CDW PEOPLE WHO GET IT™

THE EVOLVING WIRELESS NETWORK

The latest wireless solutions can improve security, add management capabilities and make deployment easier.

Executive Summary

The world is going wireless, and IT organizations must make dramatic changes to meet the rapidly increasing demand for connectivity and bandwidth. Business users expect high-quality service not only for their organization-issued devices, but also for the smartphones, tablets and notebooks they bring from home under bring-your-own-device (BYOD) policies.

Desktop computers and notebooks that traditionally used wired connections now often rely on wireless connectivity, even when the user is sitting right next to an Ethernet jack. Both of these trends rapidly drive up the number of devices connecting to networks; at the same time, modern business applications demand higher bandwidth and become less tolerant of intermittent connectivity.

The combination of these trends leads to the increased importance of wireless networking. IT professionals must pay added attention to this critical service. First, IT departments must deliver a robust wireless infrastructure that has the connectivity saturation and bandwidth capacity to meet user demand. In addition to performing well, these networks must provide strong security that is suitable for transferring sensitive data. Finally, the many burdens on IT staff time necessitate wireless solutions that deploy simply and effectively with minimal manual intervention.

Table of Contents

How can an IT department provide a robust, secure and high-performing wireless network? Finding the right wireless technologies is challenging, but major vendors such as Cisco Systems, HP and Aruba Networks offer an array of solutions.

To meet the demands of technological advances and increasingly connected users, IT professionals must understand the evolution of wireless technology, including the four pillars of wireless networking, as well as the promise of the emerging 802.11ac wireless standard and the products that can deliver on this promise.

The Need for Network Evolution

Users already place tremendous demands on wireless networks, which in turn places pressure on IT staff to keep pace. Users expect anytime, anywhere access to data and applications, and these expectations can be a huge burden on aging wireless infrastructures.

Four specific trends drive this increased demand on wireless networks:

- Mobility
- Cloud computing
- Big Data
- Video

Each of these trends increases the number of users and devices that require wireless network access and increases the amount of bandwidth those devices consume.

ARIZONA CARDINALS GO WIRELESS

The Arizona Cardinals rely on a strong, resilient wireless network to support both fans and the support staff at University of Phoenix Stadium. The team recently worked with CDW to deploy a robust wireless network that will meet ever-increasing fan demand for years to come. The Cardinals deployed Cisco Connected Stadium technology, including upgraded Wi-Fi, security and unified communications services.

Football is an entertainment business, and deploying Cisco Connected Stadium technology enhances the fan experience by allowing stadium guests to access video, statistics and other information online during the game. Fans may also post to social media, sharing their experience with friends.

During the wireless rollout process, technicians worked in the stadium, using the Fluke AirCheck Wi-Fi Tester to confirm that each new access point was installed in the best location and optimally configured to support gameday activities. On gameday, the AirCheck tool provides real-time identification of rogue wireless devices, allowing stadium personnel to locate guests with interfering equipment and ask them to shut off conflicting Wi-Fi functionality.

Mobility: Today, almost all computing is mobile. Users expect to pick up their mobile devices and travel around the office or around the world without disrupting their access to applications and data. Even when sitting in their offices, many users no longer rely on wired connections, because wireless networks are simply more convenient. Wireless is now the preferred medium for network users.

Wireless technology changes quickly, and mobility increases the demand from users. While users typically replaced desktop and notebook computers on a four-year cycle, they now replace mobile devices every two years and sometimes more frequently. As these new devices gain new wireless capabilities, users expect their office networks to remain compatible. These upgraded technologies also support higher density wireless networks, allowing individual access points to serve as much as four times as many network devices as older-generation APs.

Cloud computing: While end users are untethering themselves from wired networks, organizations are also untethering themselves from physical servers and data center facilities. Cloud computing provides the enterprise with agile, flexible and scalable infrastructure and applications that reside in outside data centers. Organizations have recognized these advantages to the point that 35 percent of IT services today are delivered totally or partially via the cloud, according to a 2015 CDW report.

