The Wireless Library: Technical and Organizational Aspects

by GERHARD SCHNEIDER

The slides of this paper can be found at: http://www.zhbluzern.ch/LIBER-LAG/PP_LAG_04/Wednesday/G_Schneider/G%20Schnei%20ppPraes%20oAn-un.pdf

ABSTRACT

The deployment of (wireless) networks in a library in order to help users to access modern digital data is possible at low cost. All necessary hardware and software components are readily available. The technical as well as organisatorial issues can be solved in a satisfactory way requiring little or no additional work for librarians. It is even possible to charge users for outside connections. Management has to decide whether this is a good idea.

INTRODUCTION

While most universities deploy wireless networks to cope with the needs of students and staff, many libraries are still uncertain whether and how they should provide Internet access to their customers. The demand from users may be acknowledged but it is unclear how such a demand could be met without added security risks for the library and what would be the impact on library funds.

THE CHANGE IN RAW MATERIALS

The dawn of the electronic age in libraries is not solely due to the introduction of online catalogues. Most modern publications are now born digital and more and more of these publications are delivered in electronic only format, either on hard copies like CDs or DVDs or just in time to the user's desktop over the network. Many PhD theses are only available online as they belong to the few publications which are fully under the control of the university system and are therefore among the first to experiment with new media. Many libraries operate large servers to provide storage space for such online data. Apart from offering fast access such online storage seems to be considerably cheaper than the traditional shelf system with its necessary building infrastructure. Long term storage issues appear to be solved at least with respect to replacing the capabilities of paper.

THE CHANGE OF USER EXPECTATIONS

In the past users were quite happy to walk up to centralized terminals in order to start their queries and then to copy the information from books or journals either by hand or with copy machines. Nowadays users want to store their information on personal storage - even if they print it out for readability because they do not yet want to afford expensive high quality displays - and therefore require means to transfer digital material from the library directly onto their private machines, copyright permitting. Typical service offerings in libraries include the data transfer to floppy disks or to CDs, rarely to modern USB memory sticks. These services become increasingly difficult to deliver as more users start to use them.

They are also becoming obsolete, as users start to bring their private notebook computers or personal digital assistants into libraries to transfer the data directly to these devices. Even more the machines can be used to access any information provided by libraries and even connect to the Internet. The most noticeable advantage for users is the fact that they can work in a familiar environment, once a connection to the worldwide network has been established. In the computer science environment such users are called "nomads" or sometimes jokingly "road warriors" as unlike the traditional paper-centric humans they carry all their data - their belongings - with them and are able to work anywhere and anytime. The percentage of nomadic students in the universities is increasing every year.

The first encounter between librarians and such nomads typically happens during their quest for a power socket. While laptops are autonomous systems for a period of time their batteries need to be recharged quite regularly. As in every household, also in most libraries sockets are never where they should be from a user perspective. While recharging their laptops users are confined to their workplace because of the possibility of theft. Unsecured laptops are an easy prey for thieves. Again most public places offer no possibilities to secure laptops, although in most cases, especially libraries, wall attached hooks would be more than sufficient. Such hooks could be used to attach a personal Kensington cable with which a laptop can be chained to its place.

A rather nice alternative can be found in Freiburg: lockers have been equipped with power sockets so that users can recharge their machines while having lunch in the cafeteria. Needless to add that these lockers are under constant human surveillance.

TECHNICAL SOLUTIONS FOR A WIRELESS ENVIRONMENT

User access to the library's data network and possibly the Internet can be offered via network sockets in certain areas or user desks. Most likely during the design of the network attention was given to administrative needs and not to user needs, as laptops were not widely spread. Therefore network sockets are not where they should be, given modern requirements. The cost of reinstalling new network cabling is prohibitive in most cases.

There is a solution to carry data traffic over standard electrical 240V wiring, called Powerline. Powerline modules are relatively small and cheap. All powerline modules on one electrical circuit form a common network with a peak performance of up to 14 Mbit/s. One module is required to connect this network to an existing IP switch. The installation of such modules is straight forward and requires little or no planning. A powerline network corresponds to a classical Ethernet. However, experience shows that the peak data rate is rarely achieved and that electrical interference may seriously disrupt the data traffic. Such interferences come from switching on lights or from a printer or even a computer attached to the same electrical circuit. It is wishful thinking to have the powerline technology incorporated into laptop power supplies. With powerline users are again confined to their desks or cubicles if they want to access digital data, even when their laptop batteries are fully charged. Mobility is lost.

