The Library Wireless Hotspot

A library's interest in establishing a wireless network may take two forms. The library may be interested in providing a wireless hotspot for patron convenience, or it may want to have a wireless network for the use of its own personnel in order to give them more flexibility so they can perform work throughout the library's physical space.

The key security concern for a library's public access wireless LAN involves isolation from the library's staff network. As noted previously, it's essential that all public access computing—both both wired and wireless—be effectively walled off from the library's staff network. Although there may be some security risk to library patrons, the risk is no greater in the library-provided hotspot than the security risks in other hotspots, such as Wi-Fi hotspots provided by coffee shops, hotels, and airports.

Because the library's hotspot is provided for the distinct purpose of giving library patrons Internet access, many of the concerns surrounding wireless security do not apply. For example, one of a security scheme's goals might be to prevent freeloaders, unauthorized individuals, from getting free Internet access. But that's the main purpose of the library's public wireless network—to provide free Internet access. Hopefully, users will take advantage of the great resources provided by the library along the way.

The legacies of War Driving and Warchalking have resulted in the fear that individuals could attempt to use the library's wireless network from the parking lot. If the library has properly configured its hotspot for public use (by isolating it from the library's business network), there is no increased risk posed by one accessing the network from the parking lot.

Wireless networks intended for library staff use should resemble a network utilized inside a corporate network. The concern focuses on ensuring the data traffic is protected, that traffic isn't intercepted and viewed by an unfriendly third party. Although libraries usually don't deal in top-secret information, some information handled by libraries is somewhat sensitive. Library budget data, personnel information, and patron data should be protected. Even the information from the library's automation system can be too sensitive to expose on an unprotected WLAN. Circulation transactions may include such details as patron names, addresses, phone numbers, materials checked out, or even social security or credit card numbers. The privacy policies that most libraries follow require that such information be restricted to library use. To be consistent with such a policy, unencrypted transmission on a wireless LAN is not appropriate.

Staff use of a wireless network can be accommodated in at least two ways. One way would involve setting up a different wireless LAN separate from public-use hotspots. The staff-use wireless LAN would at least have WEP-enabled but preferably WPA or WPA2. It would reside on the inside of the library's firewall, associated with an Ethernet switch port on the staff side of the network. The access points on the staff-use wireless LAN could have MAC address filtering enabled as an additional protection layer to limit access to authorized computers and PDAs.

The other wireless LAN option (for a WLAN utilized by library staff only) would involve the use of a VPN. In a small library, it might not be practical to have one set of access points for use by staff and another set for the public. In these cases, the library would set up a wireless LAN configured appropriately for public use—well isolated from the staff network. Library staff could make use of this network for library business through the use of a VPN. The VPN would provide adequate security for library business transactions regardless of the security options present on the wireless network.

Almost all libraries now provide Internet access. Most use stationary, specially configured computers—set up with restrictions to prevent tampering and ensure security—to provide access to library resources and the Internet. A recent study conducted by the Information Use Management and Policy Institute at Florida State University included three findings (listed in the Executive Summary of the study) that describe how US public libraries provide Internet access:

- 99.6% of all public library outlets are connected to the Internet (in 2004). Of those libraries connected to the Internet, 98.9% offer public access computing for their patrons.
- Nearly 18% of public libraries already have wireless Internet access, and 21% plan wireless access within the next year.
- Struggling to meet public demand—Public libraries have as many workstations as they can afford or their building spaces will allow, yet more than 85% of libraries report *not being able to meet demand* for computers consistently or at certain times of the day.

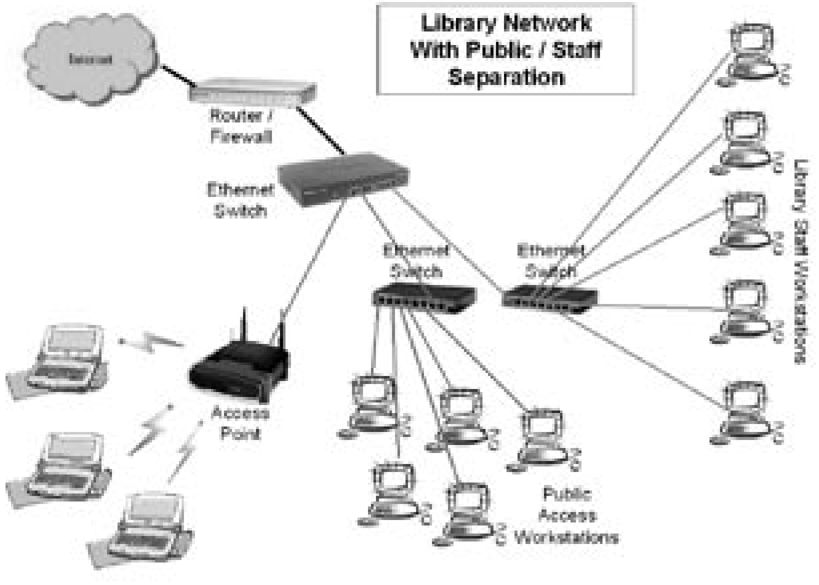

Figure 10
Network diagram illustrating the separation between public and library staff computing.

