BUILDING MODERN WIRELESS NETWORKS

A strong network foundation requires an effective plan, design and implementation to best serve the organization's needs.

The widespread proliferation of high-bandwidth smartphones, tablets and notebook computers, combined with the bring-your-own-device (BYOD) approach to computing, means that organizations rely more on their wireless networks each day. How can enterprises plan for the continued growth of wireless networks and ensure that they have a modern, robust infrastructure that is ready for tomorrow's wireless needs?

Many IT decision-makers wonder if the rapid shift toward wireless networking will render the wired network obsolete. Craig Coolidge, a networking practice lead at CDW, believes that is not the right question to ask today. Instead, he suggests asking, "How do we need to plan our wired networks to support the next generation of wireless networks?"

A strong wired infrastructure will support the robust wireless networks that enterprises need. To build that foundation, organizations will want to develop an effective network policy to address today's wireless needs, conduct a site survey to improve performance of the wireless network,

READ ABOUT

- Developing effective networking policies
- The value of site surveys
- Strategies for managing user access
- Testing the vulnerability of networks

establish a system for managing user access that meets business and security requirements, and continually test and monitor the vulnerability of the network.

DEVELOPING AND **ENFORCING POLICY**

IT teams often struggle with effective and enforceable BYOD policies. They find themselves torn between meeting the needs of users and maintaining a secure, reliable network. Creating policies about the devices that individuals may use to access enterprise networks and data is challenging and often pits these seemingly competing interests against each other. In many cases, this situation leads to a policy that falls short.

Effective policy requires an understanding of an organization's users. As a guiding principle, IT leaders should keep in mind that users attempting to connect personal devices to the network are not adversaries. Rather, they are business partners who are trying to get their jobs done as efficiently as possible. With this in mind, IT groups should craft and enforce policies tailored to the needs and security requirements of specific departments, user roles and computing scenarios. A one-size-fits-all policy is probably not appropriate outside of the most highly sensitive environments.

RATHER THAN CREATING BYOD POLICY IN A VACUUM, ENTERPRISES SHOULD FOLLOW A FOUR-STEP PROCESS THAT INVOLVES STAKEHOLDERS AND BUILDS UNDERSTANDING:

01

Develop a policy draft. After assessing the business needs and security requirements of the organization, IT leaders should create a draft policy that may be used as the starting point for conversations about BYOD.

02

Validate it against business scenarios. IT managers should work with leaders from other areas of business to vet the policy and build a base of support. They should make sure that the policy does not impede productivity without a strong rationale.

03

Communicate the policy clearly. Users will not follow the policy if they do not know it exists. They will also search for technical loopholes to get their jobs done if they do not understand the rationale behind the policy.

04

Enforce the policy consistently. Effective and consistent enforcement of a BYOD policy requires technology support. Once an organization decides what devices are allowed on the network, IT staff should implement technical controls that block unauthorized devices.

