

Centralized Wireless LAN: Thin vs. Fat Technology

By Jeff Davis

Centralized wireless local area networks (LANs) are quickly becoming the preferred deployment architecture among organizations looking for secure, scalable, performance-based wireless access. Centralized wireless LAN (WLAN) vendors are offering cost-effective "thin" access points (AP) that rely on wireless controllers for advanced intelligence, superior security and centralized management. The feature sets and functionality that enterprises are looking for are located in the wireless controller, rather than the access point itself.

In addition to gaining the benefit of robust features, IT administrators are finding that a centralized WLAN architecture is far easier to deploy than traditional individually configured "fat" access points that contain all the intelligence in each access point. As we discuss the characteristics of each type of WLAN, you'll begin to see how they differ and why centralized architecture is gaining rapid market share.

The underlying IEEE 802.11 functionality is very similar for both centralized and traditional wireless architectures. Both have support for access points using 802.11b/g (2.4 GHz) and 802.11a (5 GHz). The main differences are how each handle security, RF (radio frequency) management, performance and scalability. Total cost of ownership is another factor to consider when selecting the right wireless deployment. The wrong architecture could become an administrative, as well as, a financial burden.

WLAN Architecture Overviews

Traditional wireless LANs use decentralized fat access points that perform all the network processing and functionality in each unit. Manual configuration of each access point is required to set the power level, channel, security and other configurable parameters. Each access point is individually configured to connect to the network and often deployed in the ceiling throughout the facility. Due to security concerns, virtual LANs (VLANs) are typically configured to segregate the wireless network from other internal trusted networks. Third party software solutions are often needed for additional

Ortronics Wireless Solutions



Ortronics is the first in its industry to introduce a centrally managed wireless solution that is fully integrated with the structured cabling infrastructure. Ortronics' ground-breaking approach to wireless is an exciting evolution in the structured cabling industry, and changes the way that wireless is deployed in the enterprise.

Ortronics Wireless Solutions feature the new patent-pending Wi-Jack™ Wireless Access Point that mounts directly to a wall outlet box, using the same installation practices as for a standard wall outlet. The Wi-Jack is available in a stand-alone version to allow wireless connectivity for multiple users or in a workstation version to allow wireless connectivity and two additional modular ports to support copper, fiber or coax.

For advanced intelligence, superior security and easier management, Ortronics Wireless Controller allows centralized management and monitoring of access points, with state-of-the-art firewall, intrusion detection, VPN terminations and RF management, all in a single package. The wireless controller is available in versions to support five, 16, or 48 Wi-Jack access points and hundreds of users per controller, and is stackable for easy scalability in any size wireless deployment.

The following features are integrated into the Ortronics controller:

- RF management and planning software
- Stateful firewall
- Intrusion detection system
- Captive portal and VPN support
- Advanced security, 802.1x and 802.11i ready
- Policy-based access control
- Support for secure voice over wireless

Ortronics Wireless Solutions also offers a Power over Ethernet injector, which acts as a midspan device to provide power to the access points over a Category 5e or 6 Ethernet cable, eliminating the need for a separate power outlet at each access point location.

For more information on Ortronics Wireless Solutions, visit www.ortronics. com/wireless.

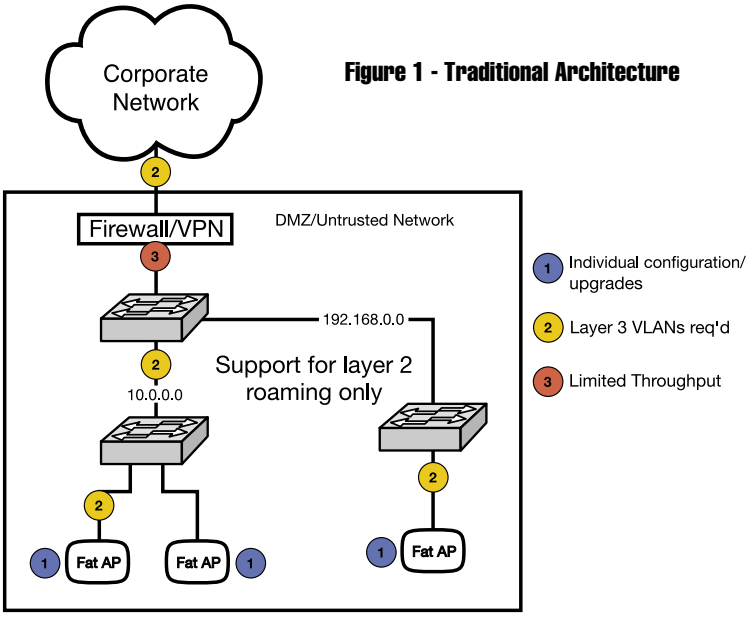

Figure 1 - Traditional Architecture

security and management capabilities, which quickly add to the total cost of ownership. The challenges and complexities of a traditional WLAN are illustrated in Figure 1.

