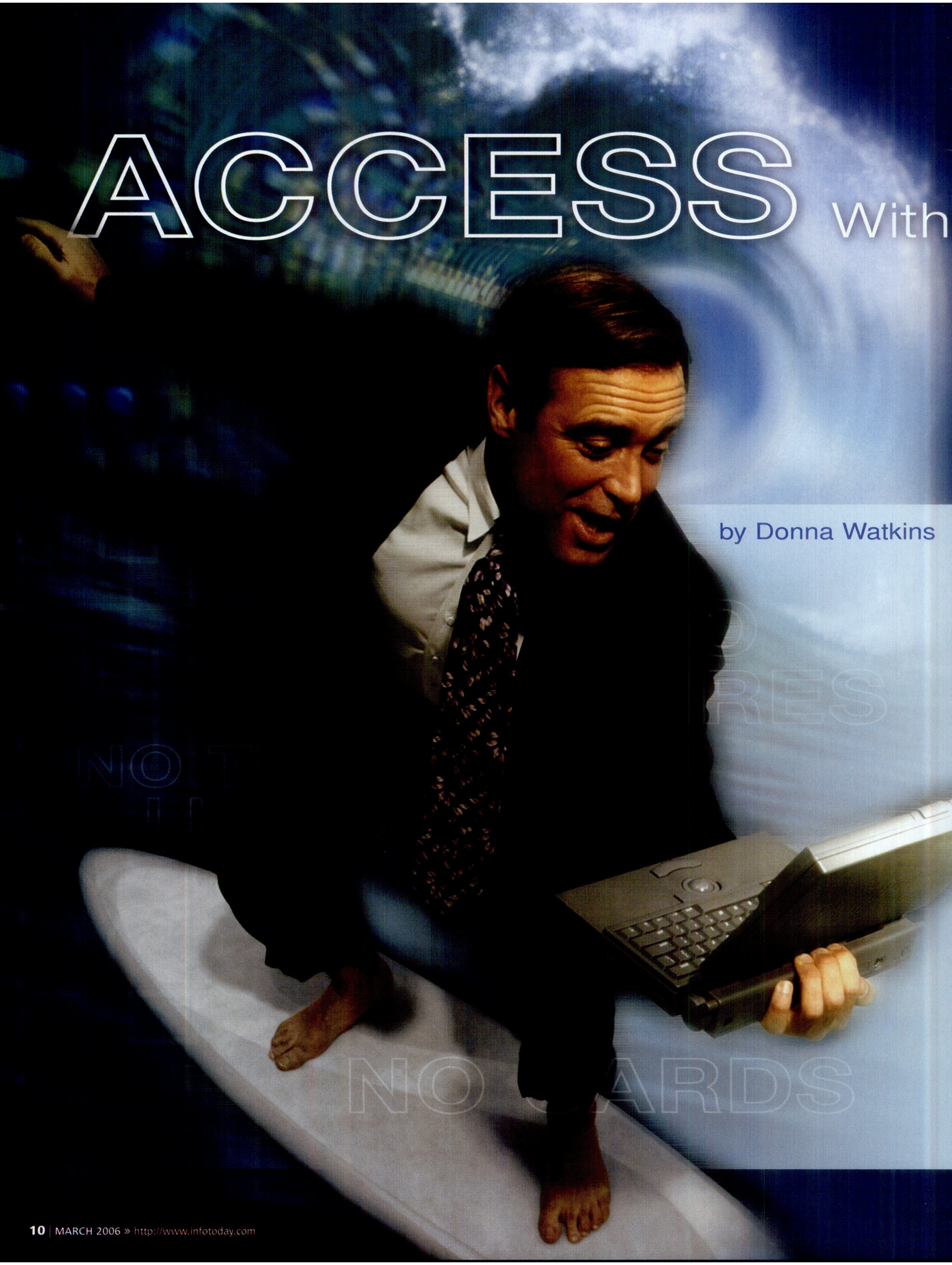
# ACCESS With

by Donna Watkins



# out AUTHENTICATION:

## HOW AND WHY WE LET ANYONE SURF OUR WIRELESS

We welcome all nearby Californians to come surf on our hassle-free wireless Internet service.

Wireless hotspots are popping up in local coffee shops everywhere. Anyone with a wireless-ready laptop or PDA can surf the Internet at one of these hotspots. The same is now true for all 32 branches of the Orange County Public Library (OCPL) in California. As the information services trainer here, I had the opportunity to be involved in implementing wireless access at our branches.

Though many public library systems are moving toward wireless access, most require patrons to have a library card for authentication in order to gain access to an Internet connection. Not so here at OCPL. Anyone with a wireless-ready laptop can come in and utilize the network without having a library card.

Connecting to the Internet with their own PCs allows patrons to do things they can't do on a branch's public-access computers. For example, there is no time limit when using the wireless network. Patrons can surf the Internet all day long without waiting in line or having to worry about when they have to give up their spots to someone else. A patron can also download information to his computer; downloading is not allowed on most branch computers. But with his own machine, a patron can essentially access the OCPL wireless network whenever he wants and download pictures, e-mail, or other documents for further processing at his convenience.

### How the Idea Started

The idea of implementing wireless at OCPL was actually brought forward by several of our branch librarians as a result of patron requests. In October 2004, county librarian John Adams began to discuss the idea with Clyde Gamboa, manager of our information services (IS) department. In January 2005, the IS department began to research the project, and wireless was actually implemented at all branches in July 2005.

As the IS trainer and a member of the IS department, my role in this was to stay informed and to develop a good understanding of the process so that I could assist staff and answer questions when it came time to implement this technology at branches and to offer this service.

### What We Required of Our System and Why

The first requirement for the OCPL wireless network was that it had to be accessible without a library card. This requirement was easily met by setting the wireless access configuration (an option in the software) so that authentication was not required to access the Internet. (However, a library card is still required to use the libraries' proprietary databases.)

Once that decision had been made, we developed a set of additional service requirements. Our service intention was to provide patrons with fast, reliable access without having to check in at the reference desk or log on with a library card. That was then translated into system requirements. The IS department came up with nine system features that it considered desirable, with six of those features designated as must-haves. The process of comparing and converting the service requirements into system requirements took about 2 weeks.

The six must-have system features for our wireless project were a DHCP Server, multiple DNS configurations including DNS forwarding, NAT (Network Address Translation), bridge filtering, a firewall, and the ability to accommodate 25 or more simultaneous users. I'll explain more about them and why they mattered:

DHCP (Dynamic Host Configuration Protocol) is an option in various

»

wireless systems. It allows the system to assign a temporary IP address to a user. This allows patrons to come into the library and access the wireless network without assistance. Without this option, each patron would have to receive an IP address from a staff member. Once DHCP assigns an IP address to a wireless computer user, he can connect to the wireless unit (or gateway) using that temporary IP address.

Another feature of the system is Network Address Translation, which provides a layer of security for the patron while he surfs the Internet. A patron sends a request to the Internet using one IP address. The information is sent back from the various sites to that one IP address. The system then sends the request to the original wireless patron.

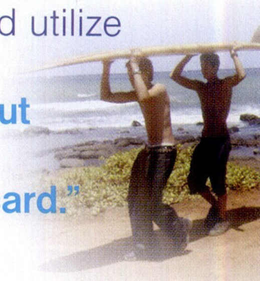
An additional feature of the wireless network that is provided automatically at OCPL is a Domain Name Server Forwarder. When a wireless user sends a request for a Web site to the wireless gateway, this request is forwarded to an already existing OCPL domain name server. This feature allows for faster surfing speeds for patrons.

## Our Security Concerns

There were two basic security concerns in implementing the wireless system at OCPL. IS director Gamboa explained, "We wanted to protect the OCPL network itself and, at the same time, protect unsuspecting patrons from possible unscrupulous users."

To accomplish the first goal, we had to choose a system with a firewall that could be configured to block access to the OCPL network. This way, the patrons would be prevented from accessing any secure data from the OCPL network. The second issue was protecting patrons from each other using a feature called bridge filtering. In a normal network, all users who are logged on to the network can "see" each other and share data and printers, etc. Bridge filtering keeps users from being able to "see" each other and having access to each other's data.

"Anyone with a wireless-ready laptop can come into the library and utilize the network without having a library card."



There are other problems that could render a patron's data less than secure. One can happen when anyone with a little bit of knowledge and a wireless computer sets her machine up to look like a legitimate wireless access point. This is called the "evil twin" phenomena. If a patron inadvertently logs on to the evil twin access point instead of OCPL's legitimate access point, he or she could be allowing the evil twin to steal personal information, such as e-mail and bank account passwords.

One way we've helped prevent patrons from falling victim to an evil twin access point was to publish our service set identifier (SSID). In this case, our network name, "OCPL wireless," is broadcast over the network. When we broadcast our network name, any people who try to pass themselves off as OCPL's legitimate access point by calling themselves "OCPL wireless" are essentially "drowned out" by our wireless access point. (To alert patrons, the IS department created handouts, which the public services staff distributed to patrons when we launched the wireless service.) Unscrupulous people could try to trick patrons into logging on to a rogue access point by calling themselves something similar, such as

»

### TWELVE STEPS TO WIRELESS ACCESS

1. Determine library service requirements.
2. Develop hardware/software requirements based on service requirements.
3. Research vendors and determine which products most closely meet the requirements.
4. Test the units selected on a small scale to determine that they actually perform as claimed.
5. Select the product that best meets your needs.
6. Perform extended equipment evaluation at a test branch.
7. Validate findings.
8. Retest as needed.
9. Create project plan and rollout strategy.
10. Generate patron information handouts.
11. Train staff in using and testing equipment.
12. Execute rollout plan.