While cloud computing is a boon to cash-strapped server infrastructure teams, it also places increased demand on networks. As more organizations move data into the cloud, as opposed to having it reside on users' devices, IT departments are seeing an increase in demand for wireless bandwidth.

Big Data: Many Big Data solutions require robust wireless infrastructures to provide real-time services to customers and employees. For example, retail environments offer prime opportunities for Big Data analytics. Customers carrying smartphones around stores represent a prime source of data, allowing an organization insight into how customers move around the store, noticing where they linger and what they ignore.

The same technology also allows a store to provide highly customized service. For example, ULTA Beauty's The Salon deployed wireless technology to support the retailer's efforts with Big Data analytics. Now, the staff knows the identity of shoppers who participate in the company's rewards program when they walk into a store and can give them special offers. This technology requires consistent, reliable wireless access at every location.

Video: Increased use of video also drives wireless consumption. Organizations increasingly use video to meet many different requirements, ranging from training to video conferencing. Video consumes large amounts of bandwidth that today's networks simply weren't designed to handle. Supporting these uses, particularly on mobile devices, requires substantial investments in wireless infrastructure.

When designed well, these solutions offer novel experiences. For example, a mobile app deployment at the Art Institute of Chicago relies on the organization's wireless network. When a visitor walks up to a painting, the mobile app provides him or her with detailed background information and may even allow the visitor to watch a video about the artist.

Mobility, cloud computing, Big Data and video all drive increased demands on wireless networks. Organizations must evolve to meet these new demands. These needs aren't going away, and they will only increase over time as new technologies come online.

These heightened expectations for wireless access lead to new applications that lead to even greater demand. IT workers may see this as a vicious cycle, but it delivers true value to organizations that take advantage of it. Evolving an organization's wireless network allows IT staff to keep up with demand and continue satisfying user needs.

The Pillars of Wireless Networking

Designing wireless networks requires technical expertise and attention to myriad details. These complexities boil down to four pillars:

1. **Security** services ensure the safety of the infrastructure and that wireless users are protected from each other and eavesdroppers.
2. **Management** technology provides wireless network administrators with the ability to dynamically reconfigure the network to meet changing needs.
3. **Ease of deployment** is critical in ensuring an efficient, effective rollout of wireless networking that uses automation to minimize hands-on staff time.
4. **Bandwidth** requirements continue to grow at a rapid rate. Wireless networks must support the bandwidth requirements of today and tomorrow.

Each of these four pillars is a critical component of wireless network design and should play an important role in network planning.

Security

Securing wireless networks requires attention to four important details: encryption, authentication, segmentation and intrusion detection. Perhaps the most straightforward of these is protecting communications from eavesdropping through the use of wireless network encryption.

Wi-Fi Protected Access version 2 (WPA2) is the clear standard for acceptable wireless security. All modern wireless networks support this standard, and network engineers should always configure it in lieu of the Wired Equivalent Privacy standard. WEP encryption contains serious known security flaws and should be avoided at all costs.

Authentication ensures that only validated members of the trusted user community gain access to the wireless network. Organizations should turn to the 802.1X protocol for authentication needs and support that protocol with a back-end Active Directory or Lightweight Directory Access Protocol (LDAP) database.

Segmentation separates the networks used by different classes of users and devices, allowing administrators to apply different controls for different classes of users. For example, staff may gain full access to network resources while guests are limited to visiting Internet sites with no access to internal systems. Similarly, administrators may place restrictions on access for BYOD devices that do not apply to organization-owned devices.

The fourth component, intrusion detection systems (IDS) and intrusion prevention systems (IPS), ensures that rogue access points and their users quickly come to the attention of administrators. These are critical components of wireless security. Many wireless solutions are delivered with advanced IDS and IPS capabilities built in. IT administrators must determine optimal settings for these tools to maximize their security benefits.