Centralized wireless LANs use a wireless controller to manage, process, and configure the radio frequency (RF) environment. The access points, sometimes called "thin APs", communicate directly with the central controller located at the edge of the wired network. Unlike traditional more costly access points, all the functionality and intelligence is offloaded to the controller. This provides a single point of administration for various policies relating to security, intrusion detection, user roles, and software upgrades. In contrast to Figure 1, a centralized WLAN deploys easily into the network infrastructure with very little complexity. See Figure 2.

The chosen architecture type will ultimately have an affect on RF management, planning, performance, security and total cost of ownership of your WLAN.

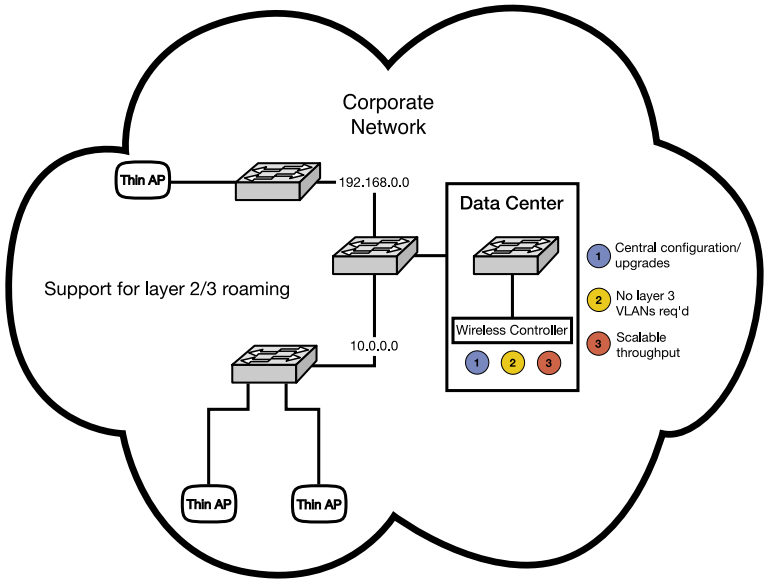

Figure 2 - Centralized Architecture

RF Management

Traditional WLAN deployments have limited built-in management capabilities. Most, if not all, have a telnet and/or a Web-based GUI (graphical user interface) where initial configuration and ongoing management is performed. Network modifications and general administration, for as few as a handful of devices, can be very time consuming. If your wireless environment requires a security, power level, channel, network setting or policy change, the changes will have to be made on each distributed wireless AP.

In a centralized environment you have the ability to manage the entire WLAN from one centralized interface. All wireless LANs use an SSID (service set identifier), which acts as a network name to distinguish one WLAN from another. It is possible to have multiple SSIDs within your organization, one for full employee access and one for limited guest access to the Internet. On the centralized controller you would manage your SSIDs and the associated security and RF configurable parameters from one location without having to make any changes to the APs. With a traditional deployment, if you were to change security settings or any of the RF configurable parameters, you would have to do it on each AP.

In addition to centralized management, many of the wireless controllers can provide enhanced functionality because they are aware of everything that is being transmitted on and around your WLAN. This further allows you to take advantage of unique features to tune and increase performance on the wireless network. Support for load balancing, calibration and self-healing are critical value-added features incorporated into centralized wireless controllers.

Load balancing provides the ability to establish policy thresholds, based on the number of users or bandwidth utilization, on a per AP or SSID basis.

As the AP becomes overloaded, the controller can prevent additional users from associating to the overloaded AP and instead allow them to associate to another more underutilized neighboring AP. While this feature is offered on newer fat access points, it is often less effective due to the distributed nature of the deployment.

