

Thin Access Points Ease Wireless LAN Administration

As thin wireless technology gains prominence, small business finds advantages coming its way.



Most enterprise wireless LANs evolved from just a few “fat” access points (APs) originally installed to support the occasional notebook user in meeting rooms or places where wires were difficult to run.

Today, wireless networks have evolved to accommodate critical business applications and incorporate solid security and management measures. There’s no question, wireless networking is getting easier and more affordable for all — including small businesses.

Along with this proliferation comes the job of managing independent or “fat” access points located throughout the office. This is a tedious job at best and one that can lead to a myriad of problems simply because fat access points must be managed one at a time.

Wireless systems manufacturers have recognized these issues and responded with the advanced design of “thin” access points that move all or some of the intelligence originally incorporated in each access point to a central management server.

Fat vs. Thin Architecture

This consolidation brings the full suite of functions including security, access control and segmentation into a single management console, making configuration and updates more convenient — and in some cases, making them possible at all.

In the previous architecture, each fat access point carried all the intelligence. If a building had 80 access points, network administrators wanting to put in a new security policy had to install the policy in all 80 access points, says Matt Barletta, director of technical marketing for Cisco’s wireless networking business unit.

In the new architecture, administrators just have to make a change in the controller and the new security policy is automatically pushed to every access point. As a result, access points are easier to manage, reducing the chance for errors.

“The thin access points and controllers are acting like one big unit,” Barletta says. “Think of it as a system where the access points are just arms on the controller and they are connected virtually through tunnels on the network.”

Controllers are smart and can automatically adjust configurations to maintain optimal network performance, he adds. For example, if a thin access point goes down, controllers are smart enough to increase the power output of a neighboring access point to cover for the failed access point. If controllers detect interference, they can automatically change channels on affected access points to avoid the interference.

Thin Access Point Pluses

The small business deploying a thin access console can benefit from a host of advantages that come from having a single point of control including:

- The centralized management and deployment of security policies provide consistency and current updates.
- The console monitors all access points and can detect rogue devices so they can be blocked or removed.

- Access can be rerouted to alternate access points if one access point fails.
- Handoff of access for users roaming between access points can be handled faster because of centralized intelligence.
- The architecture of the WLAN (wireless LAN) can be revised as necessary (depending on the product) to accommodate changes in enterprise requirements.

Another benefit is the ability for users to roam throughout a building, from access point to access point, without getting disconnected and having to reauthenticate with each new access point, says Rocky Rosas, D-Link’s senior technical marketing manager.

“Normally you have to reassociate with another access point, which could result in receiving a different IP address and an interruption in applications being run,” he says. “If you have a controller-based system, it’s more like a cellular network. You can roam the building and not lose connection.”

The new architecture also reduces the load on your authentication server, Rosas says. In the past, each individual access point authenticated users with a RADIUS (Remote Authentication Dial In User Service) server. Now, all the authentication requests can be efficiently aggregated through a controller.

These advances combine to deliver a more manageable environment, and bring the wireless LAN closer to the wired LAN in terms of security and ease of management.

Combined Throughput Capacities

Fat access points don’t rely on a centralized console, and provide access to the computing resources like servers and data stores through wired LAN connections. While this older design imposes management issues, it leaves maximum bandwidth available for data traffic since management and control functions are local to the access point.

When thin access point technology moves the management control to the central management console, management traffic from each of the access points travels across the network. And, depending on the configuration of the wireless LAN, not only management traffic, but also data traffic may flow to the console.

For wireless networks based on current standards (802.11a/b/g), throughput speeds are significantly below the capacities of wired LANs that transport the traffic between access points and the management console. That means the increased traffic generated in a thin access point architecture is not likely to introduce significant overhead to the network and interfere with actual data traffic at those Wi-Fi speeds.

Rashna Alahwat, research director with Gartner Group, believes the marketplace is driving the design of the new architecture. “Vendors are designing their products to fit specific market segments.” In particular, thin access is defined differently by different manufacturers, and a given product can be configured in a variety of ways in order to optimize the network design.

This flexibility means that while it may be technically possible to saturate a controller with traffic from a large number of high-speed access points, it is also possible to avoid overload by »

assigning various management functions back to the access point, blurring the lines somewhat between thin and fat access points.

According to Alahwat, "Thin access only means what the vendor defines it to be." The differences in architecture are less due to technical constraints than to the vendor's marketing plans, and fitting the product to the marketplace.

Moving Toward the Standard

The final ratification of standards around which wireless LAN products are built has a significant impact on the deployment of products designed around the standards. In the case of thin access point technology, the access points themselves are at issue rather than the consoles that will control them.

Wireless LAN deployments are still based largely on the 802.11b and 802.11g standards with 802.11a being implemented as needed for higher bandwidth applications.

Gartner's Alahwat recommends businesses thinking about upgrades to their wireless infrastructure consider the normal lifespan of networking equipment. At this time, firms should only implement technologies that are formally ratified — 802.11a/b/g — avoiding the yet-to-be-finalized 802.11n products.