From these findings, it's evident that a large portion of pubic libraries (about forty percent) will offer wireless access to their patrons. This means roughly sixty percent still do not yet have specific plans to do so.

Most libraries lack the space or resources to provide enough computers for public use. Since wireless LANs don't require additional space and can be installed relatively inexpensively, they can be considered as an important component for libraries' strategies in meeting their patron's Internet access needs.

Wireless access to the Internet is becoming a service with ever-increasing demand. Business travelers, students, and the general public expect and appreciate being able to connect to the Internet through public wireless hotspots. Some municipalities have deployed or are planning wireless networks. This remains somewhat controversial, given the potential competition with commercial offerings.

Wireless LAN Features and Functions

A variety of technical solutions are available to support many different approaches for establishing a library public hotspot. If the library prefers security, it can implement WEP, WPA, WPA2, or 802.1X. Those that want an open wireless hotspot can do so safely with proper attention to isolating that network from the library's business network.

Click-Through Agreements—The library may prefer to have users view a Web page that describes any restrictions that apply to the use of its wireless network—disclaimers of liability, funding credits, or warnings about security vulnerabilities. These statements can be presented on a page the user must view and acknowledge before being allowed to use the wireless network.

Access Control—Some libraries limit wireless network access to registered users. Library patrons would be required, for example, to identify themselves with their library card numbers in order to access the network. This type of access control may be enforced on an open or a secure wireless LAN.

Content Filtering—Another feature of a library's public wireless network involves filtering. As patrons access the Internet through the library's wireless network, will the content be filtered or unfiltered? Approaches to this issue vary. Some libraries take the view that they are required to filter all access to the Internet that takes place within their walls. Others do not filter because the access takes place through computers owned by the patron.

There are technical solutions to either Internet-filtering approach on a public wireless network. To effectively enforce filtering on a wireless LAN, it must be done on the network level rather than on the client level. Some filtering applications rely on client software installed on the workstation that's accessing the Internet. It would be impractical to require patrons to install such software on their computers so they could use the library's wireless LAN. A better approach would be one provided by the filtering solutions that operate on the network level. There are a number of network appliances designed to provide filtering services for networks. These can be configured with varying degrees of aggressiveness, and the administrator can select which network devices must operate through the filter and which have unfiltered access.

The choice a library makes regarding filtering will depend on its interpretation of the Children's Internet Protection Act (CIPA) and the preferences of its governing boards or other policy-making bodies. (For more information on library filtering software, consult Lori Bowen Ayre's issue of *Library Technology Reports* Mar/Apr 2004 [40:2], "Filtering and Filter Software.")

Fee-Based or Free? The library may need to charge a service fee for access to its wireless network. Although most libraries offer wireless access as a free service, there may be some circumstances in which it would be necessary to charge at least some categories of users. There are many commercial hotspots that charge access fees, and the e-commerce infrastructure to support this option could be easily adapted for library use.

Wireless Policy Development

Given that there are technical solutions to a very broad range of options for implementing a wireless network, the shape of a library's wireless network service can be formed through an administrative process; *it need not be dictated by technical or security requirements*. If the library administrators, for example, elect to offer a convenient, user-friendly open wireless network, the library's technical staff should be able to design and implement such a service without compromising the security of the library's overall network. If, on the other hand, library management chooses an authenticated and encrypted network, technical solutions are readily available. Technical staff should be consulted regarding the costs and resources involved to implement and support each option under consideration.

Wireless Networking Services

Most libraries will develop a wireless network Web page that describes the service, presents any policies and restrictions that apply, and usually provides a list of frequently asked questions (FAQ). A representative sample of libraries' wireless network information Web pages (and the URLs) are listed in the screened box above and in the screened box on page 34.

