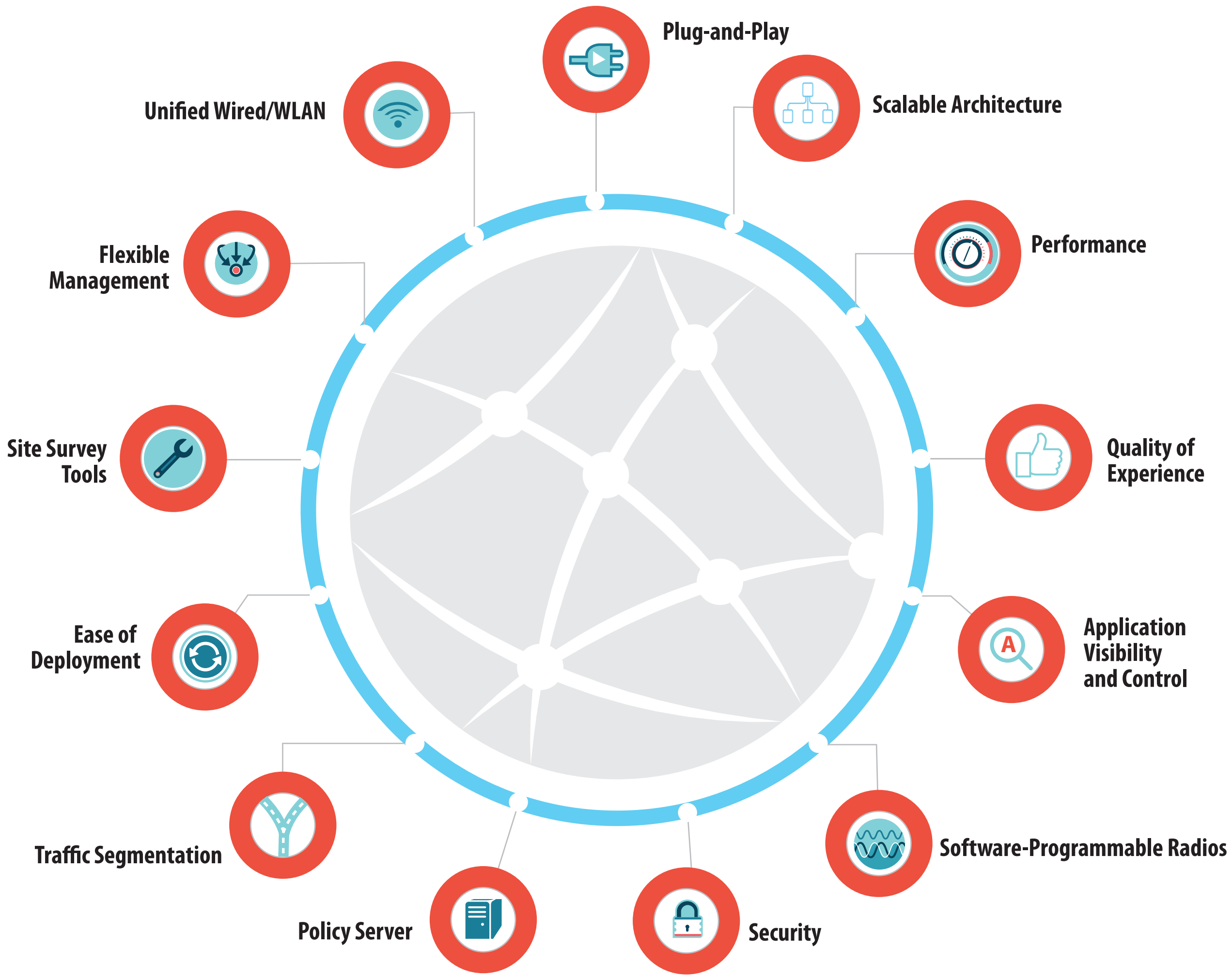
Wired networks are very consistent among manufacturers, but not all wireless solutions are created equal. Therefore, it’s important that businesses conduct their due diligence to fully understand the technical aspects of a product and ensure that the solution has all of the right built-in capabilities and fine-tuning to provide a wired-like experience on a wireless network.

Below are the key WiFi evaluation criteria for any organization looking to move forward with IoT in the next 24 months:

Plug-and-play solution: In a wired network, a device just needs to be plugged in to the port on the wall, and then a high-quality, reliable connection is established. It’s critical to have a similar experience for IoT in a wireless environment, as non-IT individuals manage many of the devices. Without a “plug-and-play” experience, the complexity level may be too high for traditional operational personnel.

