INDOOR WIRELESS NETWORKS IN GOVERNMENT

Outdoor networks dominate the news, but indoor wireless networks, too, play an important role in increasing government service effectiveness. In a September 2006 Larstan Business Reports survey, 60 percent of state and local government executives surveyed have at least one wireless hotspot, while 33 percent either already provide wireless coverage throughout the building or plan to within the next year.

Unlike wireless hotspots in lobbies, pervasive indoor wireless networks provide connectivity throughout an entire building for employees and visitors using wireless laptops, personal digital assistants (PDAs), and IP phones. “We have an opportunity to mobilize workers within the workspace,” says Ben Gibson, director of mobility solutions marketing, Cisco Systems. “When government employees have real-time access to information, they can collaborate more effectively and make more informed decisions.”

SECURE GUEST OR CONTRACTOR ACCESS

Government consultants or contractors need network access, challenging IT groups to protect confidential government or citizen information. With a pervasive indoor wireless network, the IT group can create a special guest VLAN, or “network within a network.” When contractors log on, they are authenticated and then segmented from the rest of the network. Wireless instead of wired access for contractors can also reduce costs. For example, contractors can move to other office space without network moves, adds, and changes, which typically cost government more than US$75.

REDUCING CELLULAR MINUTES WITH VOICE OVER WIRELESS

Governments that build indoor wireless networks can use them for new services that improve government effectiveness, such as voice over wireless, which was identified as a benefit of an indoor wireless network by 43 percent of Larstan survey respondents. The disadvantages of indoor cellular phone use are high cellular costs, poor reception—especially in buildings with metal walls—and the time spent monitoring two voice mailboxes, one for the office phone and one for the cell phone.

With voice over wireless, employees can place and receive calls from anywhere in the building or campus, including adjacent outdoor areas such as walkways and patios, using wireless Cisco Unified IP Phones, or laptop computers or PDAs with voice software. With new “dual-mode” phones that can connect to either a cellular or wireless network, employees can use the same phone and phone number for network-based calls from government offices and cellular calls in the field.

In April 2006, Forrester Research estimated that mobile workers can eliminate an average of 30 cellular minutes per week by replacing their cellular phones with wireless IP phones used on a pervasive indoor wireless network. This is typically enough to save $10 to $20 on a calling plan, resulting in monthly savings of $1,000 to $2,000 for an agency with 100 mobile employees.

LOCATION-BASED APPLICATIONS

Locating moveable agency assets, such as laptops, can drain productivity in government environments. In fact, some agencies routinely over-purchase certain assets in hopes that they can quickly locate one when needed. A pervasive indoor wireless network with a location appliance can be used to locate any wireless-enabled laptops or PDAs, as well as any other asset with an attached RFID tag. Government agencies that need to track the location of people, such as visitors to secure areas, can provide them with RFID.
badges. “Using RFID badges, governments can confirm that visitors remain with their escorts, or that an employee leaving with a laptop is authorized to exit the building with that laptop,” says Gibson.

ADVANCED SECURITY

Well-meaning employees often install low-cost, consumer-grade wireless networks in their departments, without IT sanction. But few of these “rogue” wireless networks provide even basic security features such as encryption or intrusion detection. Risks include the exposure of confidential information or network infections that can interrupt the continuity of government service. The Cisco Unified Wireless Network solution actively monitors for rogue wireless networks, as well as for known virus signatures and anomalous network behavior that can signal an attack.

A LAUNCH PAD FOR OUTDOOR WIRELESS

“The benefits of indoor wireless networks are amplified when governments use them in conjunction with outdoor wireless services for public safety personnel and mobile workers,” says Brian Grunde, senior manager for state and local government industry solutions, Cisco Systems. “With wireless access both indoors and outdoors, governments can become more responsive to their constituents and increase efficiency across administrative, public safety, community development, and other functions.”

Cisco indoor and outdoor wireless networking solutions can be managed as a single solution, providing the integrated security required in government environments. For information about the Cisco Unified Wireless Network solution, visit www.cisco.com/go/wireless.

For information about Cisco outdoor wireless mesh network solutions, visit www.cisco.com/go/wirelessmesh.

To learn more about Cisco solutions for local government and public safety: www.cisco.com/go/localgov.