Atlantic City Free Public Library, Atlantic City, NJ
www.acfpl.org/wireless.htm

Austin Public Library, Austin, TX
www.ci.austin.tx.us/library/wireless_at_apl.htm

Burlingame Library, Burlingame, CA
www.burlingame.org/library/wireless.htm

Chicago Public Library, Chicago, IL
www.chipublib.org/003cpl/computer/wifi/wifi.html

East Lansing Public Library, East Lansing, MI
www.elpl.org/wireless.htm

Hennepin County Library
www.hclib.org/pub/info/wireless.cfm

Linda Hall Library, Kansas City, MO
www.lindahall.org/wireless/

Menlo Park Library, Menlo Park, CA
www.menloparklibrary.org/wireless.html

Mill Valley Public Library, Mill Valley, CA
www.millvalleylibrary.org/wireless.html

Sample Wireless FAQ

Many libraries provide a Frequently Asked Questions (FAQ) page to assist their patrons when they are using the wireless network. The following is a composite of FAQ pages typically offered by libraries:

Q: What equipment do I need to access the wireless network?
A: You will need a laptop computer or PDA equipped with a wireless network card that supports the 802.11b or 802.11g standard.

Q: How do I use the wireless network?
A: To access the network, use the following settings. How you apply the settings will vary, depending on the type of computer you use.

SSID = your SSID here
WEP = disabled or off
Network mode = infrastructure
Network properties: Use DHCP to obtain values
IP Address: Obtain IP address automatically
DNS: Obtain NDS address automatically
Gateway: Obtain gateway address automatically

Q: Do I need to enter a WEP key to access the wireless network?
A: No. WEP is not used on this network. **OR**
A: Yes. You need to obtain the WEP key from the circulation desk of the library.

Q: Will I need a username and password to connect?
A: Neither a username nor a password is required.

Q: Is the network secure?
A: Information sent to and from your computer is not protected using this wireless network. Some Web pages may provide their own encryption. It's possible that others could view information you send or receive on a wireless network. Keep this mind if you access sensitive or personal information. **OR**
A: Yes, the network uses WEP/WPA to provide security on the wireless network. Information is encrypted on the wireless network but will not be encrypted on the Internet.

Q: Can my computer get a virus from using the wireless network?
A: Wireless networks do not provide any special protection from computer viruses or worms. You should be sure that your computer has anti-virus software installed, it's activated, and up to date.

Q: Where can I access the wireless network?
A: The network is accessible throughout the library building, including in some outdoor areas near the library.

Q: Can I access the library's catalog and other databases using the wireless network?
A: Yes, the library's catalog and all the resources provided through the library's Web site, [insert URL here], are available for free using the wireless network.

Q: Will content (Web pages, sites, portals) be filtered while I use the wireless network?
A: No, the library does not enforce Internet filtering on the wireless network. **OR**
A: Yes, the same Internet filtering is enforced on the wireless network as with the computers provided by the library.

Q: Can I check my email while using the wireless network?
A: Yes.

Q: Are there outlets available to power my laptop?
A: The library has a limited number of power outlets. We recommend that you come to the library with a fully charged battery.

Pasadena Public library, Pasadena, CA
(requires valid library card and PIN)
www.ci.pasadena.ca.us/library/wireless.asp

Salem Public Library, Salem, OR
www.salemlibrary.org/wireless.html

San Diego Public Library, San Diego, CA
www.sandiego.gov/public-library/searching-the-net/wirelessaccess.shtml

Spokane Public Library, Spokane, WA
www.spokanelibrary.org/about/wireless.asp

Ruth Lilly Medical Library, Indiana University
(VPN required)
www.medlib.iupui.edu/techsupport/wireless.html

Sonoma County Library, Sonoma County, CA
www.sonoma.lib.ca.us/wireless/

University of California, Davis, Davis, CA
(MAC address registration required;
authentication with UCD LoginID
and password required)
www.lib.ucdavis.edu/ul/services/computers/wireless/

University of Winnipeg Library and
Information Services (WEP key required)
http://cybrary.uwinnipeg.ca/services/systems/wireless/connecting.cfm

Warren Newport Public Library, Gurnee, IL
www.wnpl.alibrary.com/AboutLibrary/Wireless.htm

Q: Can the library help me connect to the wireless network?
A: You are responsible for configuring your own equipment. All computers are different, and the library is unable to provide assistance in configuring your computer. The documentation that came with your computer or wireless card may have helpful information. The manufacturer of your computer or wireless card may offer support services to help you.

Q: Are there restrictions on what I can do when using the network?
A: Users of this network agree to abide by the library's Internet Access Policy [insert link to your library's policy here].

Q: Can I print while using the wireless network?
A: The library does not offer printing. We suggest that you save any pages to disk that you may wish to print later, or you can e-mail the information to yourself. Printing is available on the public workstations provided by the library.

