

Wireless LANs in Libraries:

From Books to Wireless Broadband

The use of wireless local area networks (WLANs) in businesses and public locations is expected to triple over the next few years as more companies expand mobile workforces and make use of mobile applications that bring workers closer to customers and suppliers.

By 2009, 57 per cent of small, 62 percent of medium, and 72 percent of large North American businesses will have WLAN networks in operation with many making use of advanced Voice over Internet (VoIP) and other voice-enabled applications, according to Infonetics Research.

In fact, up to 75 percent of U.S. businesses are now evaluating or testing WLAN systems as extensions to existing wired networks, or as a front-office 'convenience' that may or may not connect to a company's primary wired network and information resources, adds Forrester Research.

Reasons for deploying WLAN networks in businesses vary, although there are some key motivators for adding a wireless network to an existing IT network. Chief among these is the desire to provide pervasive and immediate access to centralized information resources that might otherwise only be available through wired networks.

This is important since workers within office buildings and complexes can often spend a lot of time away from their desks and wired workstations running to meetings or interacting with other workers as part of an internal team.

Other reasons include: The need to provide seamless and secure access to email and collaborative messaging applications (for instant data exchanges with other remote workers); authenticated and easy access to specific areas of a company and its employees; and it is a cost-effective way to expand existing wired networks to a wider base of users and outside customers and suppliers.


Libraries share many of the same goals in developing and launching wireless systems, only the reasons may be more in tune with enhancing community and patron services than sharpening a competitive edge. A library's core business is to manage large amounts of information and make that information easily accessible to a wide range of people. So, a wireless network would seem to be a natural solution since it creates additional doorways and channels for that flow of information.

These same wireless networks can also be used by libraries as frameworks to support other evolving technologies that may be on their 'wish list' of expansion possibilities for internal networks and services. This list includes the use of radio frequency ID (RFID) systems and tags, Voice over IP (VoIP) networks, electronic books (eBooks) and digital distribution, virtual and multimedia reference libraries, and even database licensing opportunities.

The challenge is to develop and install wireless networks that are easy to use, secure, comply with existing technology and library standards, are flexible enough to adapt to a highly diverse clientele, and do not put too much of a service and support burden on the existing staff.

WLANs: Extending Core Services through Wireless

Libraries have a long history of cautiously adopting innovative solutions that might provide a way to better serve patrons and provide faster and more reliable access to large information resources. This history includes using the Dewey




Decimal Classification system, developed in the late 1800s as a universal way to categorize books and publications, and later adding the Library of Congress filing system to provide even more granular cataloguing.

Years ago, libraries turned to the Internet as a way to offer remote access to publication and resource catalogs and allow patrons to use their PCs to reserve books online. Many of these Internet-based networks now provide remote links to regional library partners that are linked geographically and allow users to scan multiple databases and reserve books through a local branch.

A number of larger and more progressive libraries have recently taken ease-of-access a step further by offering digital downloads of books and periodicals that can be temporarily stored on mobile devices and players. The idea is to develop new products and services that appeal to an increasingly mobile and computer-literate audience, while maintaining the benefits of its core resources.

The desire to expand services, provide access to a new class of patrons, and make use of emerging technology tools that are compatible with existing library systems and cataloging procedures is also encouraging many libraries across the country to investigate and deploy WLANs as a way of enhancing their internal services. Wireless networks are also being used to expand existing wired networks where additional hard wiring and desktop workstations are not an option due to budget or space restraints.

The Queens Library in New York, for example, installed a wireless network at its main Jamaica branch last year and has continued since then with plans to provide wireless access to all of its 63 locations in and around New York City. The library is one of the most extensive and ethnically diverse in the country and serves more than 2 million patrons per year.



Library administrators decided to install a wireless network as an alternative to adding more PCs. Now, patrons can bring in their own notebook computers and wireless devices to access the library's wireless network and hop on a high-speed T3 connection out to the Internet.

The goal was to provide a way for patrons to use their own computers to access the Internet and offer a way to disseminate information that would be consistent with library reference services, says the county's technical services manager.

This was also a part of the plan when the Boston Public Library (BPL) in Boston, Massachusetts initially offered wireless access at its downtown location and quickly expanded it to all 27 branch locations - an interesting technology contrast since the BPL is the first publicly supported municipal library in America and the first public library to lend a book.

Many libraries have discovered that wireless networks can also reduce the strain on library personnel and resources, since patrons use their own PCs to log into and use a network and browse resources. Wireless networks can also expand a library's technology infrastructure without adding significant equipment and support costs that come from adding additional workstations, extending existing wired system, or adding to the current IT staff.