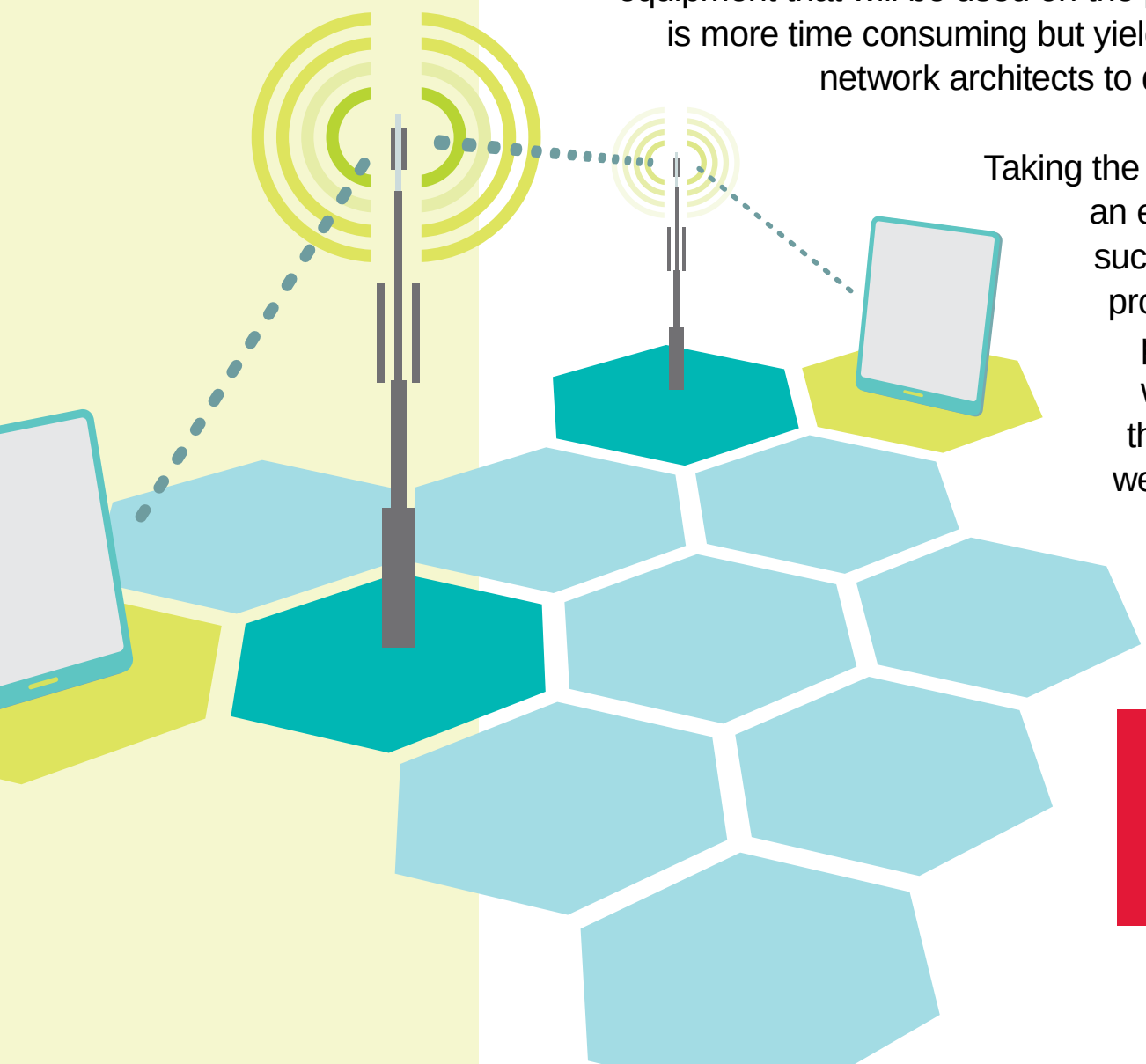
Following this process will provide enterprises with a clear, explainable and enforceable approach to personal devices on their wireless networks.

CONDUCTING A **SITE SURVEY**

Just as an architect would never build a house without first surveying the land, network engineers should not build wireless networks without surveying the radio frequency environment. Many factors influence the propagation of wireless network signals: the placement of access points, user density, device capacity, building materials and other sources of radio frequency in the area. Before an organization invests time and capital in building or upgrading a wireless network, it should commission a site survey that assists with the placement and tuning of wireless access points.

The simplest type of wireless site survey is the predictive survey. This approach consists of running blueprints through algorithms that suggest the number of access points needed for a given situation and the optimal placement of those radios throughout the site. Although this approach is easy and inexpensive, it fails to take into account several significant real-world factors, such as the construction materials used in a building or other Wi-Fi networks in the area. Using this approach may require several iterations before reaching a final design.

Organizations may avoid the limitations of predictive surveys by conducting a physical site survey. In these surveys, consultants or internal network experts actually walk the site with the same wireless equipment that will be used on the production network. This approach is more time consuming but yields very accurate results that allow network architects to quickly develop an actionable plan.



Taking the time to conduct site surveys is an excellent investment in the future success of a wireless networking project. An effective survey can prevent the dreaded reporting of wireless “dead zones” from users that might otherwise occur days or weeks into a new wireless initiative.

CLICK HERE

EXPERTS WHO GET IT BLOG

Read up on best practices for reducing rogue access points in a blog post by Craig Coolidge, CDW’s Practice Lead for Enterprise Networking.