"Wireless at OCPL." By only logging on to "OCPL wireless," patrons are additionally safeguarded against logging on to an evil twin.

Clearly, even with security measures in place, patrons need to be aware that information sent through the wireless network is not considered secure. We recommend that they don't send personal information, like e-mail passwords, credit card numbers, and banking information, as is the case when using any public library terminal. The best way to prevent this security problem is patron education and awareness. So we included this precaution in the patron handout about surfing the wireless network at OCPL.

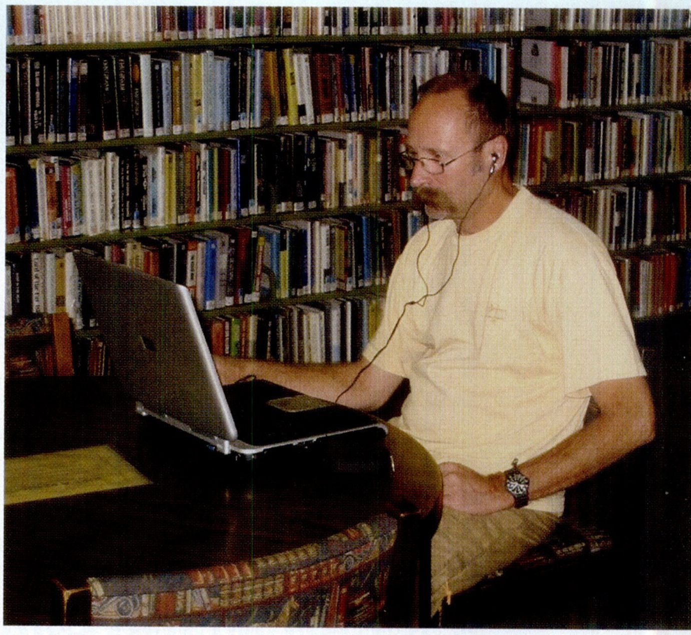
Once we had this list of required features, the IS department began to generate a list of vendors that had a product that might meet our needs. A list of nine products was completed by the end of February 2005, then we chose four products that appeared to meet our requirements most closely. They were HP ProCurve420, Proxim AP-4000, Fortinet Fortigate 60, and SonicWALL TZ170W.

## Testing, Selecting, and Installing in All Branches

After narrowing the choices down, we began a limited testing of the four selected products in our technology lab at library headquarters. After about 12 weeks, we determined that HP and SonicWALL were the two products that met our technical requirements. We chose the HP product because we had an already established relationship of technical support. Then we tried out the HP product at our test branch, Aliso Viejo, and it seemed to be working fine. But we learned a big lesson here, and that was to verify the availability of the product before starting our demonstration tests. When we went to order the device for our branches, we discovered that this specific product was being discontinued.

At that point we decided to try SonicWALL TZ170W at our test branch. After testing for about 3 weeks in May 2005, we verified that the product was working as expected. We decided to purchase and install the devices at the remaining public service branches.

As part of the installation process, the IS staff educated the branch staff by providing customized employee handouts and demonstrating how to test the system to make sure that everything was working properly. The public services department distributed the other handouts for staff to give to patrons. The actual process took about 3 weeks, and we went live in all branches by the end of July 2005. The total cost of materials for this project for all 32 branches was estimated at $19,049, while the number of staff hours to test and install was about 120.



*Mark Litsinger uses his battery-powered laptop and headphones at the Tustin branch.* (Photo by Brandi Solarte)

Unscrupulous people can **try to trick patrons** into logging on to 'evil twin' access points.

## Proactively Managing Patron Service Challenges

At OCPL we have taken a proactive approach to patron services issues by anticipating problems and providing staff with methods of handling them. We anticipated that patrons might expect staff to help them set up their equipment; we discussed this issue and others at systemwide meetings. In order to head off this problem, the IS staff developed handouts to show patrons how to configure their computers.

According to Hilary Keith, manager of the Aliso Viejo branch library where we did our testing, "Most of the users are pretty savvy. The main problems occur when patrons haven't been able to configure their computers correctly. We test to make sure the wireless network is working and though we can't configure their computer, we give them what we have and usually we can help them."

But staff are not having much difficulty assisting patrons who use the service and, said Keith, "The patrons love it."