Also, the WiFi network needs to enable **easy provisioning for IoT applications**. WiFi histor-

Evaluation Criteria for IoT



Source: ZK Research, 2015

ically has been used to wirelessly connect user-controlled devices such as mobile phones, tablets and laptops to the Internet. Personal computing devices have a visual display to indicate the connectivity status and some kind of application to make the process of connecting easier. Additionally, the device itself makes connecting easier by continually scanning for available networks. After selecting the network, the user enters a password, and then the connection is made.

The challenge with IoT devices is that most of them do not have a display or a signal indicator, and many don't even have a user interface. These devices need an alternate method to find a network and have a password entered, but the alternate provisioning method needs to be easy and secure. In some cases, a computer or mobile device can be used as the user interface for the IoT device. However, once the connection is established, it's important that WiFi vendors offer some kind of connectivity method for a non-IoT device.

Performance can also vary among products of the same standard.

IoT scalable architecture: A wireless network that aspires to be optimized for an IoT environment cannot be built on an archaic architecture that caters to legacy standards, speeds and device capabilities. Many wireless architectures force all traffic from APs through a central controller. This approach will not be able to scale to support thousands of IoT devices with their deluge of data traffic. An IoT-ready architecture for wireless must ensure that traffic from the APs directly transitions into the wired network and then follows the fastest and optimal path to the destination—the IoT platform or application server where immediate action can be taken. This approach can also support the concept of edge analytics, where a local agent for the analytics or

IoT platform sits at the edge of the network and processes the IoT data, makes quick inferences, takes quick action and forwards only the summarized data back to the centralized IoT platform.

Performance levels: Unlike wired networking, where every vendor's connection speeds are comparable, wireless speeds of different standards can vary greatly. For example, all Gigabit Ethernet ports on wired switches from different vendors will have performance characteristics that are similar. However, even though 802.11n and 802.11ac are industry standards, the products made available from different vendors can vary greatly in performance. This is because each standard has several release cycles, so an early version of a standard like 802.11ac may not perform as well as a later version. For example, while two vendors may both offer "ac" products, the speed of one 802.11ac solution can be markedly different from the other. Performance can also vary among products of the same standard. For example, some early-release next-generation 802.11ac Wave 2 products provide less throughput than existing 802.11ac Wave 1 products. Therefore, it's critically important that businesses conduct due diligence to test each vendor's products.

Quality of experience: Although many interference sources can degrade a user's experience, as listed above, there are things IT can do to improve the quality of experience. The solution should include radio frequency (RF) optimization capabilities to ensure a continuous, high-quality user experience. Examples of this are a dedicated radio for continuous monitoring, interference detection and adaptive configuration changes to AP settings such as wireless channels, AP output power and client connection settings.

Application visibility and control: Historically, one of WiFi's challenges is the fact that a single bandwidth-intensive application could degrade the performance of other applications for all users. It's important that IT has the tools to ensure all applications are running optimally. This starts with rich application visibility, so IT understands what's running on the network and what is consuming bandwidth. Also, the IT department needs the capability to set policies and prioritize business-critical applications such as IoT services above other "best effort" category services. Having the ability to make these changes on the fly based on business need, time of day or network location can be even more helpful to the administrator who is trying to maximize the investment from IoT services deployed over this wireless network.