Management

Networking teams are not growing at the same pace as the networks they manage, resulting in higher device-to-engineer ratios. Managing networks in this environment requires simple management interfaces that work across the wireless infrastructure.

For example, CDW's networking engineers experienced this firsthand when they helped build the wireless network for University of Phoenix Stadium, site of the 2015 Pro Bowl and Super Bowl for the NFL that deployed 835 access points. IT administrators could have manually monitored all of those, but that would have created a massive amount of work. Instead, they used a single management platform that gave them visibility across all the access points.

CHANGING GUEST NETWORKS

Organizations face significant security and regulatory pressure to identify all network users. Inappropriate use of networks and pressure on bandwidth consumption drives them to close off networks, limiting access to authorized users. The days of leaving wireless networks wide open are gone.

At the same time, issuing user names and passwords to guests is time-consuming. Organizations want guest networks that are both secure and easy to manage. However, they don't want IT staff spending their time issuing usernames and passwords.

Self-service portals provide the solution to this dilemma. The wireless network redirects guests to a registration site where they provide an email address or cellphone number. Before gaining access to the network, they must enter an authentication code sent to them via email or text message, validating their contact information in the event a future investigation requires contacting the user.

600

The number of wireless access points that the Kansas City Chiefs have installed at Arrowhead Stadium to provide connectivity to fans on mobile devices

SOURCE: CDW, "Kansas City Chiefs Wi-Fi Moves the Chains"

When the time came to switch Arizona's University of Phoenix Stadium over from the Pro Bowl to the Super Bowl, this management interface proved its worth. The league wanted the Super Bowl to have a different service set identifier than the Pro Bowl. To perform this switch, administrators had to change the SSID configuration on all 835 access points literally overnight. A management platform allowed them to pervasively configure the entire solution without requiring an engineer to manually work on each access point.

Ease of Deployment

Wireless network designers should also monitor the ease of deploying wireless solutions — both in rolling out new access points and in connecting clients to the existing wireless infrastructure.

Modern tools make it easy to deploy new access points in central and remote locations. Wizard-based access point configuration tools allow the connection of new APs to an existing network in seconds. It literally takes longer to hang the AP on the ceiling than it does to connect it to the network.

From a client perspective, the wireless network should allow the easy connection of new users and devices. Many IT experts advocate the use of self-service onboarding mechanisms that connect users to a generic SSID and walk them through the onboarding of their device. Such capabilities make it much more automated, simple and secure to add a new device to the network.

Bandwidth

Organizations must be able to provide high-bandwidth solutions to support the many devices that users bring to the network and the high-bandwidth applications they run. Video is a major driver of this need for bandwidth and is particularly intolerant of network issues. If the network is slow to load a web page, users often don't notice. Choppy video, on the other hand, ruins the experience entirely. How serious is this trend? Many organizations are seeing network bandwidth requirements double every two to three years.

Compounding this increased demand is the fact that manufacturers are building high-quality equipment that doesn't wear out before it becomes obsolete. Users find themselves dissatisfied with old wireless networks, but IT departments maintain the equipment because it continues to function normally.

Security, management, ease of deployment and bandwidth are critical concerns facing wireless network planners. IT workers must consider the costs and benefits of technologies supporting each of these pillars when planning new wireless network deployments and upgrading existing networks.

Bringing on 802.11ac

One of the ways networks will evolve to meet new demands is through the higher capacity technology promised by the new 802.11ac standard. Next-generation 802.11ac networks use the 5-gigahertz radio spectrum to achieve much higher performance than 802.11n networks and older standards. Users will quickly drive this adoption as they bring newer 802.11ac devices to their offices and expect them to work seamlessly with their employer's wireless network.

