

Wireless Networking - Now or Later?

by LD Bean, CFO-Xcentric LLC

Wireless Networking is becoming almost unavoidable. Nearly every notebook/laptop computer comes with built-in wireless technology. Many coffee shops, hotels and airports are offering wireless access for a fee or for free to attract customers. In these scenarios, if you are not savvy about Wireless Networking technology, you may be inadvertently exposing information from your personal laptop.

Wireless networking can be a great tool or it can be a security nightmare. Within the next twelve months, wireless networking will become ubiquitous. However, it is important that you make the decision about when you will use wireless networking.

In order to make a good decision on when to implement wireless networking, there are several questions you must answer:

- What is Wireless Networking?
- What benefits can be realized through Wireless LANs?
- What are the disadvantages or risks of deploying Wireless LANs?
- Can those disadvantages or risks be minimized?

What is Wireless Networking?

Wireless Networking, Wireless LANs (Local Area Networks) or WLANs all refer to the same thing. It is simply a transport mechanism between wireless devices and among wireless devices and traditional wired networks – LANs and the Internet. WLANs make use of radio transmissions rather than the cables used by traditional networks.

WLANs have two basic components: wireless workstations and wireless access points. The workstation is simply a desktop computer or laptop that has a wireless Network Interface Card (NIC). This can be an external or internal NIC. Workstations can connect to each other without a wireless Access Point (AP) in “Ad-hoc” mode. APs are in effect hubs that connect the workstations to the wired network and to each other in “Infrastructure” mode. Generally, they have visible antennas and create the bridge to the wired network (LAN or Internet) via a regular Ethernet connection.

What benefits can be realized through Wireless LANs?

WLANs are faster to deploy than wired networks. There is no need for installation of Ethernet cables through walls, ceilings or conduit prior to implementation of a wireless network. Such cable installation can be expensive, so WLANs also generally have a reduced cost of ownership.

The ease and speed of deployment also makes for greater mobility and flexibility of WLANs. This is an ideal situation for audit or remote teams to easily communicate and share files, printers and other resources even while dispersed throughout the client location. It is also possible to use an AP as a router in order to connect your audit or remote teams to the client internet connection.

WLANs are also easily configured and modified in order to allow access to required applications and to accommodate as many users and resources as necessary for the growth of the organization.

What are the disadvantages or risks of deploying Wireless LANs?

Nearly all of the disadvantages of deploying WLANs are security related. Improperly configured Access Points or even improperly configured workstations on the WLAN could breach the security of the organization's wireless and wired networks in several ways. Lack of encryption, weak passwords and unprotected or default Service Set Identifiers (SSIDs) (the ID needed to access the WLAN) are a few of the configuration issues that could allow unauthorized access to the organization's network.

Frequently, a well-intentioned staff member will deploy unauthorized or "rogue" Access Points or workstations. This merely opens a gateway for hackers to exploit vulnerabilities of the network.

One non-security related disadvantage is the speed of WLANs. The wireless network standards used today consist of the 802.11 specifications as defined by the IEEE (Institute of Electrical and Electronics Engineers). These standards include 802.11b, 802.11a, 802.11g, 802.11x, 802.11e and 802.11i. The most common standard used is the 802.11b standard. It operates in the spectrum of 2.4 GHz and communicates at speeds up to 11Mbps. As for the 802.11a standard, it operates in the spectrum of 5 GHz and provides speeds up to 54Mbps. 802.11g operates in the spectrum of 2.4 GHz like the 802.11b standard, but it also provides speeds up to 54Mbps and is quickly replacing 802.11b as the preferred standard. The wired networks of today generally operate at 100Mbps with the Gigabit network (1000Mbps) beginning to gain popularity as the prices of equipment continue to fall. Obviously, such slow speed could make it painful for large file transfers or backups.

Can those disadvantages or risks be minimized?

There are several avenues of risk mitigation available. Because of the continued security threat inherent in WLANs, the IEEE continues to make improvements to security for wireless networks.

Wired Equivalent Privacy or WEP was the first wireless security and continues to be commonly used. This offers the most basic security and is the easiest to implement. However, WEP is known to have several security flaws.

In order to address these flaws, the IEEE and the Wi-Fi Alliance came up with a temporary fix to WEP called Wi-Fi Protected Access or WPA. This is a pre-cursor to the much anticipated 802.11i, or WPA2, standard – the supposed "silver bullet" for wireless security issues. WPA enhances and strengthens the encryption and user authentication of WEP. In order to implement WPA, there is generally a firmware upgrade for the WEP enabled hardware currently being used.

The most recently approved security standard is 802.11i. As mentioned, this standard is quite similar to WPA, but includes enhanced security through use of mutual authentication, dynamic key management and features a new encryption scheme called the Advanced Encryption Standard (AES). The 802.11i standard is much more robust than the previous standards. Unfortunately, it will require replacement of wireless networking hardware. Most wireless hardware vendors will have the new hardware available in May. Whether 802.11i is truly the silver bullet to wireless networking security can only be determined with the passage of time.

In addition to these wireless networking security standards, it is important to implement and enforce a firm-wide security policy. In addition to your current network security policy, below are some examples of policies you should incorporate if you implement a WLAN:

- Carefully consider where and when to place APs – consider window and door locations to minimize leakage of signal external to your building.
- Scan for and detect rogue APs.
- Default management passwords on APs and workstations should be changed to strong passwords – at least 8 characters, including at least 1 alphabetic, 1 numeric and 1 special character .
- SSIDs on APs and workstations should be changed prior to installation on organizational networks.
- Install WLAN on a separate network than the wired network with a firewall between the two when possible.
- Use a Virtual Private Network (VPN) to connect to your wired network from the WLAN.
- Enable a minimum of 128-bit WEP encryption on your WLAN.
- Control access to your WLAN via “MAC” address of authorized users.

When properly implemented a WLAN can be a powerful tool for your firm; enhancing productivity and increasing profits. It would be advisable to consult with a technology consultant to assist you with determining if a WLAN is appropriate for your firm. However, each firm is unique and only you can decide if the benefits outweigh the risks for your firm.

LD Bean is the CFO of [Xcentric](#), LLC, a technology consulting group that specializes in providing “Certified Networks for CPAs” and technical support solutions to CPA’s across the country. He can be reached at 678.297.0066 or at LD@xcentricgroup.com.

About Xcentric: Xcentric, LLC is focused on serving the technology needs of CPAs across the country. Through planning, deploying, maintaining and enhancing the total IT infrastructure, Xcentric puts CPAs in a position of leverage through the use of technology. Xcentric offers single-point accountability for end-to-end solutions that enhance profitability through increased revenue, productivity and customer loyalty. Xcentric provides expertise in consulting, collaboration, interaction, hosting and knowledge solutions that enlighten, empower and extend enterprise technologies.