



## **White Paper**

# **Debunking the WLAN Switch: Intelligent Access Points Provide a Superior Wireless LAN Solution for the Enterprise**

## Introduction

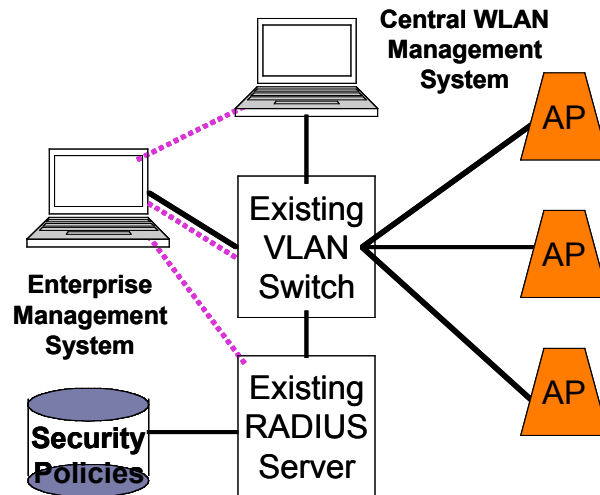
While there is much excitement over a new category of WLAN equipment, the WLAN switch, an alternative architecture using intelligent wireless LAN access points offers a superior enterprise WLAN solution. In fact, all the benefits attributed to WLAN switches can be created using a network of intelligent access points that are centrally managed by a wireless LAN management system. Moreover, intelligent APs provide better manageability, scalability, interoperability and lower costs than the alternative WLAN switch-based approach.

## Competing Enterprise WLAN Architectures

Among several architectures that have emerged for the deployment of WLANs within an enterprise, the Extension Architecture leverages a familiar networking model. It uses distributed processing to deliver scalable WLAN services, and a central management system for ease of operation. In contrast, the WLAN Overlay network centralizes all aspects of WLAN processing and management in a central switching system.

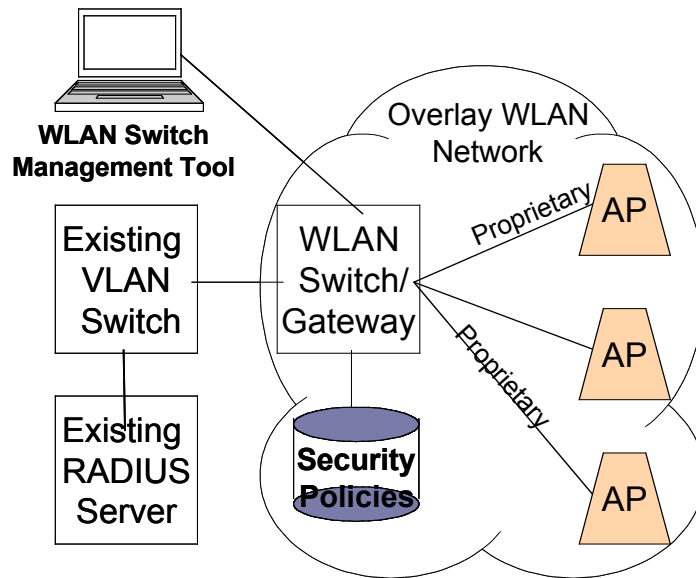
The Extension architecture uses intelligent wireless APs to offer to wireless users the same network services that are accessible to users of the wired network. Intelligent APs are distributed on the edge of the enterprise network and process all the unique functions associated with wireless connectivity. A central management system provides unified management of the wireless Extension service, including radio coverage, security policies and other attributes controlled by the APs.

The Extension architecture defines a secure boundary between the wired and wireless networks, and uses open interfaces to leverage the existing wired network infrastructure. The intelligent access point applies a consistent set of network security policies to traffic traversing the boundary using an existing back-end policy database, such as RADIUS. The packets it places on the wired network can be switched or routed by the existing infrastructure using security mechanisms that are already in place, such as VLANs.



**Figure 1: The Wireless Extension Architecture uses intelligent APs, open interfaces, and a central wireless element management system to integrate into the existing network infrastructure**

The Overlay architecture creates a separate network that is dedicated to wireless users. It is composed of WLAN switches interconnected with either proprietary or standards-based “thin” access points over Ethernet cabling. Similar to intelligent APs, the thin access points perform IEEE 802.11 MAC layer processing and include a standards-based radio. However, they do not implement any security policies, leaving this function for the WLAN switch.



**Figure 2: The Wireless Overlay Architecture uses a WLAN switch connected to proprietary “thin” access points to create a separate network with its own security and management systems**

The WLAN switch is a central processor for security and management of the wireless network. It lies directly in the data path, processing all packets for the APs that are attached to it. Many switches replicate the wired network’s security administration infrastructure by providing a separate authentication database for wireless user authentication. Some vendor’s switches do not integrate into the enterprise security infrastructure, or interface with a central RADIUS database; they require all security policies must be locally administered. As more functions are centralized in the WLAN switch, its processing requirements and expense increase.