Organizations will see tremendous enhancements in network speed as they adopt 802.11ac networking. The new standard's speeds far surpass those of 802.11n networks. Wave 1 of 802.11ac devices, already on the market today, breaks the gigabit networking barrier, offering speeds up to 1.3 gigabits per second, almost tripling the capacity of 802.11n. As new waves of 802.11ac technology come on the market, this capacity will eventually increase to more than 6Gbps.

The performance benefits of 802.11ac also include enhancements to the use of multiple antennae on access points and endpoint devices. This technology, known as multiple-input/multiple-output (MIMO), increases the capacity of the network. While MIMO was available on 802.11n networks, the 802.11ac version brings enhancements in two areas: spatial multiplexing and multiuser access. Engineers describe MIMO networks by the number of antennae supporting data transmission and reception. For example, MIMO with three transmit and four receive antennae is called 3x4 MIMO.

With spatial multiplexing, each antenna is used to transmit and receive portions of the complete data signal. Each of these portions, known as a spatial stream, carries data proportional to the channel size. The MIMO implementation in 802.11n is limited to four spatial

IDENTIFYING AND DEFENDING AGAINST WIRELESS THREATS

Identity theft is a significant risk facing wireless network users. Many organizations want to provide customers, vendors and visitors with wireless network access, but they must guard vigilantly against a potential compromise of a customer's identity.

Experts recommend deploying wireless intrusion detection and prevention systems to protect against this risk. IDS and IPS technology watches for brute-force network login attempts and locks users out after a set number of failed logins. They also monitor the network for rogue access points that imitate a service set identifier in an attempt to steal user credentials.

streams, while 802.11ac doubles that limit to eight spatial streams. This enhancement doubles the maximum possible throughput of the network.

Older versions of MIMO allowed the use of multiple spatial streams, but required that all streams belong to the same client connection. The 802.11ac standard throws this out the window with support for multiuser MIMO (MU-MIMO). With this technology, different clients may use different antennae at the same time, increasing the ability of the access point to serve multiple users simultaneously. MU-MIMO will become available beginning with 802.11ac Wave 2 access points.

The 802.11ac standard also brings support for wireless network beamforming. In a standard Wi-Fi network, the antennae on an access point transmit their signals in an omnidirectional pattern, forming a sphere centered on the access point itself. This is highly inefficient, as the actual device communicating with the access point is in only one of those directions. Beamforming uses multiple antennae to steer the signal toward the client device. This increases the amount of the signal that reaches the client, improving the range and capacity of the wireless network. In addition to these benefits, beamforming reduces the power necessary for communication and improves the battery life of wireless clients.

The performance benefits of 802.11ac are so dramatic that organizations should move now to adopt Wave 1 technology, rather than wait for future enhancements. Some 802.11ac Wave 2 products will hit the market in 2015, with greater numbers expected by the end of 2016. The primary benefit of future 802.11ac waves will be increased bandwidth through wider channel sizes and simultaneous bonding of multiple channels. Some 802.11ac equipment, including products offered by Cisco in particular, will be field-upgradable to 802.11ac Wave 2 through the use of an expansion module.

BEST PRACTICES FOR DEPLOYING 802.11AC

Organizations preparing to roll out 802.11ac networking can take steps now to ensure their readiness for the new technology, even if they're not quite ready to deploy 802.11ac today. Three steps will help prepare for 802.11ac deployments:

- **Deploy Power over Ethernet-Plus (PoE-Plus) switches throughout the enterprise.** 802.11ac networks require significantly more power than older access points. As organizations replace switches, they should plan to deploy sufficient PoE-Plus capacity to support future 802.11ac deployments.
- **Increase wired bandwidth to support future wireless networks.** High-speed wireless networks won't do the enterprise any good unless they are backed by high-capacity Internet connections.
- **Pull two Category 6 connections to each AP location.** Full use of 802.11ac capacity will require two CAT 6 Ethernet runs to each access point. As organizations build and rewire buildings, pulling two cables can help avoid expensive rewiring projects down the road.

Implementing these best practices will reduce the time and resources required to deploy 802.11ac networks in the future.