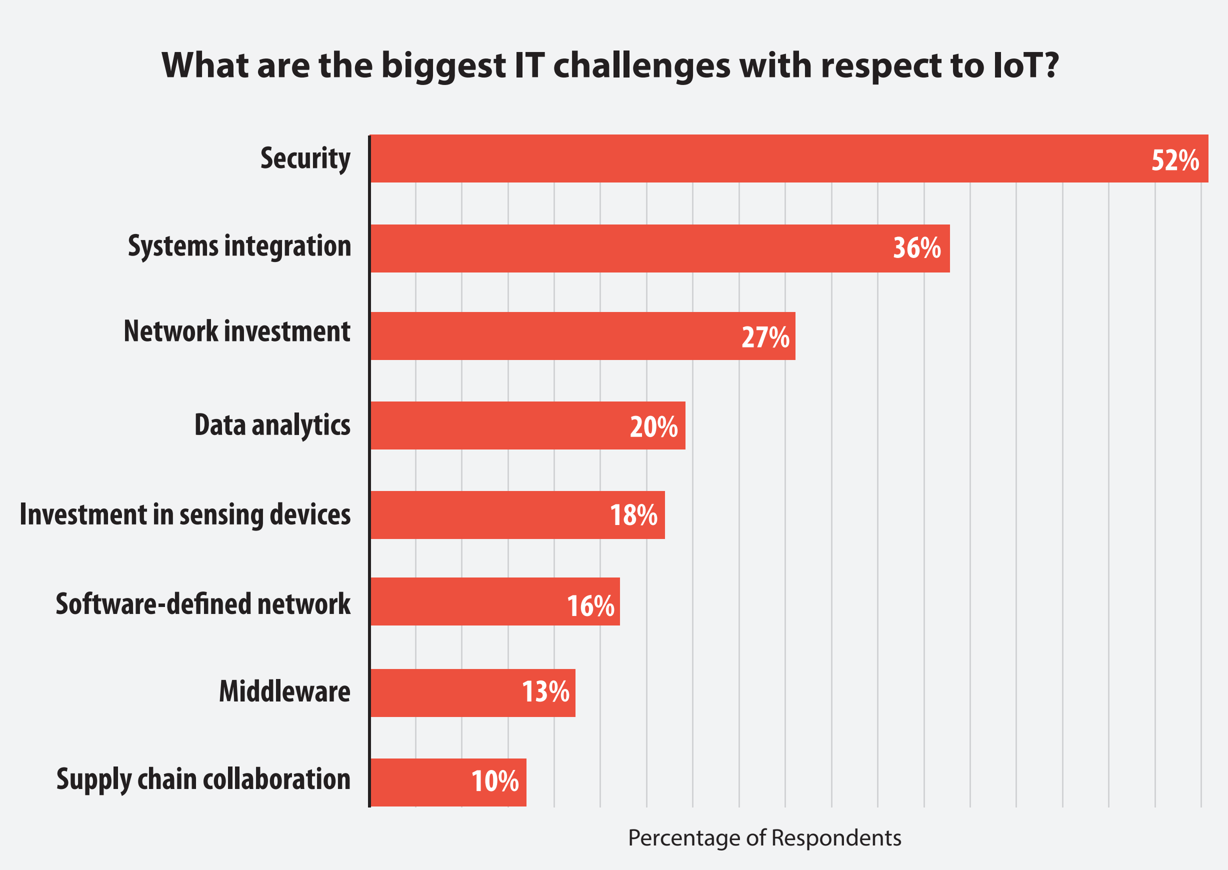
Security remains the biggest challenge to overcome with respect to IoT.

Software-programmable radios: The 802.11ac specifications for WiFi are changing rapidly, with new features and higher speeds being added with each release. Software-programmable radios ensure that the business always has the latest feature set and the best possible throughput. They also ensure that each radio in the AP is tailored to the right mix of users and their device capabilities—for example, having the ability to choose 2.4 GHz for one or more radios in a situation where IoT devices are predominantly of the legacy type. In addition, having the luxury of changing the radio type to 5 GHz as more IoT devices start supporting this higher speed would offer great flexibility to network administrators.

Secure solution: Security remains the biggest challenge to overcome with respect to IoT

(Exhibit 3). IoT is dependent on a wealth of data being collected from numerous systems, many of which contain sensitive company or customer information. Any kind of security breach could compromise the organization's customers, workers or even the business itself. This could bring

Exhibit 3: Security Is the Top Concern for the Internet of Things



Source: ZK Research 2015 Network Purchase Intention Study legal action or other costly remediation actions, which could negate any value gained from IoT. The WiFi network needs to provide the highest levels of security including encryption, intrusion detection capabilities and secure authentication capabilities, even for guest access.

Policy server: IoT requires a policy server to address the operational issues of managing every new device that joins the network. The policy server can automate IoT devices' access to the network. IoT has the potential to add an order of magnitude more connected devices to the network, making policy administration nearly impossible to manage manually.

Smart traffic segmentation: An IoT deployment is most productive when the traffic deluge from the myriad of sensors and end devices is intelligently segmented, prioritized and in some cases isolated from the rest of the enterprise network traffic. It will be most appropriate to channel time-sensitive, life-critical or bandwidth-consuming IoT sensor traffic on a separate wireless network (e.g., SSID) and divert it separately and securely to the IoT platform's location, where the data can be analyzed, useful inferences can be made and timely action can be taken.

Ease of deployment: A successful IoT deployment is dependent on traditional IT departments working with the facilities or operation technology (OT) departments within an organization. Consequently, it's possible for non-technical individuals to deploy technology infrastructure. Also, most CIOs today are focused on reducing the overhead required to run IT by simplifying the environment. Regardless of whether IT or OT is deploying and managing the wireless network, the solution needs to be simple to deploy. In addition to the plug-and-play solution previously mentioned, the solution should be field upgradable to avoid having to "rip and replace" the solution when an upgrade is required.

Site survey tools: IoT has the potential to increase the number of connected devices by an order of magnitude. Combined with technology advancements in WiFi, this means that a site survey will need to be done to optimize the placement of the APs. ZK Research actually recommends that any time new APs are deployed, a site survey should be conducted to optimize performance and minimize problems. The WiFi provider should offer a robust site survey tool to simplify this process.