"Gartner's recommendation is to stay with the current standards for wireless LANs," says Alahwat. "The 802.11n technology is likely to be widely available some time late in 2009, and we normally recommend a three- to five-year life for network gear." That would make the timing of an upgrade of an existing wireless LAN to the 802.11n standard right in line with availability of products.

Steve Brannigan, president of Cyanline, a wireless security consultancy in Eatontown, N.J., looks forward to a formal ratification of a thin access point specification. According to Brannigan, the current draft specification addresses many issues that are currently delaying deployment: "Enterprises would like to implement the thin access products, but without interoperability they are locked into one manufacturer."

Brannigan says that the current draft contains provisions that would let products from different vendors work together on the same network. However, while having the option to mix and match products from a variety of manufacturers offers flexibility, most businesses standardize their network equipment around one manufacturer. The advantage of being able to add another vendor's product to the wireless infrastructure may be lost if administration functions are not perfectly compatible.

"The old fat access points will still need to be replaced because they weren't designed to talk to the controller and take orders," he says. "That means replacing the whole set."

Products to Fit the Architecture

For its part, NETGEAR has recently announced the ProSafe Smart Wireless Switch, WFS709TP. Designed for small- and medium-sized companies, this full-featured wireless controller delivers enterprise-class connectivity and secure wireless LAN functionality by providing companies with the ability to configure, control and manage up to 48 wireless access points across the wireless infrastructure.

3Com's Wireless Access Points 7760 and 8760 are specifically designed for the small business market and offer built-in migration paths that allow firms to install the products as standalone, or fat access points for very small deployments. And they can seamlessly transition to thin architecture by adding the company's Unified Gigabit Wireless PoE Switch.

According to 3Com's wireless product line manager Alan Miano, the 3Com Unified Gigabit Wireless PoE Switch was designed specifically to address the needs of small- to medium-sized businesses when planning a migration from fat access point architecture to thin network architecture. "The 3Com switch comes with 24 wired ports of Gigabit Ethernet. Each port includes full Power over Ethernet (PoE) and a 24-port wireless management console."

PoE support allows organizations to deploy devices that can accept their operating current through the Ethernet cable rather than requiring AC current and adapters. Wireless access points are prime examples of PoE-enabled devices. The technology allows access points to be located wherever an Ethernet cable can reach.

In addition, the 24-port access point management console allows organizations deploying the device to simply turn on the management function at the console, converting the 3Com 7760 and 8760 access point devices from fat architecture to thin architecture without having to replace the units.

"The 3Com Unified Gigabit Wireless PoE Switch is priced competitively with other 24-port Gigabit Ethernet switches. However, we've included the 24-port thin access point management functions at no additional charge. Competitive products sell the management console as a separate device," Miano adds.

D-Link recently released its first wireless controller, the D-LINK AirPremiere MobileLAN DWS-1008. The wireless LAN switch is optimized for deployment in the small- and medium-sized enterprise environment.

Every CDW account manager
is backed by a team of
LAN/WAN specialists
extensively trained in the latest
technologies and services.

The DWS-1008 is designed to allow easy user installation and operation yet support advanced wireless switch features such as secure mobility, policy enforcement, as well as Administration, Authorization and Authentication (AAA) and 802.1x offload capabilities.

Cisco offers thin access products that incorporate its Unified Wireless Network (UWN) management functions. According to the company, products such as the Cisco Catalyst 3750G switch include UWN and make overall management easier for administrators.

Cisco's spokesperson, Chris McKie points out that "Thin access delivers improvements in packet handling within the switch, providing better performance for Voice over Internet Protocol (VoIP) and other latency-sensitive applications."

McKie points out that many customers still have fat access point technology deployed. "Some people will be fine with the current network, but new implementations and upgrades will want to go with UWN architecture in order to get the advantages of the new features," he says.

Those new features allow advanced mobility services to be more easily deployed. For example, enterprises are increasingly using wireless networks to enable asset location tracking, Voice over Wireless LAN (VOWLAN) and to segment guest wireless access from the enterprise computing environment.

WLAN Size Main Determinant

Using a central management console to consolidate access point administrative activities is an answer to a significant issue for organizations struggling to maintain network security and availability. However, replacing a small number of older, fat access points with an equal number of thin access points and adding a management console may be overkill for some smaller organizations.

The new architecture makes sense with a network with three access points or more, Cisco's Barletta says. "If you need a single AP in an office, just program it standalone. But if you have six in an office, centralized [control] makes the most sense," he advises.

Cisco has loaded its access points with the Lightweight Access Point Protocol (LWAPP), the latest thin AP draft specification from the Internet Engineering Task Force (IETF).

The new Cisco Wireless Express Mobility solution is specifically designed for small and medium-size businesses to cost-effectively deliver business-class mobility, standards-based security and streamlined management.

Thin access technology is the way to go for any organization planning to grow beyond just a few access points. Planning ahead, and buying products that can deliver both present and future functionality, is always a best practice. Fortunately, it's possible to make those kinds of decisions today. ◇