Evaluating Wireless Vendors

One of the most important decisions an organization makes when deploying or upgrading a wireless network is selecting a network equipment provider. Three major companies compete in the wireless networking space: Cisco Systems, HP and Aruba Networks. Each of these vendors manufactures high-quality equipment and brings different strengths to the market.

Cisco Systems

Cisco, the long-standing market leader in wireless networking, is well known for manufacturing high-quality equipment that works for years beyond its expected life. Cisco has long had some of the best engineering radio technology on the market. Excellent receiver technology makes Cisco APs an excellent option to use in difficult and sensitive environments.

Close alignment between Cisco's wireless networking platform and the company's Identity Services Engine (ISE) allows policy-based network management without a high administrative burden. For example, an accountant might have access to highly sensitive information within an organization. When he brings his enterprise-issued notebook to work, he can freely access this sensitive information. However, if he tries to access this information from his personal tablet, ISE would recognize that it is not a registered device and prevent him from accessing the sensitive server while still allowing Internet access.

From an ease-of-deployment perspective, Cisco Prime Infrastructure provides templates that facilitate rolling out widespread network changes with minimal effort. Administrators may change thousands of device configurations at the same time by simply modifying a template. Cisco Prime also offers real-time monitoring and notification for administrators and provides a consistent guest network experience.

Cisco's management interface provides powerful tools that help administrators manage products in the Cisco ecosystem. Organizations that live entirely within this ecosystem benefit from strong tools allowing consistent management across Cisco devices. These tools do not, however, provide cross-platform network management for products from other manufacturers. Organizations with mixed network environments may consider a third-party network management tool or use multiple network management platforms.

Cisco's Meraki cloud-based management system provides a consistent, easy-to-manage experience for both network administrators and end users. Meraki hardware integrates seamlessly with the cloud controller software that lets network administrators quickly make adjustments without memorizing arcane commands. For example, an administrator may quickly search for policy templates governing YouTube use and adjust the priority of that traffic with a few clicks.

Organizations seeking a more traditional wireless network solution may turn to the Cisco Aironet product line with its three lines of products that promise to future-proof organizations with 802.11ac support. These include:

- The **Aironet 1700 Series**, providing 3x3 MIMO support with two spatial streams and 866 megabit-per-second capacity. The 1700 series supports 802.11ac Wave 1 technology and is best suited for small to midsize organizations.
- The **Aironet 2700 Series**, which offers higher sensitivity reception due to an additional receiver, bringing 3x4 MIMO support and adding a third spatial stream. The Aironet 2700 family can handle 1,300Mbps throughput. These devices also support 802.11ac Wave 1 out of the box and will be field-upgradable to 802.11ac Wave 2.
- The **Aironet 3700 Series**, Cisco's most advanced line of access points. This series offers 4x4 MIMO with three spatial streams and 1,300Mbps capacity. In addition to offering field upgrade support for 802.11ac Wave 2, the 3700 series accepts other upgrade modules, including Cisco Wireless Security and Cisco 3G Small Cell modules.

Each of these Cisco product lines also brings access to Cisco's world-class support and engineering network.

HP

HP positions itself in the market as a unified network service provider. Customers often look to HP for converged network solutions, which can provide switches and wireless infrastructure from the same firm. HP's networking products fit within a single management platform, providing network engineers a coherent view across the entire network from a single console.

HP's Intelligent Management Center (IMC) is the heart of this converged management approach. IMC provides a "single pane of glass" approach to monitoring, managing and configuring both wired and wireless network devices. IMC's Wireless Services Manager also offers wireless performance monitoring, radio frequency heat-mapping and reporting capabilities.