Options for wireless LAN management: When it comes to managing the wireless network, many organizations will choose a traditional premises-based management solution. However, smaller enterprises or highly distributed organizations may prefer cloud-managed WiFi and leverage the ubiquity of a cloud service. Solution providers should offer both to ensure customers can use the management solution that fits their organization best.

Wired Network Considerations

Historically, the wireless network was perceived as an augmentation to the wired network, as the wired network had significantly more throughput than WiFi. The latest version of WiFi, 802.11ac, is the first standard in which wireless speeds can exceed gigabit speeds (the typical connection between the AP and the wired network). Exhibit 4 shows how WiFi speeds have increased from 2 Mbps in 1997 to 6.9 Gbps with a future release of 802.11ac Wave 2. Even though the 6.9-Gbps speed is futuristic, technologies currently are close to breaking the gigabit barrier, which would exceed the speed of current wired networks. Therefore, architecting the wired network differently needs to be a consideration.

The biggest factor to consider with the wired network is how to connect the AP to it. Most APs have a single 1-Gbps connection as a backhaul connection. However, if the speed of the

802.11ac is the first standard in which wireless speeds can exceed gigabit speeds.

Exhibit 4: The Evolution of Wireless LAN

STANDARD	DATE	FREQUENCY (GHZ)	DATA RATE
802.11	1997	2.4	2 Mbps
802.11b	1999	2.4	11 Mbps
802.11a	1999	5	54 Mbps
802.11g	2003	2.4	54 Mbps
802.11n	2009	2.4, 5	1x1 radio – 50 Mbps 2x2 radio – 300 Mbps 3x3 radio – 450 Mbps
802.11ac Wave 1	2013	5	2x2 radio – 866 Mbps 4x4 radio – 1.73 Gbps
80.211ac Wave 2	2015	5	Up to 6.9 Gbps

Source: ZK Research, 2015

wireless network is greater than 1 Gbps, the wired network will become a choke point for the wireless process. This could seriously degrade the performance of an IoT process, particularly a high-bandwidth one.

One option is to have two 1-Gbps connections on the AP bonded together to create a 2-Gbps connection. This can be impractical for some organizations, as the cost of pulling a new cable to the AP is estimated to be $300 per pull, according to ZK Research. This could cost large enterprises thousands of dollars.

Another option is the emerging NBASE-T standard (www.nbaset.org), which brings several options to the wired network. NBASE-T enables APs to connect at 1 Gbps, 2.5 Gbps or 5 Gbps using standard Category 5E copper cabling. The standard also enables the AP to connect at 10 Gbps over Category 6 cabling.

The other primary consideration with the wired network is Power over Ethernet (PoE). Most APs that have been deployed require only 15W PoE to be powered on. However, many of the 802.11ac APs require 30W PoE for power. It's crucial that businesses understand the WiFi requirements for both throughput and power and deploy the proper wired networking technology to support their mobile and IoT initiatives.

Businesses should take a unified approach to wired and wireless networks.

Lastly, businesses should take a **unified approach to wired and wireless networks**. Typically, the management, policy and security of wired and wireless networks are handled independently. This can lead to gaps in security, as the wireless network may have strict access policies but the wired network may not, or vice versa. A unified approach will ensure that the wired and wireless networks are in alignment, creating consistency with respect to network management and security.

IoT is a network-centric compute model.

Section III: Conclusion and Recommendations

The era of the Internet of Things is currently under way. The forces of cloud, social media, connected endpoints, wireless technology and big data analytics have come together to enable the biggest transformative shift in business since the birth of the Internet. Organizations should be prepared for this transition and be aware that it will happen at a rate much faster than the growth of the Internet. The winners in IoT will be organizations that understand how to weave IoT technology into the fabric of the business to compete with both traditional competitors and new market entrants. Those that cannot make the shift will likely struggle to survive. Investing in IoT must be at the top of every IT and business leader's priority list because of the speed of evolution. To help organizations get started, ZK Research makes the following recommendations:

Consider the network to be a strategic enabler of IoT. IoT is a network-centric compute model, so the network will play a significant role in the success of IoT initiatives. The network—particularly WiFi—should be considered a strategic IT resource and a platform for IoT today and into the future.

Choose a vendor that can meet IoT criteria for WiFi. When choosing a vendor, it's easy to make a decision based on vendor incumbency or market share. Although this strategy might have worked in the past, it's important to understand that the wireless network has shifted from being a best-effort network that augments the wired network to being the primary facilitator of IoT. Choose a vendor that can meet the unique requirements of IoT. ZK Research recommends that businesses evaluate at least three vendors before making a decision.

Ensure the wireless network has the highest level of security. With IoT, it's imperative that security is not compromised. CIOs must focus on ensuring that the wireless network is secured correctly, with features in the access point as well as security technologies deployed in the wired network.

For questions, comments or further information,
email *zeus@zkresearch.com*.