### Security Comparison

Intelligent access points and WLAN switches provide comparable wireless security. Both architectures implement the same security standards, ensuring wireless data integrity is maintained and protecting the wired network from unauthorized access.

### Security Feature Comparison

	<u>WLAN Switch</u>	<u>Intelligent AP</u>
<b>Client Authentication</b>		
802.1X	✓	✓
EAP	✓	✓
VPN	✓	✓
RSA SecurID	✓	✓
PKI	✓	✓
Captive Portal	✓	✓
<b>Client Encryption</b>		
WEP/WPA	✓	✓
IPSec	✓	✓
<b>LAN</b>		
802.1q (VLAN)	✓	✓
MAC Filtering	✓	✓
<b>RF</b>		
Rogue AP Detection	✓	✓
<b>Management Interface</b>		
VPN tunnel		✓
Access control	✓	✓

The security weakness the WLAN switch vendors most often cite when comparing their products with intelligent APs is physical security. They argue that malicious users can tamper with APs that are mounted in public areas and gain access to the device's management interface. While this may be true of some consumer-grade products, it does not apply to enterprise-class APs that feature secure management interfaces.

Colubris Networks intelligent APs feature management interfaces that can be completely secured using VPN encryption and authentication. RADIUS security policies and a built-in firewall can be used to restrict access to the management interface to designated WLAN users, or users on designated VLANs or IP subnets. In addition, Colubris Networks Management System (CNMS) continuously audits the configuration settings on all APs to ensure there are no malicious or accidental changes to the network.

The Detractors further claim that a malicious user could attach a foreign end-node to the enterprise Ethernet after unplugging the AP, exposing the LAN to a security breach. This is specious, since enterprise-class Ethernet switches provide MAC layer verification. The switch would detect a different MAC address and shut-down the Ethernet port. CNMS also safeguards the network by automatically detecting a missing or failed access point, or the activation of a rogue access point.

*Security Comparison: Comparable*

## Manageability Comparison

Intelligent APs, complemented by a central WLAN management system, are easier and less costly to manage than WLAN switches because they use open interfaces to integrate into the existing corporate network infrastructure. The authentication and security mechanisms implemented by Intelligent APs are an extension of the existing network and can be managed by existing enterprise management tools. For example, Colubris Networks intelligent APs use RADIUS protocols to reference the same central RADIUS policy mechanisms used by the enterprise network for per-user authentication and per-user VLAN assignment. Changes made to this server are immediately applied to both the wired and wireless networks.

Management attributes that are unique to the wireless Extension network, such as radio configuration and monitoring and initial security settings, are managed by a central WLAN element management system. For example, CNMS uses SNMP protocols and open MIB extensions to configure and monitor a network of intelligent APs. CNMS makes management of large networks of intelligent APs easy by providing group configuration policies that enable a network manager to detect new APs and implement configuration changes or download new software in seconds.

CNMS also provides tools to integrate into an enterprise management framework. It includes a snap-in for H/P OpenVIEW Network Node Manager, and Colubris Networks APs are manageable under Micromuse NetCool™. This capability gives network administrators centralized monitoring and troubleshooting of the combined wired and wireless networks.

The Overlay architecture takes a different approach. Security configuration and administration for wireless users are typically defined in the WLAN switch, separate from the enterprise network. In addition, the switch itself, a relatively sophisticated piece of gear that replicates many of the functions already performed by Ethernet switches, and the associated “thin APs” are separately managed. This makes the Overlay management system much more complex than the system used to manage the wireless Extension network. Network operators must be trained to trouble-shoot and operate a new system that performs many of the same functions as existing Ethernet switches, instead of leveraging the tools and systems already in place.

Some vendors of WLAN switches provide proprietary element management systems to ease the complexities of managing large networks of their equipment. Other WLAN switch vendors offer only embedded tools that manage individual switches; they provide no centralized management for multi-switch networks. Both solutions are more complex than the centralized element management used in wireless Extension networks.

In both cases, the WLAN switch vendors do not provide multi-vendor management of third party access points, forcing network managers to standardize on a single vendor solution, or implement multiple management systems. Colubris Networks takes an open, multi-vendor approach with its management system by providing comprehensive support for APs manufactured by the top ten vendors in the industry.

The WLAN switch vendors sometimes claim that the RF coverage for a network of intelligent APs is more difficult to configure and manage as compared to WLAN switches. They claim a central switch connected to proprietary “thin APs” makes the RF pattern more uniform and easier to control and monitor because the APs provide a detailed RF management interface. While this is indeed a laudable goal, it does not require an Overlay network.