EVALUATING WIRELESS SOLUTIONS

	CISCO	ARUBA	HP
POLICY ENFORCEMENT	Identity Services Engine	ClearPass	Intelligent Management Center; User Access Manager; and User Behavior Analysis
INTRUSION DETECTION	Adaptive Wireless Intrusion Prevention System	RFProtect	Clear Connect
VENDOR-NEUTRAL MANAGEMENT PLATFORM	No	AirWave	Intelligent Management Center
CLOUD-BASED MANAGEMENT PLATFORM	Meraki	Aruba Central	HP Cloud Network Manager
802.11AC MIMO	3x3 (Aironet 1700 and 3600) 3x4 (Aironet 2700) 4x4 (Aironet 3700)	2x2 (200 Series) 3x3 (210, 220, 228 and 270 Series)	2x2 (HP 525, 527) 3x3 (HP 365, 517, 560)
5GHz TRANSFER RATE	866Mbps (Aironet 1700) 1,300Mbps (Aironet 2700, 3600 and 3700)	866Mbps (200 Series) 1,300Mbps (210, 220, 228 and 270 Series)	866Mbps (HP 525, 527) 1,300Mbps (HP 365, 517, 560)
SPATIAL STREAMS	2 (Aironet 1700) 3 (Aironet 2700, 3600 and 3700)	2 (200 Series) 3 (210, 220, 228 and 270 Series)	2 (HP 517, 525, 527) 3 (HP 365, 560)
MODULAR SUPPORT FOR 802.11AC WAVE 2	Yes (Aironet 2700 and 3700) No (Aironet 1700 and 3600)	No	No

IMC also provides outstanding security services for enterprise network administrators. The IMC User Access Manager (UAM) plug-in manages the BYOD challenge by enforcing access control policies based on the identity of both devices and users. Administrators may use UAM to govern network access for guests and personally owned devices, limiting the security risks from these types of network activity.

HP's 525 and 560 Series of 802.11ac access points also offer integrated wireless intrusion detection and prevention capability. This technology allows security administrators to quickly locate and mitigate rogue wireless access points and other security threats that arise on the wireless network. In cases where persistent interference jeopardizes the security and reliability of a wireless network, HP's Wi-Fi Clear Connect technology uses radio resource management to mitigate the interference and improve the user experience.

Small and midsized businesses may opt for a fully cloud-managed solution with HP's Cloud-Managed Networking product offering. This technology combines the HP 365 access point with HP's Cloud Network Manager to remove the need for on-premises wireless controllers by offloading much of the complexity of wireless network management to HP's cloud management platform.

Organizations deploying traditional wireless networks may turn to the other product lines offered by HP. Among the company's 802.11ac offerings:

- The **517** and **527 Series** of access points target universities, hotels and other environments with a high density of access points. These APs fit inside existing wall jacks and offer 866Mbps (for the 527) and 1,300Mbps (for the 517) capacity.
- The **525 Series** of access points is the workhorse access point in HP's lineup. These APs support 866Mbps access along with 2x2 MIMO and two spatial streams in a standard wall- or ceiling-mounted form factor.
- The **560 Series** comprises HP's premier 802.11ac access point line, offering 1,300Mbps capacity with 3x3 MIMO support and three spatial streams.

HP's product line has evolved over the years, and its acquisition of Aruba Networks in March 2015 makes it likely that this evolution will continue.

Aruba Networks

The third major player in wireless networking, Aruba Networks, focuses on providing strong functionality and ease of management across multiple hardware platforms at a cost-effective price point. Many networking shops choose Aruba technology because of its vendor-agnostic approach to network management. Aruba products support the management of mixed networks that include competitor hardware.

16%

The percentage of IT decision-makers who have plans to upgrade their wireless infrastructure in the next 12 months

SOURCE: CDW, "Surveying Your Network: A CDW Advisory Board Decision Maker Study," July 2014

Aruba differentiates itself on the security front by including an application-layer network firewall in its wireless controller line. This firewall allows the deep inspection of network traffic and the use of role-based access control policies. Aruba complements this firewall with its ClearPass Policy Manager for devices, which can accommodate both BYOD and enterprise deployments. ClearPass provides an intuitive interface for network access, as well as device and application security management on any vendor's wireless infrastructure. Aruba also provides the RFProtect wireless intrusion detection and prevention system as an optional software upgrade.