The use of WLANs within public and private libraries will most likely grow over the next few years, and may even keep pace with the use of wireless LAN systems within the enterprise, which grew about 30% in the fourth quarter 2005, according to the Dell'Oro Group, a market researcher.

As noted earlier, libraries share many of the same concerns as businesses when it comes to wireless networks. These include:

- Security
- Reliable user access and authentication
- Centralized control and management
- Bandwidth control
- Overall cost
- Costs associated with service and support

Libraries must also deal with their own unique set of worries when it comes to wireless LANs because of the highly diverse makeup of users, governmental regulations related to privacy and confidentiality, and an operating environment that mingles the characteristics a WiFi hot spot with an information-sharing environment consisting of a wide range of media formats.

While businesses and municipalities may launch WiFi networks as a controlled public service or 'customer-facing' convenience, libraries must also wrestle with such things as U.S. Constitutional and censorship issues when designing and developing a wireless network for patrons.

At the Queens Library in New York, for example, the role-based policy management capabilities of the wireless network and a variety of content management software is used to restrict Internet access within the young adult sections of the library. This is done to comply with the federally-mandated Children's Internet Protection Act (CIPA), which was enacted to shield young patrons from obscene or pornographic material that is on the Internet. The wireless controller and software does this by looking at ID and log-in authorizations, and then matching that with the information contained on each patron's library card record.


Wireless Best Practice Meets Dewey Decimal

All wireless LANs, or WiFi networks, employ the same basic operating principle—to transfer data and information via radio waves rather than through wires and cabling. For small-office home-office (SOHO) applications, a WiFi network might consist of a cable or DSL broadband modem and high-speed connection; a wireless router or access point (AP), that communicate with the broadband modem; and one more wireless client devices, such as a notebook computer with built-in wireless connectivity or an add-in wireless card or plug-in transmitter.

In a typical operation, data is transferred to a broadband modem (cable or DSL) over a cable or telephone network, passed through the wireless router or access point, and then transmitted to a wireless client device. The flow is reversed for data traveling from the client device back through the broadband modem and out to the Internet.

Most wireless access points and client devices incorporate basic encryption and even firewall protection, which can be activated by the user to restrict unauthorized access to network. However, this type of protection is not suitable for business applications because it is more or less a deterrent rather than an adequate safeguard against serious security threats.

Also, basic consumer and SOHO wireless network configurations are not designed to provide secure user authentication, management and wireless traffic tracking functions – all of which are critical to effective business and library wireless local area networks.



In order to create a secure enterprise-class wireless network, you must add a controller to the system that sits between the point of connection to the Internet (usually, but not always on the protected side of a firewall) and a company's wired local area network connection. The controller works in conjunction with a computer server and directory software to authorize users and manage access to the Internet and through one or more wireless access points deployed throughout the network.

In effect, the controller functions as a second internal firewall to extend a wired network and provide protection and control without impacting the operation of that network. It can also be used to assign various levels of access to specific people or departments, restrict access to defined areas of the Internet (such as a library's home page and Website), and limit the size of information transfers through the wireless network (which can prevent unauthorized and illegal content downloads).

All controllers are not the same, however. Some function more as switches and data channeling devices and do not add any value in term of security and management functions. In evaluating controllers, libraries should ask the following questions to evaluate a system's features and functions:

1. Does the controller employ an open systems architecture that is able to support a range of wireless devices and industry standards? Also, can it support emerging and future wireless communications standards and protocols?

2. Is the controller compatible with WLAN security standards (such as 802.1x, WPA and 802.11i) without requiring additional client software? Also, does it allow users to roam seamlessly throughout a wireless network environment without requiring re-authentication?

3. Does the controller provide role-based management privileges and access levels for different categories of users, and match those to a library's or organizational structure? Also, can it be used to assign control levels to different user locations, time and schedules, and bandwidth priorities?
4. Can the controller also handle *selective filtering* to allow adult users' role-based access to all areas of the Internet and internal databases, while restricting access to younger patrons?
5. Does the system initially direct users to a customized log-in page for user authentication, and then allow that user access to the library files and Internet based on predefined role-based rules? Does this entry page also restate the rules of conduct on the library wireless network, and force users to agree to these rules before continuing onto the network?
6. Is strong data encryption and intrusion detection a part of the controller's core feature set? In addition, does the controller support IPSec (Internet Protocol Security) standards so that it can smoothly interact with virtual private networks (VPNs) and company firewalls (to accommodate business users who make use of a library's wireless network and related services). Also, can it defend against sophisticated identify theft and denial-of-service attacks from hackers?
7. Does the controller offer adequate safeguards against viruses, worms and other bits of malicious code that may reside on a user's computer that can inadvertently enter the wireless network? If so, is the controller able to quickly identify and block wireless traffic from these users and provide 'real-time' monitoring and filtering across the wireless network?

8. Finally, does the controller provide robust quality of service (QoS) controls that are able to examine each packet of data and shift performance characteristics and bandwidth to accommodate higher-priority applications or converged voice, video and data traffic?

A final piece of the wireless technology framework, available from only a handful of solutions vendors but quickly becoming a necessary element, is a dedicated intrusion detection and protection system that constantly scans a wireless network for signs of unauthorized users, rogue access points and potentially malicious activities. These systems can operate with independent sensors that monitor wireless traffic, and can also work with management software to provide a detailed audit of activities to document suspicious activity.

Securing the Wireless Library: From Books to Bandwidth

Security and user management are obviously of prime importance in library wireless networks, since these organizations routinely deal with a diverse user base and must also comply with a range of internal and governmental guidelines concerning content. In this post-9/11 environment, it is also important for libraries to be able to track user access to specific types of content and quickly identify users if they are legally required to provide data to law enforcement sources.

From a technology standpoint, wireless security can be broken down into three basic levels:

Level 1: Consisting of wireless products that offer some degree of wireless signal monitoring and limited ability to detect wireless traffic within a network environment. These products generally lack any capabilities to manage activity within a defined radio frequency (RF) space. They can,

however, be used to restrict user access to a specific AP or set of APs through MAC address IDs or user passwords;

Level 2: Includes wireless products that offer a basic signal monitoring and identification capability, and may provide some level of network roaming and bandwidth management. These systems may also be able to identify rogue access points and unauthorized intrusions, and be programmed to perform specific actions as they relate to predefined security policy enforcement rules;

Level 3: Wireless security systems that offer all of the capabilities of Level 1 and 2 systems, but add a strong and proactive control and management capability that is either embedded as part of the controller or independently installed on the outside 'edges' of the wireless network.

These systems may offer flexible content and network provisioning, location tracking and monitoring, real-time logging and auditing, and the ability to identify and isolate unauthorized access and accidental (or deliberate) associations with non-approved wireless access from outside the wireless environment.

The best security solutions include controller technology that is able to control and manage user access; software that is designed to automatically discover new devices across a network and apply enforcement, intrusion prevention and policy management rules; and a centralized management console that works in conjunction with independent sensor technology to watch over a wireless LAN and isolate questionable activities before they become serious problems.

In some cases, these sensor solutions make use of independent sensor units that can monitor RF activity throughout a multi-story library or across various

departments within a library. The most effective sensor systems incorporate a high-gain phased-array antenna to cover a wide area. They are also designed to monitor activity within a wireless network and work in conjunction with centralized controller-based security software, but work independently of the wireless network.

A Sensitivity to Standards: Keeping In Step with SIP2

Effective wireless security is more than just deploying the right hardware and software, however. It also involves applying these security tools and tactics to the organization and operational model of the library. Even the best security systems and safeguards will fall short if they are difficult to use or require library patrons to leap through too many authentication hoops to get onto and stay on the network.

Just as enterprise networks must be compatible with the existing database and information exchange structures within a company, library networks must also comply with unique standards established for this industry. One of these standards is the Standard Interchange Protocol (SIP), a de-facto standard in libraries for exchanging circulation data and transactions between different types of automated systems.

Most libraries use SIP2 (the latest version) for their relational database technology, and as an integral part of library self-checking systems, telephone renewal systems, security systems, and even RFID tagging applications.

SIP2 is also used as a common library data exchange format in wireless networks and is primarily used to authenticate users against patron databases. At least one wireless solutions company (Bluesocket, Inc.) has embedded the protocol into the management fabric of its wireless controllers, working with SirsiDynix Corp., a global developer of strategic technology solutions for libraries (www.sirsidynix.com).

Taking That First Step Toward a Best of Breed Wireless Solution

Most libraries base their decision to add a wireless network on two things: Recommendations from other libraries, which have gone the wireless route and lived to talk about the success of the system; and demand from library patrons, who may have had some exposure to wireless systems at their homes, office or local coffee shop hotspot, and see no reason why they shouldn't have wireless access at the local library.

Once the decision has been made to deploy a wireless network, the best route to success is to work with a systems integrator that is not only familiar with wireless technology but has a keen understanding of library operations and a range of experience in library automation. SirsiDynix, for example, has been involved in library applications since 1978 and has worked with approximately 4,000 clients and more than 23,000 libraries worldwide.

A systems integrator can recommend the best wireless hardware solutions and work with the library staff to integrate those solutions into existing systems with the least amount of pain. However, in order to design an effective wireless solution and develop user policies that maintain a high level of security and control, the library should first define exactly what it hopes to accomplish with the system and how it expects the system to grow and evolve over time.

The following is a quick checklist that can be used by libraries to develop a basic framework for a proposed wireless network and plan ahead for future expansion and technology improvements.

ü Think about what you hope to accomplish with a wireless network and how your patrons will interact with the system. If it will connect to an existing


wired network, or will be used by library personnel, remember to think about such things as user IDs, passwords and log-in pages. Also, don't make the mistake of putting too much effort into security and not enough on ease of use and user interface.

- ü Once you think you know what you want, find a systems integrator who understands the library business and automation and can work with you to design the best solution. Systems integrator candidates should have a strong track record in library systems design (and deployments), and a good relationship with wireless solutions vendors. They should also be aware of leading library system standards (such as SIP2) and offer solutions that comply with these standards.

- ü Develop a clear and well-organized wireless policy and list of procedures that are understood by everyone who will have access to the WLAN. Make sure these policies are clearly spelled out to users as they log into the system, and that users are required to agree to them by entering their log-in ID and password.

- ü Work with your systems integrator and wireless solutions provider to map out the planned wireless system, taking into consideration any unusual building structures, such as supporting columns and large shelves of books. Conduct a series of site surveys, using any one of several available tools to identify poor signal areas and dead zones. Continue these surveys as the network is constructed.

- ü In designing the system, you may want to develop specific 'hotspots' within the library. These stations could be a source of revenue if you decide to charge patrons for their use.

- 
- Ü In evaluating and selecting a wireless controller and related equipment (access points, sensors, etc.) look for 'best of breed' solutions that are designed to easily integrate and work together. Also, select systems that are compatible with industry-standard equipment or your own existing hardware and software.

 - Ü Be sure the systems you select will meet or exceed present needs and easily scale to fit future demands and changes in your wireless network.

 - Ü Designate a WLAN testing team, consisting of people from the library IT department, library personnel and patrons. This should be done in the early planning phases and continue throughout the design and deployment process.

 - Ü Develop training programs and formal ways of educating personnel and patrons on using the wireless network. Recruit those people who were part of the initial WLAN testing team as trainers and 'wireless champions' who can help limit the impact on internal (or even non-existent) service and support groups.

 - Ü Don't hesitate to ask the wireless solutions provider and systems integrator some tough questions about the system's capabilities. These include:
 - Does the solution provide adequate bandwidth management and user authentication procedures?

 - Can you easily adjust the system to increase or expand bandwidth to different users and user group, according to your role-based policies?

 - Can the solution be tailored to provide multi-level user access, based on pre-determined and assigned roles?

- Does the solution offer strong air-link protection and encryption, and is it able to quickly block unauthorized accesses and identify and isolate viruses?

- Can the wireless controller provide RADIUS accounting support and the ability to track usage by the length of time connected and/or the amount of data sent and received? (Important in restricting different types of data sent over the wireless network.)

- Does the system let users roam seamlessly between access points without having to log in again and restart their applications, even where the access points are on different subnets?

Case Histories



In early 1994, Sonoma County Library became the first public library in California to provide Internet service to its patrons.

The challenge was to develop a wireless network and provide Internet access to patrons since the library did not have enough computers for use by the public. By providing wireless access to the Internet, patrons could come to the library and use their own computers for high speed access. This would free up library computers for users who do not have their own computer.

Success Profile:

<http://www.bluesocket.com/pdf/govern/BluesocketandSonomaCountyLibrary.pdf>



The Queens Library is located in Queens, one of five boroughs in New York City and one of the most ethnically diverse counties in the U.S.

The challenge was to install a wireless solution to better serve more than 2 million patrons per year at 63 branch locations. The system would also be used to expand an existing wired and supplement an earlier wireless network used by library personnel. The library selected a Bluesocket, Inc. ® BlueSecure 5000 Controller as the base of a wireless network that helps the library continue in its role as the information hub of the community.

Success Profile:

<http://www.bluesocket.com/pdf/library/QueensLibrarySuccessStory-September2005.pdf>