Q: Can I download large files over the wireless network?
A: The wireless network bandwidth is limited and shared by all users of the library. We ask that you not download very large files or view streaming audio or video.

Small-Screen Devices

Wireless networks incorporate many types of devices. Although the most common may be the notebook computer equipped with a wireless radio, other devices may also take advantage of the technology. PDAs (personal digital assistants) and other small-screen devices should also be taken into consideration in the design of wireless network services. These smaller devices don't necessarily introduce any new requirements for connectivity; they implement the same communications and security protocols as full-sized mobile computing devices. But their smaller screens do introduce concerns related to the content delivered on the network. How effectively do the library's Web pages, online catalog, and other resources display on a small-screen device? Many of these resources are tested only on full-sized displays.

To the degree that you anticipate access of your library's content services by users with small devices, development and testing should be performed. XHTML and cascading style sheets (CSS) are well suited to the development of pages that display well on both full-sized and small-screen devices. The CSS environment provides the ability to present different page characteristics based on the "media" specified. The media option "handheld" is available to specify how any given element in the page should be displayed for small-screen devices. Creating Web pages that display well for different types of devices is one of the greatest challenges in Web content management.

Although the library may have control over the design of its Web site, it doesn't have as much influence over many of the Web-based applications it uses, such as the Web OPAC of its library automation system. It may be desirable, though, for the library to offer a Web OPAC that works well for small devices. Innovative Interfaces offers a version of its Web OPAC, called AirPAC, designed specifically for small devices.

Although this report doesn't include cell phone communication technologies, it's worth mentioning that cell phone service plans usually include an option for Internet access. The efforts devoted to creating pages that display well for PDAs connected through wireless LANs will also pay off through an improved experience for those that access library Web services through cell phones.

Wireless in the Academic Library

Increasingly, it's expected that wireless access will be provided on college and university campuses. Many students take computers to campus, and more of those computers are of the mobile notebook variety. Ideally, wireless access would be available throughout the academic campus. Given the size and complexity of many campuses, access may be selective. Residence halls, classrooms, student centers, and libraries are some campus facilities in which wireless access is commonly available.

Providing wireless access in academic libraries can be an important part of the library's menu of services. If wireless networking is available in other campus locations rather than in the library, it could result in reduced activity levels.

Wireless Benefits for Library Staff

Wireless networks and mobile computing can also facilitate the work of library personnel.

Remote Circulation—Circulation activities don't always have to be tied to the traditional service desk. A renovation project or unplanned facility problem may cause the library to temporarily offer circulation services from an alternate location that may not have a wired connection. If it's in range of the wireless network, the temporary circulation desk could use it, provided adequate security precautions were in place.

In addition, a library may hold special events after hours or in a part of the facility not convenient to the circulation desk. As part of the event, librarians may have selected library materials that can be offered to attendees. A temporary circulation desk could be set up to conveniently check out these materials.

Most libraries track the use of materials consulted in-house as well as those checked out. The circulation module of most library automation systems offers the ability to track in-house use through scanning barcode numbers. A library worker will collect the books that have been consulted, transport them to the circulation desk, and scan their barcode numbers before reshelving them. If the circulation desk is distant from where the books are collected, a wireless mobile computer can minimize physical trekking, thus saving staff time. Staff members could scan the books to record in-house use, saving themselves the round trip to the circulation desk.

Inventory—A wireless network can also make an inventory project more efficient. In order to perform an inventory or shelf-reading project, it's necessary to scan all the books in a section of the library's book stacks. These barcode numbers representing the books actually on the shelf can be fed into a program that compares them to the theoretical holdings as defined by the library's automation system. These lists can be reconciled to determine missing items and errors in the database. Using a wirelessly connected hand-held PDA or notebook computer, these inventory tasks could be performed more conveniently.

AirPac by Innovative Interfaces
www.iii.com/mill/webopac.shtml

Reference Service—Mobile wireless computing can be used to improve reference service, too. A reference librarian equipped with a wirelessly connected laptop computer—with full access to the library's online catalog or other resources—can assist users throughout the library.

In general, librarians tend to move around a lot. They spend time working in offices or cubicles, cover shifts at service desks, attend meetings, take work home, and travel to conferences and business meetings. Like professionals in other fields, library personnel can work more efficiently with the mobility enabled through wireless networks.

Keep in mind, though, the points regarding security requirements associated with library personnel's use of wireless networks. It's imperative that a wireless network utilized by library staff operate with security features enabled.