Aruba's AirWave Management platform forms the heart of the company's network platform. AirWave provides a unified approach for managing wired and wireless networks with hardware from any major vendor. The platform eases network deployment with configuration templates and provides administrators with deep insight into network performance and troubleshooting functions. AirWave's VisualRF technology maps wireless coverage on top of floor-plan drawings, providing clear, actionable information about coverage gaps.

Aruba also offers a cloud management platform, Aruba Central, which works in conjunction with its Aruba Instant access point hardware to provide an easy-to-administer wireless platform. This approach is particularly well suited for organizations that have many remote offices. Administrators may configure an access point in Aruba Central and then ship an Aruba Instant access point to an office. Staff at the remote office simply connect the access point to the network, and Aruba Central handles the network configuration.

Organizations that wish to deploy Aruba 802.11ac wireless networking hardware have several product lines to choose from:

- The **200 Series** offers affordable, entry-level access points. These APs provide 866Mbps network capacity and support 2x2 MIMO with two spatial streams.
- The **210 Series** and **220 Series** support up to 1,300Mbps throughput and 3x3 MIMO with three spatial streams.
- The **228 Series** specifically targets rugged indoor environments, such as stadiums and warehouses. These APs also support up to 1,300Mbps throughput and 3x3 MIMO with three spatial streams.
- The **270 Series** also provides support for up to 1,300Mbps throughput and 3x3 MIMO with three spatial streams. These devices are specifically designed for all-weather outdoor use.

Aruba's wireless management platform and access points continue to grow in popularity among organizations large and small, particularly due to the company's vendor-agnostic approach to wireless management. This approach allows organizations to try pilot deployments of Aruba wireless networking without disrupting their existing networks running hardware from other vendors.

Cisco, HP and Aruba all provide excellent wireless network product offerings that fulfill the requirements of organizations of any size, with any mission. IT decision-makers should carefully evaluate each of these three providers and select the solution that most closely matches their technical needs.

CDW: A Networking Partner That Gets IT

CDW is prepared to assist you with every phase of your wireless network upgrades, serving as a one-stop shop for all wireless networking needs. CDW embraces a multipartner approach that ensures you will receive balanced, independent information about the wireless networking products available from many different vendors. Your CDW account manager can draw upon the expertise of wireless networking solution architects who specialize in 802.11ac wireless networking upgrades.

CDW takes a comprehensive approach to identifying and meeting the needs of every customer. Each wireless networking engagement includes five phases that help you identify the best ways to upgrade and improve the performance of your wireless network. These phases include:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing wireless network environment and the definition of project requirements
- Detailed vendor evaluations, recommendations, future design and proof-of-concept
- Procurement, configuration and deployment of the final solution
- Ongoing product support throughout the lifecycle of your wireless network

The services available from CDW representatives draw on the vast expertise of our team of technology specialists. To learn more about CDW's wireless network solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/wifi.

To learn how wireless networking upgrades at sports stadiums help teams improve the fan experience as well as their business operations, check out CDW's infographic "Win-Win Situation."

Cisco Gold Partner

Optimize wireless network performance while lowering costs and increasing operational efficiency. Deploy wireless controllers to help centrally manage, secure and configure access points throughout the organization.

CDW.com/cisco

aruba®

Aruba® Enterprise® wireless LANs provide pervasive Wi-Fi coverage across a global enterprise network delivering consistent, secure access to mobile devices anywhere at any time to employees, contractors and guests.

CDW.com/aruba

HP Networking lets organizations enable tools to configure the network for efficient transport of information, bandwidth optimization and enhanced application performance or automation of operations. HP enables efficient transport from LAN to service provider, across WAN links hosted in the data center.

CDW.com/hp

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT™