

NLE
1276 S. 1380 W.
Orem, UT 84058
www.nle.com
www.wifilibrary.com



NLE Technology Report

Wireless Networks in Libraries



*Solutions for Creating and Managing
Wireless Networks in Libraries*

*Leveraging Existing Information
Technology Investments in Libraries*

Update: March 2006



Solutions for Wireless Network Implementation in Libraries

This document is written for librarians and library systems administrators to help provide a roadmap for introducing wireless data networks into their libraries.

What Are The Driving Factors for Wireless Networks in Libraries?

The rapid pace of change in the last decade in library information systems and knowledge sharing technology have created a lot of uncertainty for librarians and library administrators. Finding and implementing an appropriate solution for the library can be delayed by factors of cost, maintenance, standards, resources, confusion, etc.

The ideal information system environment for each library and library system should be based on the ability to use the best of what the library already owns, while allowing for the addition of new devices and processes.

Library information systems, such as those supplied by SirsiDynix™, have given libraries the ability to experience the usefulness of information system technology, and to apply this technology for the benefit of librarians and library patrons.

The addition of wireless (WiFi 802.11a/b/g) networks in libraries offers an opportunity for libraries to expand the reach of a library data network to include more patrons, devices, processes, knowledge-sharing, and community building experiences.

Outlined below are some of the factors that are driving the need and benefit for using wireless networks in libraries:



- **Libraries are installing and offering internet access.**

Libraries have been installing personal computers (PC's) for patrons to access the library card catalog, and usually have an Internet connection on those PC's to allow the patron to search for information through a Web Browser. While some libraries have this access, others may not yet have Internet access on every PC. In future visions of the role of public libraries, it is a foregone conclusion that the general public will expect Internet access. This trend yields other issues, such as local security policy enforcement, content filtering, desktop management, network infrastructure costs

- **Libraries must determine ratio of books vs. computers.**

Libraries would like to keep every book that has been purchased, but usually this is not possible due to lack of shelf space. The desk space required to hold standard PC's is as large as any book reading desk space. Libraries have limited amounts of space to yield to computers.

In addition, the cost of maintenance, upgrade, repair, and troubleshooting of networked PC's is estimated by industry analysts to be about \$ 2,500.00 per PC per year. In a large library, it may be typical to see that several computers at any given moment are non-functioning due to software, hardware, or other configuration issues.

The restricted number of PC's usually means additional mechanisms must be in place to control the time that the patron is allowed to use the computer. This means that the patron is limited to their accomplishments of research and productivity using the computer based on this time factor.

- **Laptop portable computers and PDA's with wireless network adapters are ubiquitous.**

Wireless networks in libraries could allow the opportunity for patrons to bring computing devices that they already own. This would create other opportunities for the library to expand other information systems and electronic media offerings by saving money on PC replacement and maintenance.

Most laptops sold today have an industry standard (WiFi 802.11a/b/g) wireless client device built in. Older laptops usually have a "wired" adapter, and if the right security infrastructure could be built, the library could allow these devices onto the network as well.



If patrons could use devices that they already own, this could improve patron access to information and allow the library to offer better use of information technology dollars. Budget monies now being spent on PC maintenance could be spent on needed network security, network infrastructure, and upgrades to the library information systems and databases.

- **Electronic Multi-Media offerings are increasing rapidly. Patrons will need access by electronic devices.**

The addition of electronic media in libraries requires additional access devices. The conversion of historical documents to electronic imaging is happening at an accelerated pace. The CDROM is now 20 years old, and DVD storage is a viable medium today. Magazines and journals are being offered in both print and electronic formats via the Internet. Libraries are using the Internet to order their books, and create catalog entries simultaneously.

- **Community events and private seminars at library facilities need access to information.**

Libraries can create opportunities for community development and offer use of facilities for local business and government. As these events may need access to information via the Internet, wireless networks are the perfect solution for allowing these events to improve in quality and quantity.

Even a book-fair in outdoor spaces of the library could benefit from a wireless network for conducting their transactions, ordering books on-line, etc. Using public libraries as a place of building the community by using shared access to information is accomplishing the highest ideals of libraries. Facilitating this by using wireless networks allows for rapid setup and tear-down for community and business events.

- **Older buildings are expensive and difficult to wire.**

As libraries are attempting to add PC's, printers, and other network devices, the cost and difficulty of wiring must be considered. Older buildings are difficult to wire because of the methods of wall and ceiling construction, lack of wiring closet space, etc, and this increases the costs. Wireless networks are the most logical solution to this problem.



What Are the Design Challenges of Wireless Networks in Libraries?

- **Public devices will include a mixture of laptops, network cards, and other wireless devices.**

When the library patron brings their own computing device, it will include a mixture of different vendors, operating systems, and network devices. The design of a wireless network will need to be open to most devices in use. The “ease-of-use” factors must be considered.

- **Public devices will have various operating systems, IP addresses, DNS settings, etc.**

The library patron may have a fixed IP address and additional DNS (Domain Name Services) addresses defined. The design solution should include the ability to use “port address translation” (PAT), and “network address translation” (NAT).

- **A public wireless network may need to be isolated from a private network already in existence.**

The design solution must include the ability for creating a “walled garden” where the patron can get to the servers, networks, and other network services, without exposing the existing network that the staff uses. This is accomplished by the use of firewall devices in the internal network, which in turn prevents the library from having to build a separate network for the patrons to use the wireless network.

- **Creating a wireless public network will require documentation of any existing network (routing, switching, firewall, etc).**

The design solution should be able to accommodate any existing network equipment used for switching, routing, etc. This is important to reduce the cost of implementation and maintenance. Defining the installation locations and position of the wireless network components may be a challenge for the library, however, if good documentation of the existing network exists then it can be easily reviewed by others who can help.

If the library is including a wireless network to a new construction project, the placement of the wireless network components needs to be considered in the design.



The NLE recommended solutions include placement of a wireless network access control gateway (internal firewall) before the first router hop. This is the main design consideration for determining the location of the wireless network components.

- **Radio frequency interference must be analyzed.**

In each wireless network environment, there is the potential for radio frequency interference that will cause poor network performance, prevent access, create other support issues. There are excellent radio frequency tools available to help the design process, and to continuously monitor the radio frequency environment.

- **Public network must be designed with “ease-of-use” for users.**

In every design of a wireless network for libraries, the primary measure of success will be the “ease-of-use” factor. The criteria should be that if the patron and staff can use an internet web browser, then they can gain access to the wireless network in the library. Additional functionality should not be dependent on adding additional software to the patron’s laptop or PDA device.

- **Administrative and support tasks must be included in the design.**

In addition to “ease-of-use” design, the wireless network design should be easy to administer and configure. If the library staff needs to make changes to the access policies, the change management process should be easy to understand, to train others to do, etc.

The administrative interfaces of the wireless components which are “web-based” are considered to be the easiest to understand and to train others. It is recommended that all of the wireless components have some web-based management.



- **Design must include methods to “future-proof” the investment, and accommodate emerging wireless standards.**

The wireless networks industry standards have been in the process of change, especially since 1998, and will be continuously reviewed and improved. Changes in the way the radio signals are processed and optimized will continue to be made. The design of the wireless network should try to isolate the components that will change over time, or require replacement, and minimize the replacement of the methods for creating policies and access control. This will reduce the cost of ownership and keep the network flexible to rapid changes as the technologies change.

The wireless network in libraries should try to reach the broadest compatibility with industry standards in order to accommodate the greatest number of patron devices. The deployment of 802.11g (22 Mb/sec through-put) access-points, for example, will allow patrons to use 802.11b (11 Mb/sec through-put) wireless devices, due to the backward compatibility of the industry standards.

What Are the Security Challenges of Wireless Networks in Libraries?

- **Public wireless network will require method to control bandwidth use – especially for Internet access.**

One of the top security concerns is someone’s attempt in a public network to consume all of the available bandwidth with large file downloads, launch of a denial-of-service attack, or other types of “bandwidth hogging”. The ability to limit bandwidth for each user is an important security feature that must be available for wireless networks in libraries.

- **Public wireless network will need method of authentication to keep network for library patrons.**

The goal for creating a wireless network in libraries is not to create an open public internet “hot-spot” for everyone. The goal is to allow the patrons to use their own networking devices for access to library services. Most libraries have some form of an electronic card-catalog, electronic media subscriptions, etc. The method for authentication is generally initiated from information contained in a library card. Access to the wireless network should follow the same authentication procedures as other PC devices already owned by the library.



NLE, in partnership with SirsiDynix™, has identified the authentication methods for libraries that use the widely deployed SirsiDynix™, and SirsiDynix™ Horizon patron databases. NLE has been successful in deploying wireless network access control to library resources by using the 3M SIP2 authentication method, as well as the Dynix Remote Patron Authentication (RPA) as the intermediate access device. When either method is used to query the database, this resultant patron information can be used as a mechanism for controlling access to the wireless network. The wireless access-controller must have the ability to define the credential parameters as an external authentication server. When traditional databases are evolved into LDAP standard databases, then the wireless network access control components must be able to support this type of access too.

- **Public wireless network must be able to leverage existing authentication databases without having to re-create.**

Even a small city public library can have thousands of patrons. The existing database of patron information needs to be utilized, not re-created. The administrative and security issues of having to use a separate database for access control would be difficult to manage.

- **Public wireless network will need to require no additional client software other than current standard web browsers, etc.**

This is also a design issue. If additional software has to be installed on the patron devices, this would limit the ability of the library to change the methods of access, available network resources, etc. In addition, there would be administrative, management, licensing, and potential liability problems with trying to disseminate and control software to a patron owned device.

- **Public wireless network will need to prevent security risks such as “peer-to-peer” file-sharing software, spam email launching, rogue access-points, denial-of-service attacks, etc.**

The wireless network administrative tools must be able to detect and prevent other security risks that are presently known to be present in networks. This will include the ability to prevent the creation of “ad-hoc” wireless networks using the library resources, spam email launches, peer-to-peer file downloads through the library network, etc.



