Switch to **Speed** and **Simplicity**

A growing number of "carpet environments" — company main offices and branch/remote offices — are following the lead of "white-tile environments" — hospitals, retail, manufacturing and other vertical markets — in deploying 802.11 (Wi-Fi) wireless local area network (WLAN) service pervasively throughout their locations.

"You now have a workforce generation used to being mobile, to having wireless connectivity for handheld and notebook devices," Ben Gibson, director of mobility marketing, Cisco Systems Inc., points out. "Mobilizing workforces has become an employee satisfaction issue."

Rather than use enterprise-oriented wireless access points (APs), small- to medium-sized businesses (SMBs) are turning to wireless switches, also called wireless controllers — from such vendors as Cisco, D-Link, Linksys and 3Com, among others — along with lower-cost "thin" or "right-sized" access points, to deploy and manage pervasive wireless service quickly, securely and cost-effectively.

In addition to standard features of wired network switches, wireless switches incorporate additional software to manage wireless network traffic, security functions and central control of the access points' radio frequency (RF) channel settings and power. This is important, says Craig Mathias, principal at technology advisory firm Farpoint Group. "Otherwise, if you plug an AP into a regular wired switch, the switch won't know what it is."

"With wireless switches becoming more cost-effective to deploy and use, it makes sense for SMBs to consider them if they have anything over three or four APs," says Rohit Mehra, director of product management, wireless solutions, 3Com Corporation. "This gives you a single point of control and management, rather than having to manage each access point."

Wireless switches for SMBs and remote/branch offices include D-Link's 1008 Wireless Switch and DWS-3200 Series Wireless Switches. As with offerings from other vendors, D-Link's solutions support both wired and wireless service. And customers select how many access points they want to license the wireless software for.

For example, D-Link offers 10-AP and 25-AP licenses for the DWS-3227 and DWS-3250 Wireless Switches, according to Jennifer Wu, director of product management for switches, D-Link Systems. "Licenses can be shared among »

Wireless switch technology can cost-effectively ease your wireless network deployment, while offering better security and support for future applications.

multiple switches and the switches can be anywhere in the network, so you can create a virtual switch managed through one interface." Similarly, Cisco's Catalyst 3750G Switch includes embedded WLAN capability to support 50, 100 or more access points.

Companies looking to add support for up to six access points to an already-installed Cisco Integrated Services Router (ISR) can use a Cisco 2800 or 3800 Wireless LAN Controller Module. "The ISR is a secure modular router designed for smaller businesses and branch offices," says Cisco's Gibson. "There are over three-quarter of a million ISRs in use around the United States." Cisco also offers its 2006 Wireless LAN Controller, a standalone controller that connects to a router or Ethernet switch and supports up to six access points. "And you don't need to deploy a controller at every location — you can manage your APs remotely and securely," Gibson notes.

3Com's wireless switch products include the WXR100 Remote Office Wireless LAN Switch, supporting up to three APs, as well as switches supporting up to 12 or 120 APs for larger offices. All of these companies also offer 802.11 access points. While access points from different vendors should interoperate and provide such basic wireless features as authentication, capabilities like management and auto-configuration will require switches and access points from the same vendor.

"Businesses are looking at a centralized wireless network architecture, instead of traditional access points," confirms Kaushik Ramachandran, product manager at CDW. "By putting the intelligence into the switch, a company can add a thin access point, let the switch configure it and the AP starts working. And most of the new wireless switches support Power over Ethernet, which means that the APs don't need power lines installed by licensed electricians, further reducing the time, cost and complexity of deploying WLAN service."

Simplicity is a big selling point for SMB IT and network managers. "Large enterprises can afford a network operations center and IT help desk. Most SMBs have to look more for ease of use," says Farpoint's Mathias.

Easier Deployment and Management

The ability to automate many of the access points' parameter and configuration settings through the centralized wireless switch not only saves time but results in a more optimized wireless environment, points out 3Com's Mehra. "For example, if your company has eight or ten APs in its location, when you configure all of them, you want to make sure there is minimal interference in the channels you're going to use. The channel and power control are two of the key attributes that a wireless switch manages very well, versus a traditional wireless installation like a wireless gateway, which could handle access settings but not help with the configuration, channel or power settings in the APs."

"If your WLAN controller can do real-time RF management, the system can do things like automatically adjust the power output of one AP when another goes down, boost power if there's interference or move users from one cell to another to load-balance," says Cisco's Gibson. "That's important, for example, if you have hundreds of users at a conference center. These things all promote a higher level of wireless performance and reliability."