Wireless environments are subject to a number of changes that could affect signal coverage and quality. In a warehouse inventory levels may fluctuate and in an office environment the number of people could vary significantly over time, potentially causing problems. RF calibration is one of the most useful capabilities offered by robust wireless controllers to overcome such problems. Because the access points are sending all data back to the controller, it has the ability to analyze the 802.11 management frames of all access points to determine if there are problems. When such problems are discovered, the wireless controller can automatically change the power level or channel setting of one or multiple access points to overcome signal quality issues and/or mitigate channel interference. If a channel becomes overloaded with noise from a nearby source such as a cordless phone, the controller can switch the AP channel and any surrounding AP channels as needed to eliminate signal degradation.

RF calibration is also useful during deployment. After APs are installed, power and channel settings can be automatically selected by using calibration. This frees network administrators from having to select the proper channels and power levels and eliminates possible configuration errors, saving valuable time.

Self-healing features add an important level of redundancy to your WLAN, which eliminates downtime and improves the overall wireless user's experience. In the event that an AP fails, the wireless controller can automatically raise power levels of adjacent APs to provide additional coverage for the failed AP.

In situations where the wireless network is running critical applications, such as in a hospital or warehouse environment, this capability is very valuable and affords time to replace the



failed device without disrupting workflow. Many wireless controllers also support Virtual Router Redundancy Protocol (VRRP) to allow for failover to a backup wireless controller in the event that the wireless controller fails (hot standby redundancy). Eliminating the controller as a single point of failure is an important step in the adoption of WLANs for critical applications.

In a traditional WLAN, calibration and self-healing capabilities are rarely available as native features within the access point. It is more than likely that we will begin to see third-party software available to add this functionality; however the, effectiveness in a distributed fat access point environment remains to be seen.

RF Design and Planning Tools

Traditional wireless LANs require manual time-consuming site surveys that often come at a considerable expense. Also, due to the higher cost of fat access points, they are

often deployed using a signal coverage model in which placement is determined by temporarily locating an access point in an area of desired coverage and then measuring the coverage area. The problem with designing a WLAN, based on coverage, is that it doesn't take into account the number of users per access point, a factor that heavily impacts performance and the user experience. As wireless access becomes more prevalent, there is a need to design for more dense access point deployments to achieve greater user capacity and better performance.

In a centralized WLAN deployment with thin APs, the need for a site survey is practically eliminated. Sophisticated 3D planning tools based on imported floor plans help model wireless requirements, such as data rates and the number and placement of access points. By entering different data rates and types of APs (802.11a or b/g), you can dynamically see expected coverage zones and determine how many APs are needed to meet capacity levels throughout a building. The planning tools may also provide for additional features. Since they are incorporated into the wireless controller, they may also have the ability to triangulate wireless end-user devices and/or access points. This can be beneficial when attempting to track down unauthorized users or access points or to locate staff members, such as doctors in a hospital environment.



Performance

Ease of deployment and integration into the network are important aspects to consider when choosing a WLAN vendor. Many organizations will create VLANs to form a demilitarized zone (DMZ) (Figure 1), and place a firewall or Virtual Private Network (VPN) between the DMZ and the trusted internal network. This often leads to immediate performance problems. Typical wired firewalls and VPNs may only support up to 300 Mb/s of unencrypted throughput, which can quickly be consumed by a handful of access points funneling wireless traffic toward the wired network. In addition to being prone to bottlenecks, seamless wireless client roaming is often very slow - 50 -150 ms at Layer 2 (AP to AP), or not even possible at Layer 3 (AP to AP on different subnets) (Figure 1).

Centralized wireless controllers eliminate many of the performance problems associated with traditional WLANs. The need to create VLANs on the wired network is eliminated since thin APs can communicate with the wireless controller using encapsulation protocols over the existing network. Gigabit uplinks and separate hardware encryption processors can support up to 400 Mb/s encrypted (3DES) throughput. Wireless controllers can more seamlessly allow users to roam from one AP to another on either Layer 2 or Layer 3 without having to worry about authentication or latency problems. AP-to-AP roaming often happens in less than 10 ms because the controller is aware of each AP and each roaming wireless client. Therefore, it knows when and where to send data once the user has moved to another AP. Reliable, fast and seamless mobility will become must-have capabilities as voice and other quality of service applications use the WLAN.

Security Differences

In terms of general wireless security the current traditional and centralized products support the same types of security methods. Wireless security standards such as:

- WEP (Wired Equivalent Privacy),
- TKIP (Temporal Key Integrity Protocol) with MIC (Message Integrity Check),
- WPA (Wi-Fi Protected Access),
- 802.1x EAP (Extensible Authentication Protocol) and
- WPA2 (Wi-Fi Protected Access 2)

These are all possible whether you are using fat or thin access points, however, the real differences exist in security implementation and management. Fat access points require that security settings be configured on each individual access point and because there is security information stored on the flash memory of the access point there is the potential for a network breach in the event that an access point is stolen. Enough security and network information can be obtained from a stolen AP that an unscrupulous attacker could access the network. As new standards evolve, such as with the recent ratification of 802.11i (WPA2)

in June, 2004, older fat access points may not have the memory and processor power to handle AES (Advanced Encryption System) and/or other new standards.

In contrast, thin access points do not contain or process any security configuration information. The wireless controller processes and manages security for each access point. As new standards are ratified, wireless controller software is updated as opposed to replacing access points. In a worst-case scenario, having to upgrade or replace controller hardware is more advantageous than having to replace and reconfigure dozens or hundreds of individual fat access point units.

In addition to basic security standards, wireless controller vendors are offering integrated value-added security software designed specifically for WLAN security. The integration of additional features such as "stateful" firewall, VPN termination, and IDS (intrusion detection system) into one platform makes WLAN deployment as secure as a wired network.

Having a stateful integrated firewall designed to handle wireless traffic greatly enhances security. Stateful firewalls classify and track the state of active connections so that only legitimate traffic packets are allowed to pass through. The ability to create firewall rules and policies allows granular control over what is allowed to pass to and from the wired and wireless network.

The addition of an intrusion detection system is another added feature to bolster the security of any wireless deployment. WLANs are susceptible to typical wired LAN attacks, as well as, their own unique types of attacks, requiring an IDS built specifically for them.

Rogue access points are a very common intrusion type that can erode the highest levels of security in any organization. All it takes is for someone to install an unsecured wireless AP on your network to leave you vulnerable. Wireless controllers typically have the ability to detect this and other types of intrusions and prevent or alert administrators of their existence. Some controllers prevent wireless clients from attaching to rogue access points by creating a Denial of Service (DoS) attack against the unauthorized AP.

Many centralized wireless deployments have the ability to program access points to monitor the air. In this type of scenario the job of the air monitors is to constantly scan all 802.11a/b/g channels for IDS signatures that match a known attack type. Once an attack is identified, the wireless controller can take action to prevent or notify network administrators of intrusions such as:

- Passive and active probing,
- Wireless bridge detection,
- Detection of common attack tools (Asleap, AirJack),
- Man-in-the-Middle detection and prevention and
- Client impersonation

As with a wired network, layered security is the best way to secure your WLAN. The perception that wireless networks are insecure is quickly changing.

Reduced Total Cost of Ownership

The last important consideration is which WLAN deployment offers the lowest total cost of ownership (TCO). The major elements of TCO include hardware/software acquisition, upgrades, ongoing maintenance and labor costs throughout the useful life of the product.

It is extremely important to consider all the costs associated with each deployment to fully understand the savings of one versus the other. In most circumstances, deploying a fully integrated, centralized WLAN greatly reduces costs associated with purchasing separate software to support VPN, intrusion detection, RF management, VoIP (Voice over Internet Protocol), mobility and advanced security. By comparing the costs associated with acquiring the same functionality, you would find that the integrated central controller has a significantly lower capital expenditure. Because the functional components are all integrated, the operating costs over the life of the product are also significantly lower.

Conclusion

It is no surprise that centralized wireless vendors are rapidly acquiring market share. Organizations planning to adopt wireless networks may now choose from a number of solid product offerings that are secure, easier to manage, and have the functionality needed for any size application, from a small office to a large enterprise. As the market continues to evolve, traditional WLAN vendors will be forced to find a way to offer the kinds of features and functionality currently offered by the top centralized wireless vendors. ■

Jeff Davis is a wireless systems engineer at Ortronics Inc., where he is responsible for supporting the wireless product line. He has worked as a network administrator for the past five years supporting, troubleshooting and securing IP networks.

ORTRONICS®
888-879-0724
www.ortronics.com