Colubris Networks’ intelligent APs, combined with CNMS, deliver the same ease of RF control and comprehensive monitoring while adhering to open standards. The APs provide MIBs with RF management capabilities that are comparable to “thin APs”. This enables the Extension Architecture to provide the same RF management services as the

Overlay Architecture —network-wide rogue scanning, RF coverage mapping and load balancing— while leveraging the existing enterprise management infrastructure.

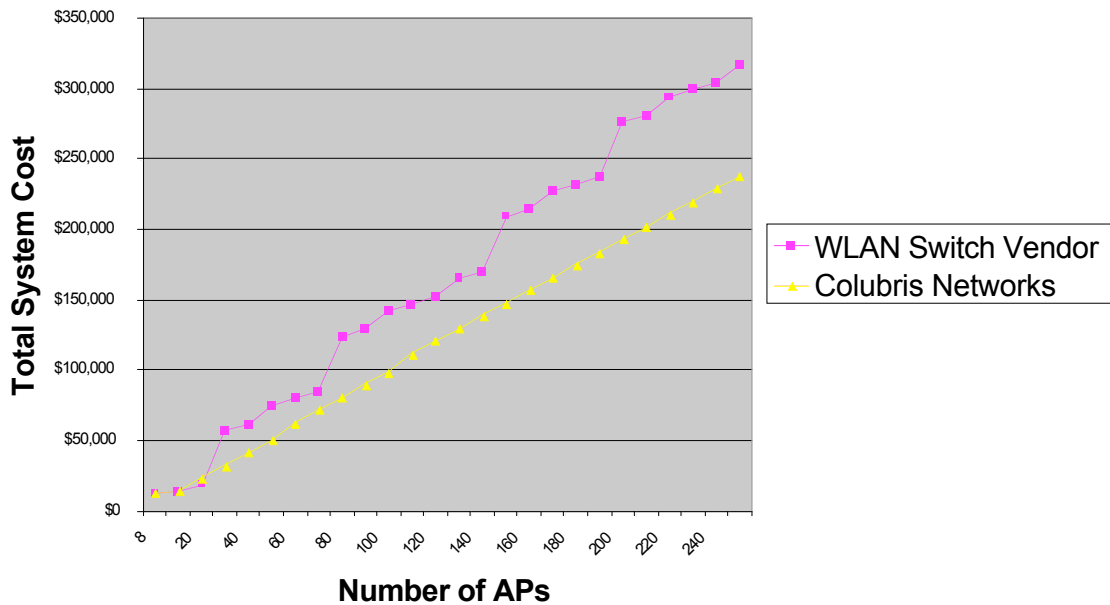
*Manageability Comparison: Advantage goes to Intelligent APs*

### Capital Expenditure Comparison

WLAN switches add significant cost to the deployment of a WLAN network. While “thin APs” are about 40% less expensive than Intelligent APs, this lower cost is more than offset by the very high cost of a central WLAN switch, regardless of the size of the network.

The chart below illustrates the low cost and linearity of a Colubris Networks solution, as compared with a typical vendor of Overlay networking equipment. It assumes that each type of AP has similar range and performance; the number of APs required to cover a given geographic area drives the cost of each network.

### Acquisition Cost Comparison Hardware, Software and Management System



The comparison shows that intelligent APs complemented by a central Wireless LAN management system provide very low costs, from entry-level to very large network configurations. In addition, Intelligent APs exhibit a nearly linear cost curve, making them a more scalable alternative.

In contrast, the Overlay Architecture adds significant costs for WLAN switches and associated software licenses, which are sold on a per-switch basis. This causes the cost disparity between Overlay and Extension architectures to grow, as the network increases in scale. An Overlay network supporting 250 APs is 30% more expensive than the equivalent wireless Extension network.

*Acquisition Cost Comparison: Advantage goes to Intelligent APs*

Cost Assumptions:

List Prices	WLAN Switch Vendor		Colubris Networks (Intelligent AP)		
Access Point	\$500 (Thin)		\$899 (Intelligent)		
WLAN switch	\$5,000	\$17,000 + \$8,000/blade	N.A.		
WLAN Switch Capacity (ports)	24	0-72 (24/blade)	N.A.	N.A.	N.A.
Management Software	\$9,000	\$9,000	\$3,500	\$6,000	\$10,000
Management Software Capacity	License per switch	License per switch	50 APs	100 APs	1,000 APs
Management Platform (Hardware)	N.A.	N.A.	\$2,000	\$3,000	\$5,000

**Scalability Comparison**

Network managers planning to deploy enterprise-wide WLAN networks need solutions that can scale-up to many hundreds of APs. The scalability of a solution is typically based on several factors, including acquisition cost, manageability, ease of deployment and performance. Intelligent APs excel in each of these dimensions.