Since about five years wireless IP networks are available. The technology is called WLAN or WiFi and there are several standards. The oldest and most common standard is IEEE 802.11b which operates in the 2.4 GHz range and allows a data rate of up to 11 Mbit/s in one cell. This data rate is shared between all computers in this cell. The new standard 802.11g is fully compatible with 802.11b and offers up to 54 Mbit/s. The 802.11a standard operates in the 5 GHz range and also offers up to 54 Mbit/s. It is expected that laptops will soon understand all three standards; modern machines will at least adhere to 802.11b/g. The maximum energy of a sending station must not exceed 0.1W and is typically around 0.03W. This is in contrast to mobile phones which use up to 2W (in the 900 MHz range). The range of this wireless technology varies. Under ideal circumstances 300m can be covered; in concrete buildings the range may drop to 20-50m. The range can be extended with special antennas and under ideal conditions (across a lake) up to 10km have already been achieved.

In any case the current WLAN technology allows to provide widespread network connectivity in libraries. Relatively few access points suffice to completely cover user work areas as well as the most often used shelf spaces. For best performance the access points should be connected to the network with traditional cables. The most advanced systems connect special antennas via a traditional TP cable to a central management station. There are also access points with a wireless uplink to a central switch as well as access points with powerline uplink. A WLAN based network can therefore be installed very quickly at low cost. This makes it ideal for libraries. The best locations for access points are usually found by trial, based on educated guesses. It should be added that there are specially designed access points and antennas which match special conservational or design needs. It must be pointed out that WLAN is no replacement for proper network cabling. Proper cables allow much higher speeds, offer better security and are almost immune to interferences from external sources.

Bluetooth is another wireless technology which operates in the 2.4 GHz range but it uses the spectrum in a different way. The maximum data rate is 1 Mbit/s and the sender uses less than 0.01W. Thus Bluetooth is ideally suited for devices with small batteries, like mobile phones or personal digital assistants (PDA). However, the range is reduced to some 10m. Bluetooth LAN access points provide the same functionality to PDAs as the WLAN access points do for laptops. Experience shows that both technologies can coexist.

Most laptops as well as PDAs have an infrared interface. The properties of light make such interfaces ideal for point to point communication and a classical application is the direct exchange of electronic business cards. Internet traffic can also be sent over infrared connections with a maximum speed of 4 Mbit/s for each individual connection. Therefore it makes sense to offer infrared access points at certain highly frequented locations, so that users can at least update their personal information from time to time, even if they cannot make use of the options offered by a WLAN network.

Given the right set-up all three technologies can be used in one single network without extra management overhead. It therefore makes sense to provide a WLAN network in a library based on IEEE 802.11b/g and to supplement it with a number of Bluetooth access points and with several infrared access points. In addition a number of network sockets should be offered in cubicles to allow for high bandwidth communication with multimedia servers. Powerline technology can be used as a substitute for cables in areas where performance or throughput are not an issue.

ORGANIZATIONIAL SOLUTIONS IN A LIBRARY ENVIRONMENT

A major topic in wireless networking is security. Many papers have been published on the various loopholes of different implementations. The experiences gained in universities however prove that wireless networks can be securely integrated into an existing environment. Rather than individually connecting the various access points to the production network (the intranet), it is better to set up an entirely separated network in order to interconnect the access points. This network should not have any connection to the library's intranet. While in former times such an approach required a separate cabling infrastructure, today's VLAN technologies can be used to set up a logically separated network at no cost. Network administrators then no longer have to worry about potential security hazards.

This separated network should be connected to the library network outside the firewall (if there is any) or Internet gateway, so that users on the wireless network have the same privileges as any other user on the Internet. Access to the wireless network (including the network sockets open to users) should be made as easy as possible. Otherwise support issues may turn into an overwhelming problem. DHCP servers can supply user machines with IP addresses as soon as they connect to the network. It remains a management issue to decide whether or not this separate network should be directly connected to the Internet. Most University set-ups rely on authentication gateways where userid and password or other credentials are checked before individual connections are enabled.

For libraries it may be a tedious job to authenticate users, which is also unnecessary as libraries are in the same situation as many Internet cafes. Therefore their fairly advanced hotspot technology software for gateways can be used. It allows to issue day accounts or weekly accounts to users "over the counter" with very little administrative overhead, if any. The fee for such an access must not be prohibitive as otherwise people will be scared away from modern technologies for monetary reasons alone.

In a University environment it is wise to integrate the library wireless network into the University's wireless security concept to allow for roaming and to use a separate hotspot gateway for external users. It must be noted that eavesdropping is very easy in wireless networks. It should be left to the users to secure their individual connections. This is done implicitly by many mail clients when they contact their mail server via SSL-protected connections. Most users will be used to setting up an encrypted tunnel (IPsec) to their home institution before they start to communicate. The security of such encrypted tunnels is far better than the security offered by access points; in fact current knowledge suggests that such security is unbreakable.