"The more RF cells of wireless coverage you need to deploy and manage, the more a wireless switch approach becomes attractive to provide central management, versus managing multiple cells of coverage. This lowers the cost of ownership," says Manju Mahishi, director of product management for the wireless infrastructure division at Symbol Technologies.

Wireless switches can simplify the planning and placement of access points, using software offered by many of the wireless switch vendors, as well as third-party programs.

"When you had independent APs, [such tasks as] doing a site survey and determining what channels you'd assign so adjacent APs wouldn't interfere with each other would require a lot of work," says Cisco's Gibson. "With a switch-based wireless architecture, we've dramatically simplified and automated a lot of this. You can load maps, and when you deploy an AP, it can go into scan mode."

"[3Com's] Wireless Switch Manager planner tool recommends what APs to use, how many and where to put them to get the best signal across your floors," says 3Com's Mehra. "It also takes into account expected traffic loads; for example, if you have a conference room, you can indicate heavy traffic areas."

"Many remote offices have little or no IT expertise onsite, so remote management is critical," says Symbol's Mahishi. "If you're planning to manage dozens or hundreds of wireless switches and APs, especially if they're spread out through many regions, centralized management and a lot of auto-update functionality is essential."

Wireless switches are also adding security features that previously required separate appliances. These include unauthorized or rogue access point detection and intrusion detection/prevention, for example, the ability to "shun" — de-authenticate, and not pass traffic — for rogue access points or for users attempting to send Denial of Service (DoS) attacks or other inappropriate traffic, whether deliberately or due to spyware or virus infection. Other common security features in wireless switches include the WPA (Wi-Fi Protected Access) and WPA2 authentication mechanisms, and the option of having different service set identifiers (SSIDs, or the network's "name") for different virtual LANs, which simplifies policy enforcement.

More Wireless Service, More Wireless Applications

In addition to speeding and simplifying the deployment of current applications, these new affordable wireless switches make it easier than ever for SMBs to deploy Wi-Fi service and Wi-Fi-enabled applications, such as Voice over Internet Protocol (VoIP) over Wi-Fi.

VoIP over Wi-Fi lets sales staff, technical support, maintenance crews and other employees conduct untethered phone conversations without running up costly cellular minutes, using VoIP or dual-mode (Wi-Fi/cell) handsets or wireless-enabled handhelds.

Supporting real-time, latency-sensitive applications like VoIP in a wireless environment requires not only Quality of Service (QoS) features, but also the ability to minimize or avoid delays as employees roam from one access point's coverage to the next.

Notebook users aren't likely to be moving around while they work wirelessly, but VoIP and handheld users are. For roaming users, "today's wireless switches are designed to allow users to roam not just from AP to AP, but also among virtual LANs and among sub-nets," says 3Com's Mehra. "This keeps your call authenticated and connected, so voice quality won't suffer. Traditional APs don't provide for that."

Many wireless switch vendors, along with mobile device makers, are beginning to add support for the Wi-Fi Alliance's WMM (Wi-Fi Multimedia), which is based on the 802.11e standard. "WMM offers a structured way to provide QoS over wireless," Symbol's Mahishi explains. "Each access category is given a priority level — for example, VoIP is always given first priority and video second, while print jobs might be third and Web surfing fourth. While you can never guarantee service, WMM makes sure that VoIP packets are sent out at the highest priority."

Other features to help SMBs optimize Wi-Fi service for VoIP users includes 3Com's new Call Admission Control (CAC), says 3Com's Mehra. "CAC assesses the VoIP load on the AP, and allows the network administrator to set limits like how many voice users will be allowed — the N+1th user will be connected via an adjacent AP for load-balancing."

Plan for Growing Use of Mobility

With the dramatic increase in mobile and remote operations by businesses of all sizes, the experts agree on one mantra: Plan ahead.

"Plan your capacity for today and tomorrow," stresses Farpoint's Mathias. "Be sure to survey your users as well as the site. Understand the current workload and how many users are doing what, in what locations. Also, guesstimate what the future workload will be, when more will want to use wireless service for voice and video as well as data. Make sure that your cabling will support Power over Ethernet — most of your access points will use it and most wireless switches will have it. And don't just buy 802.11g equipment — buy APs that support 802.11a, b and g."

"Even if you don't have mobility apps rolled out today, you know that more Wi-Fi-enabled clients will be coming, so be ready to provide that coverage," says Cisco's Gibson. ◊