The preceding section demonstrates that intelligent APs are more economically scalable. The network management system is the only fixed cost associated with an Intelligent AP solution. The remaining costs scale linearly with the geographic size of the network and the number of APs required for coverage.

The management leverage associated with an Extension Architecture, augmented with a wireless management system, give intelligent APs a manageability edge. WLAN switch vendors claim their solutions are more manageable, but they usually assume intelligent APs are not centrally managed. When the central management capabilities of both wireless architectures are considered, the advantage goes to the intelligent AP.

The management systems used in both architectures can automatically discover APs and configure them with proper RF and security settings. But, the Overlay architecture requires a physically separate cable plant to support direct connections between the WLAN switch and AP, making deployment more complex and costly than the Extension architecture. In addition, some WLAN switches operate at layer-2 and don't interoperate with 3<sup>rd</sup> party switches and routers. This further complicates deployment and operation.

Intelligent APs provide better performance than WLAN switches as networks scale-up because of their distributed processing capability. Each AP includes a processor that executes all the tasks that are unique to the wireless network. The embedded processor provides full throughput (up to 54 Mbps) for a single AP. There is no over-subscription at the individual access point. Processing power and performance increase with each AP that is added to the network, maintaining full throughput for the entire WLAN and its associated users.

In contrast, the WLAN switch offers a fixed amount of processing power and performance regardless of how many thin APs are connected to it. Its performance may vary, depending upon the amount of over-subscription it is designed to support. For example,

many first-generation switching technologies have been designed with oversubscription ratios exceeding 2:1.

The Extension Architecture has a further advantage in geographically distributed organizations because it can be implemented in a building of any size, from small branch offices to large headquarters buildings, while consolidating the entire infrastructure under a central management system. The Overlay Architecture does not offer the same range of cost-effective solutions, forcing network managers to deploy costly hybrid wireless networks that are designed specifically for each type of building.

*Scalability Comparison: Advantage goes to Intelligent APs*

## **Interoperability Comparison**

Interoperability is the keystone of the wireless Extension Architecture because it uses industry standard interfaces to leverage investments in existing network infrastructure. Intelligent APs provide complete interoperability and give network managers the flexibility to install a best-of-breed wireless network solution.

Colubris Networks intelligent APs provide superior interoperability on both the wired and wireless LAN interfaces, implementing important industry and de-facto standards at layers 1 through 7. These standards enable Colubris Networks products to interoperate with 3<sup>rd</sup> party VPN clients and servers, industry standard RADIUS and certificate-based (X.509) authentication systems, SNMP management systems, and much more. Moreover, Colubris Networks APs and network management systems can be mixed and matched with existing wireless equipment, protecting your initial wireless investment.

In contrast, the Overlay Architectures promoted by the WLAN switch vendors are largely proprietary. They lock-in customers to a single-vendor solution for all wireless components, from “thin APs” to management software, and force customers to retire any investments they’ve made in alternative wireless solutions.

Many WLAN switch vendors do not interoperate with 3<sup>rd</sup> party VPN clients. For network managers that want to leverage VPN standards to secure all network access, from dial-up to wireless, this limitation adds cost and complexity. Multiple clients must be installed and maintained on the user’s laptop, one for wireless access and another client for all other types of access.

Several WLAN switch vendors have proposed a standard for their “thin AP” management interfaces, called Light-Weight Access Point Protocol (LWAPP). If this ambitious standard is ratified, it may open one of the proprietary aspects of the Overlay architecture. Its success is far from certain, since the initial proposals are based on patented technology owned by one of the standard’s promoters. In addition, various vendors have not yet agreed on a single approach to satisfy their wide-ranging objectives. If LWAPP is ultimately successful, it likely won’t be commercially available for some time.

*Interoperability Comparison: Advantage goes to Intelligent APs*

## **Conclusion**

When Intelligent APs are combined with a wireless network management system in a wireless Extension Architecture, users receive the centralized control and manageability associated with the Overlay Architecture without the drawbacks. The Extension Architecture provides greater scalability, lower cost, ease of management, higher interoperability, and security management that is integrated with the existing network infrastructure.

The Overlay Architecture causes users to invest in expensive WLAN switches that replicate many of the functions already performed by enterprise Ethernet LAN switches, while locking the customer into a proprietary wireless networking system.

**Summary Comparison**

<b>Evaluation Criteria</b>	<b>Extension Architecture Intelligent AP</b>	<b>Overlay Architecture WLAN Switch + Thin AP</b>
<i>Security</i>	Comparable	Comparable
<i>Manageability</i>	Advantage	
<i>Acquisition Cost</i>	Advantage	
<i>Scalability</i>	Advantage	
<i>Interoperability</i>	Advantage	