FIREWALLING
WIRELESS NETWORKS

The growing presence of personal devices on enterprise networks (by both employees and guests) leads to a heightened desire to protect the enterprise-owned devices also on those networks. Organizations increasingly make use of firewalls to segment wireless networks from wired networks and keep different classes of users and devices from each other.

The design of a wireless segmentation scheme depends on the unique business needs of the enterprise. In the most basic scenario, organizations might create separate wireless networks for employees and guests and restrict the access that each group has to other devices on the network.

This approach protects enterprise assets from untrusted systems. In some situations, organizations may also wish to segment sensitive systems from the rest of the network. For example, engineers might create a restricted network for wireless point-of-sale devices that process credit card transactions in a retail setting.

Organizations can build a segmented wireless network by combining firewalls with their existing wireless infrastructure. One common way to do this is to create separate service set identifiers for each wireless network and then associate each SSID with separate virtual local area networks. Firewalls can separate the VLANs from each other, implementing different access policies for traffic between wireless VLANs and between wired and wireless VLANs. Enterprises can implement this solution using existing firewalls or by choosing wireless products that incorporate firewall technology.

As enterprises plan for expected growth in wireless network use, they should also ensure that the supporting infrastructure scales appropriately. For example, a network segmentation strategy will only serve an organization effectively if the firewall enforcing the separation has enough capacity to support all connected VLANs. Otherwise, the firewall itself becomes a bottleneck and limits the capacity of the entire network.

ROLE-BASED **ACCESS AND ENCRYPTION**

Maintaining separate SSIDs works well when organizations need to separate only a few classes of users and devices from each other, but it is not a very scalable solution. Running too many SSIDs on the same wireless network can reduce efficiency and create a substantial management burden for network engineers.

Organizations that wish to maintain granular access policies but bump up against the limitations of multiple SSIDs may choose to instead deploy technology that supports 802.1X, a protocol that helps to authenticate devices wishing to connect to a network. With this approach, the enterprise can run a single SSID and apply individual policies to each user based on his or her role. Engineers customize the network experience for each role, tailoring the network to meet the needs of each group of users.

From the user's perspective, 802.1X is nearly transparent. Users simply sign into the network using their regular credentials and then access their resources normally. Behind the scenes, the network authenticates them, confirms the access policy for that user's role and then applies appropriate security policies to ensure that only authorized resources are accessible.

From the network engineer's perspective, 802.1X allows organizations to provide a single, unified wireless networking experience across sites while still meeting security requirements. This technology allows granular access control while minimizing network overhead and scales to meet even the most complex security requirements.

VIRTUAL **PRIVATE NETWORKS**

Enterprises may wish to implement network access control that is more independent of the transmission medium. For example, an organization might restrict network access to a sensitive server in a way that applies across wired, wireless and remote networks. One time-tested way to apply this type of security is through the use of virtual private networks (VPNs).

Most users are already familiar with using VPNs for remote access to enterprise resources through an encrypted network tunnel. Connecting to the VPN virtually places them on the network while they are at home or traveling. This scenario is the most common deployment, but VPNs may also be used to facilitate user access from within enterprise networks. An organization might restrict access to a sensitive resource to only those users connecting through a particular VPN. Users may then securely access the resource over the VPN from whatever network happens to be available to them, be it the LAN in their cubicle or an airport wireless network.

The primary advantage of controlling resource access with VPNs is that this approach simplifies network topology and design. There is no need for complex SSID schemes or 802.1X access policies. Instead, authentication and authorization become centralized in the VPN, and any network merely acts as an access medium facilitating VPN connections. This approach is particularly useful in environments with decentralized computing models, such as universities and hospitals, where users may use several networks in a single day but require access to sensitive systems from each of those networks.

CLICK HERE

EXPERTS WHO GET IT BLOG

Read about how to arrange wireless access policy around a single SSID in a blog post written by Jesse Wiener, Converged Infrastructure Security Technical Architect for CDW.

MANAGING BYOD AT THE BIG GAME

Picture 75,000 fans carrying smartphones and tablets in approximately 40 acres of space: It is hard to imagine a wireless environment more complex than the championship game of a premiere professional sports league. Many of those fans (intentionally or accidentally) had the personal hotspot functionality enabled on their devices, creating multiple miniature Wi-Fi networks on the same channel. This crowded spectrum created a nightmare for officials trying to provide official gameday services using the same space.

