ENTERPRISE NETWORKS & SERVERS
A chronicle of information for networks and servers in the enterprise
CISCO • 3COM • Juniper • Nortel • Foundry • F-5 Networks • Lucent SUN • HP • IBM • UNISYS • DELL • SGI

Search
Go

The magazine
This month's issue
Previous issues

More articles
Industry news
OpinionWire
TECHwatch
ARS Analyst Outlook

Resources
Book chapters from Cisco Press
Media kit
Contact us

Subscriptions
Subscription center
Free 3-month trial
Free e-mail newsletter
E-mail unsubscribe

Links
Unisys World magazine
Serverworld back issues
Enterprise Networking Magazine back issues

December 2004 issue

Education

Published by: PCI

Use the Right Wireless Tool for the Job at Hand

By Ken Chipps

Wireless networks (or wireless additions to existing wired networks) are being deployed every day. This is one of the active areas in an otherwise uncertain technology market. With all of this activity many new standards are constantly arriving on the scene. A common question asked is: Which method should be used where?

WiFi (short for "Wireless Fidelity," a wireless networking standard that uses high-frequency radio signals to transmit and receive data at a theoretical rate from 11 to 54 Mbps) is the most familiar system, so many users attempt to use it for everything. But WiFi is not designed — nor is it suitable — for most uses outside of a local area network.

The differences in the various systems are most easily explained by discussing them in relation to the size of the area best covered by each. Any system can be adapted for use in other areas, but each one works best when left in its natural environment.

The first type of use is a LAN, which is a network in a single building or several floors of a single building. WiFi systems utilizing the various IEEE 802.11 standards (802.11a, b, and g) were designed to operate in this environment. With WiFi-certified equipment a wireless onramp to an existing wired LAN can be added.

The main problem with a radio frequency wireless connection is signal containment. With proper network design the signal can be mostly contained inside the building by locating access points properly and by adjusting the power output levels of the access points. As the signal cannot be contained entirely, however, security of the information transmitted is also a concern. This problem can now be overcome with the WPA2 and 802.11i standards that have been approved, although doing so adds an administrative burden to the network management staff.

A campus area network (CAN) connects one or more LANs in buildings within easy walking distance. One way of connecting these buildings is to lay fiber optic cable. Doing so requires the purchase of switches with fiber ports. When you total the cost of the installation, the fiber-port-equipped switches, and the time it all takes to install it all, however, it becomes clear that this is a high-cost connection method.

The same equipment used in wireless LANs can also be deployed in bridge mode to connect buildings in a CAN. This is done by changing the antenna from one that's omnidirectional to one that's directional. The idea in changing the antenna is to restrict the signal to just the area between the two buildings. There are several problems with this method.

First, the radio-frequency signal can never be completely contained. A radio frequency signal, no matter how well the antenna is designed, will leak its signal to each side of the point-to-point connection, behind each antenna, and for quite a distance behind the other end of the connection. This makes security very difficult. The only way to secure this type of connection is with the addition of add-ons, such as a VPN (Virtual Private Network).

Second, the frequencies used for these connections are commonly unlicensed. By using an unlicensed frequency you open yourself up to interference from everything from portable telephones to someone else's wireless network. Finally, the theoretical data rates are typically one half their stated 11 to 54 Mbps rating in actual practice, due to the network access control overhead this type of system requires. Actual speeds are more on the order of 5.5 to 24 Mbps.

A better solution for a CAN link is a Free Space Optics (FSO) connection. This type of wireless system uses a highly directional, high bandwidth, and inherently secure link between the two points. A good example of this type of system is the Canon Canobeam DT-110 that we currently have deployed to connect two buildings at DeVry University-Dallas. At 475 feet this is a high-speed, all-weather link. The Canobeam DT-110 offers a wide range of data speeds from 25 Mbps to 156 Mbps; the Canobeam DT-130 offers 1.25 Gbps for Gigabit Ethernet networking at up to 3,280 feet in distance. Even higher speeds are possible. Installation took about three hours, compared to several days for a fiber optic cable connection. Security is inherent in the tight beam pattern produced by the unit.

The students in the Network and Communications Management program at DeVry University-Dallas use the Canobeam unit for lab experiments. Data flows seamlessly at Fast Ethernet speeds between the two buildings. This equipment and the link itself have proven to be easy to use and highly reliable. Even new students find this equipment easy to set up and manage.

The final type of wireless network is a metropolitan area network (MAN). This type of network covers an area that one can drive to and back from in a short amount of time. WiFi systems have been used in their native mode as well as in adapted forms to provide point-to-multipoint coverage for MAN networks. An example of this application is a Wireless Internet Service Provider (WISP).

The students at DeVry University-Dallas are deploying 802.11b-compliant equipment right now to create a WISP. The main challenges they are seeing with this initial set-up are similar to those seen when it is used as a point-to-point bridge connection. These problems include interference from other systems, the inability of the WiFi protocols to deal with long distances, and hidden nodes. When using unlicensed frequencies as WiFi does, interference is to be expected. There is no way to avoid this problem.

Timing problems limit the distance over which a WiFi-based link can be maintained. WiFi in a LAN uses the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) method to control access to the network. This does not work well in a MAN environment when each node cannot see all of the other nodes. The timing and hidden node problems can be overcome by moving the system away from the WiFi standard to a proprietary system. Doing this raises costs and reduces interoperability. It does not eliminate the interference problem.

A better solution for the MAN is WiMax, the name given to the IEEE 802.16-based solution that's just now arriving on the market. Unlike 802.11, the 802.16 systems are designed for deployment in an MAN. In their initial deployments these systems will use licensed frequencies to deliver high-speed signals over a wide area. Speeds up to 75 Mbps over 30 miles are possible.

This system can support fixed users now and mobile users soon. Unlike the limited spectrum available for the unlicensed 802.1b1 WiFi systems, WiMax users will be able to select from a range of licensed frequencies.

Using the right technology for the job at hand is critical at this time. The radio-frequency based WiFi and WiMax systems are both useful when used in the right kind of network. They are risky when misused. For high-security, high-speed, campus connections, laser-based FSO equipment is a better choice. Likewise, for high-security, high-speed metropolitan area connections WiMax 802.16 systems are a better choice. WiFi 802.11 systems work quite well in the environment for which they were designed, the LAN.

Ken Chipps is an Associate Professor at DeVry University-Dallas. He can be reached at www.chipps.com.

This article appears in the December 2004 issue of Enterprise Networks & Servers.

Order reprints of this article

Other articles in this section

- **The Missing Link**
- **View all articles in this issue**

Home • Contact us • Subscriptions