NLE, in partnership with SirsiDynix™, has deployed tools that will accomplish the prevention and detection of these types of security risks. Libraries can use these tools and feel confident that their network infrastructure is being used appropriately.

- **Public wireless network will need to be capable of managing multiple levels of security based on type of user (staff, patron, etc.)**

Access control components need to support different policies for different types of users of the wireless network. The library staff will naturally need to have greater access to library information systems, whereas the patron will probably only need access to card-catalogs, electronic media libraries, the Internet, etc.

Policies that are “role-based” are the ideal method of delivery. Access control components should be able to support “role-based” administrative users as well, to have other library staff be able to monitor wireless network use, troubleshoot a patron problem, etc.

- **Public wireless network must have a mechanism to enforce acceptable use policies, Internet content filtering, proxy server redirection, etc.**

Public libraries that use U.S. federal government funds may have the additional requirement to be able to perform Internet content filtering. This may require additional proxy server controls. The wireless network access control components may need the ability to force TCP (port 80) traffic to be redirected to a proxy server.

If the library needs to enforce other “acceptable use” policies, there needs to be methods for restricting a selected user if there is violation of an acceptable use standard. This means that individual user control must be a feature of the access control components.

What are the Benefits of Public Wireless Networks in Libraries?

- **Libraries can improve patron satisfaction by fulfilling greater demands for access to information (eliminate patrons waiting for a PC, etc.).**



- **Libraries can reduce the capital expenditures for PC's and reallocate these budget dollars to create better content, services, or information systems.**
- **Libraries can utilize desk space more effectively, and create new areas for reading and accessing electronic media owned by the library.**
- **Libraries can utilize open space, conference rooms, and outdoor patio space more effectively by creating access to information in these areas.**
- **Libraries can better support community events and conferences by providing secure access to information and the Internet.**
- **Libraries can utilize the wireless network infrastructure to start testing or deploying other emerging wireless technologies such as RFID, IP telephony, PDA's, etc.**

What are the Goals for Public Wireless Networks in Libraries?

- **Goal 1: Solve the Design and Security Challenges listed in this document.**
- **Goal 2: Use the existing network infrastructure as much as possible.**
- **Goal 3: Use wireless network components that will: support industry standards, adapt to emerging standards, reduce "total-cost-of-ownership", and provide methods to transition from one technology to another.**
- **Goal 4: Create a public wireless network that utilizes existing authentication methods already in use by the library, such as SirsiDynix™ Remote Patron Authentication.**



What are the Components Required for a Wireless Network in a Library?

One of the purposes of this report is to emphasize the requirements needed for a successful installation of a wireless network. The components and equipment that are required is based on many factors, such as size of the library, number and size of open areas for wireless, level and type of existing network equipment, and a range of issues as previously outlined in this document.

This NLE Technology Report is accompanied by two case histories of Libraries that have followed the NLE design approach with success.

The NLE approach to design and implementation of wireless networks in libraries is based on three major components:

- **1. Access Control Layer Components**

NLE's approach is to use "internal firewall" components to create wireless networks. These internal firewall components are used as security gateway devices, and must be able to support any type of wireless access-point. NLE has chosen the best components to solve the design and security challenges discussed in this paper.

*NLE technology leader selection:
Bluesocket™ Wireless Gateways with NLE-SirsiDynix™
enhancements.*

- **2. Radio Analysis Components**

NLE's approach is to use wireless network management tools that give the best management value, ease of administration, analysis of the wireless traffic, performance and security monitoring, etc.

*NLE technology leader selection:
AirMagnet™ Wireless Network Analysis tools.*

- **3. Wireless Access-Point Components**



NLE's approach to wireless access-point components is to use radio components that are reliable, scalable, and easy to install and manage. One approach of the last two years is to increase the functionality within the

access-point, however, this approach is not likely to be the best long term investment protection based on the changing standards of radio frequency types (802.11a, 802.11b, 802.11g, etc.) NLE sees the industry moving towards a lightweight access-point that is tuned to maximizing throughput. The role of security will be the function of the first component above (access control component). This will yield a better solution based on the ability to expand the wireless network, use the internal firewall for wired devices as well as wireless devices, and transition from one method of authentication and/or encryption to the next.

NLE technology leaders selection:

- Bluesocket™ AP1500/AP1540 lightweight AP
- Cisco™ "Aironet" access-points: 350, 1100, 1200.
- Proxim™ access points.
- Hewlett-Packard™ ProCurve access-points
- Home-grade, or small-office grade AP's are **NOT** recommended.

Conclusion – Wireless Networks Create New Library Environments

Indeed, providing access to information using patron computing equipment is an important next step to library environments. These new library environments need to have a network infrastructure that can maintain the library security while providing the patron reliability and ease-of-use. NLE has the culmination of these technologies to not only introduce this rapidly deployed technology safely, but also gives a strategy for confronting an ever changing segment of high-adopted wireless technologies.

For further information, please contact NLE at 1-800-243-5267, or your SirsiDynix™ representative.