CDW networking specialists partnered with the stadium personnel to clear the air of rogue wireless devices during the big game. Craig Coolidge, a network practice lead at CDW, and a team of networking specialists used Fluke AirCheck technology to pinpoint the location of personal hotspots in Arizona's University of Phoenix Stadium and then explained the situation to fans at small booths throughout the site, helping them reconfigure their devices to eliminate interference with official activities.

The result? "We went to great lengths to make sure that there was good Wi-Fi at the game," said Coolidge. "We set records for the amount of data sent over a wireless network."

TESTING WIRELESS SECURITY:
VULNERABILITY ASSESSMENTS AND PENETRATION TESTING

Network security is an ongoing process that requires constant attention and vigilance. Small configuration changes may have significant downstream security effects and expose the organization to security risks. For this reason, every wireless network should undergo periodic security testing to validate that it meets security standards. There are two main tools to assist with this effort: vulnerability assessments and penetration testing.

Vulnerability assessments involve scanning the network for known security issues and reporting them to administrators for follow-up and appropriate remediation. Conducting a proper vulnerability assessment includes analyzing wireless configurations and scanning the network to ensure that the implementation meets the organization's security policy. It may address these questions:

- Are all networks configured to support only strong WPA or WPA2 encryption?
- Do any wireless network components have default or weak administrative passwords?
- Can nonadministrative users access configuration ports on wireless devices via Secure Shell, HTTPS or other mechanisms?
- Do all wireless network components have current firmware updates and security patches applied?
- Are devices properly logging both successful and unsuccessful authentication attempts?

Administrators may supplement vulnerability assessments with wireless penetration tests. In these tests, normally performed by external parties such as CDW, skilled security specialists try to break into a network by undermining security controls. Penetration tests are the most realistic form of security testing.

One important technique used in both vulnerability assessments and penetration tests is the detection of rogue wireless access points. Users often connect unauthorized wireless APs to enterprise networks, and those rogue devices significantly undermine network security. They create an insecure method of access to the enterprise network, potentially bypassing authentication controls and opening the network to penetration risk. Enterprises should use rogue AP detection technology to routinely scan their networks for the presence of unauthorized APs.

COMBINING VIRTUALIZATION WITH VPN

Security-conscious organizations do not want sensitive data proliferating across a variety of personal devices because of bring-your-own-device (BYOD) practices. Placing data on employees' personal devices creates many forms of risk, including the potential exposure of that data if the devices are not securely configured and the difficulty of retrieving sensitive information if the worker leaves the organization. At the same time, enterprises want to encourage productivity-boosting BYOD practices. This creates a dilemma.

One approach to resolving this problem combines the use of virtual private networks (VPNs) and virtual desktops. Enterprises may create a virtual desktop infrastructure that provides employees with controlled access to sensitive information. The virtual desktop includes all of the productivity tools that users require to work with sensitive information, as well as access to shared storage.

When a remote worker needs to access sensitive information, he or she connects to the VPN and then uses it to access a virtual desktop. The data never leaves the virtualized environment, leaving no trace on the user's personal device after the connection terminates. This approach provides the power of BYOD without the risk of sensitive data proliferation.

CONCLUSION

Wireless networks are quickly overtaking their wired counterparts as the workforce becomes increasingly mobile and enterprises adopt BYOD computing policies. The typical user now carries multiple devices, each capable of consuming large amounts of bandwidth, further straining existing wireless infrastructure.

Organizations seeking to remain ahead of the wireless adoption curve must continue to research and implement next-generation wireless networks. In addition to improving network performance (by deploying new 802.11ac-enabled technology for increased capacity and optimizing the use of existing bandwidth), they must also design authentication and authorization mechanisms that extend security controls to wireless networks both inside and outside of central IT's control. This includes the adoption of 802.1X standards, VPNs and rogue AP detection in a manner that both protects wireless users and allows segmented, role-based access to enterprise resources.

Enterprises that adopt forward-thinking wireless strategies will find themselves well-positioned to take advantage of new wireless technologies that come on the market. These organizations will remain ahead of the wireless adoption curve and promote greater productivity among users. ■

>>