## Early Problems and Fixes

An initial problem that we encountered had to do with an extra product feature that was not part of our requirements. This additional feature allowed the product to be turned on and off. A problem arose when we realized that although the product shut itself off as planned after branches closed, sometimes the device did not turn itself back on in the morning. There was no way to predict when or at which

continued on page 50 »

« continued from page 14

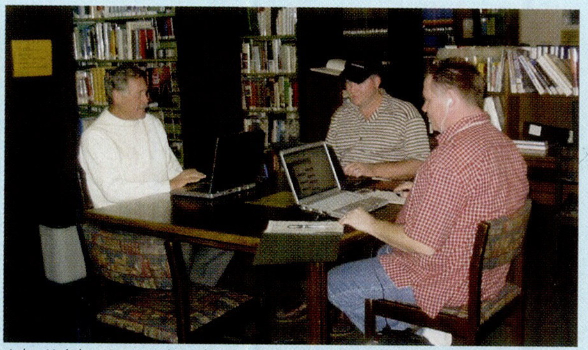
branch this would happen. Branch employees had to call the IS staff at headquarters and ask to have the system restarted. The solution to this problem was to disable the feature and allow the system to be on all the time.

Though most branches did not report many problems, patrons at the San Clemente branch were not able to log on to our access point. After some investigation, the technician assigned to that branch discovered that a wireless signal coming from a company across the street was actually conflicting with our access point. To solve this problem, we simply changed the channel that we were broadcasting from.

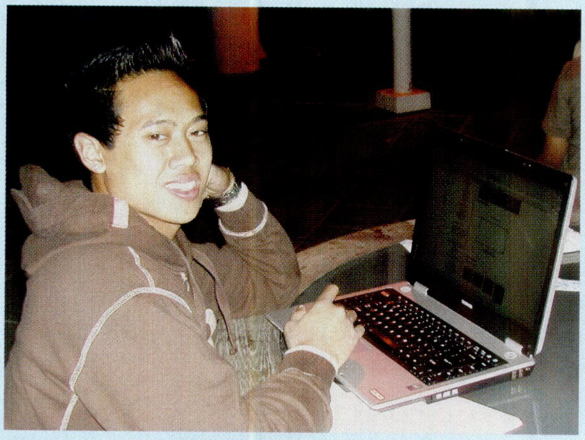
Another difficulty that branch staff members have encountered is not having enough electrical outlets for patrons to plug their laptops into. This is especially true at some of the older branches, for example the Tustin Branch Library, which was built in 1974. This feature will be taken into consideration for our newest construction project, Irvine's Wheeler branch, which is scheduled to be built by June 2007.

## Conditions Are 'Epic,' Surfers Are 'Dialed In'

Aside from the problems mentioned, the project, which has been up and running since July 2005, seems to be progressing smoothly at most branches. Though we don't keep statistics, staff members are noticing patrons frequently using laptops to surf the Internet through our wireless network. La Habra's branch manager, Jill Patterson, said, "It's going well. Half the time we don't even know patrons are using it. The only time we know for sure that it is being used is if it's not working. In that case the procedure for fixing it is usually pretty simple."



John Knight, Ken Reed, and Tim Bittner crowd around a table with an electrical outlet to use the wireless at the Tustin branch of OCPL. (Photo by Brandi Solarte)



Jaymie Tumaliuan takes advantage of the free wireless Internet service in the outdoor atrium at the Aliso Viejo branch of OCPL. (Photo by Hilary Keith)

Tustin branch adult services librarian Tim Scott also noted, "It's a great service and it relieves the regular Internet stations so that people who truly have no other way to access the Internet can use these stations."

The response from patrons is positive as well, as noted through staff observation and patron comment. According to Flora De-Asis, a wireless user at the El Toro branch, "It's a wonderful service and I appreciate it very much. I like it because there is no time limit and often the regular Internet is full."

How does offering wireless access points to *anyone* (with or without a library card) support the mission of the public library? According to our county librarian, John Adams, offering wireless access to anyone is very much in line with our mission. Adams said, "The basic mission of the public library is to provide information and access to our educational and cultural heritage to the public. Obviously for a number of years now electronic information has been a crucial part of that mission in addition to our traditional modes. The wireless installation is only a further extension of that."

All materials for our 32 branches **cost less than $20,000.**

Adams continued, "It was a response to a request from a number of library users. It's actually a financially beneficial way for us to meet our objectives. In literally every branch we have, the demand for Internet access at a computer exceeds the supply we have available. This way folks can come in with their own PC. They can take advantage of the network we offer but we don't have to add another PC and get wiring to it. It was never really an issue whether or not to make access available to the network with a library card or not. We already allow access to nonresidents so there is nothing inconsistent about that."

Our intention is to continue to provide this service and to monitor the system to ensure that it is up and running efficiently at all branches.

*Donna Watkins works for the information systems department as the information systems trainer at Orange County Public Library in California. She is responsible for assisting staff in using and explaining new technology so that they can better assist patrons. Watkins holds an M.L.S. from San Jose State University in California. Her e-mail address is DJWatkins@ocpl.org.*