



WHITE PAPER

Colubris TriPlane™ Architecture: Unprecedented WLAN Scalability



Enterprise wireless LANs (WLANs) save money, boost productivity and unleash valuable new applications. IT Managers want to extend WLAN support to include more users, more locations, more applications and more types of wireless devices. These growing demands, however, are too much for today's "switch-centric" WLANs. The monolithic design of these systems doesn't scale—up or down—cost-effectively, and their outdated architecture can't provide the differentiated services required to support a broad mix of applications. Moreover, WLAN switches don't provide a migration path to unified WLANs which use new LAN/WLAN access layer switches to unify network security, QoS and management regardless of the media type used to access the network.

With its unique TriPlane Architecture, Colubris Networks introduces the industry's first highly scalable, truly multi-service WLAN solution. By dedicating separate resources to management, control and "fast-path" packet processing and by distributing network intelligence to the wireless edge, the TriPlane Architecture brings a new generation of versatility, scalability and affordability to enterprise WLANs. In addition, the TriPlane Architecture creates a migration path to the Unified Services Network—an integrated platform for both wired and wireless access to best-in-class business services

Towards a New Architecture

The limitations of today's switch-centric WLANs make it clear that a new model is required. A model that combines the advantages of central WLAN control and management with a more scalable data switching method. Accordingly, this year is witnessing an architectural trend towards separation of the data plane—where the packet processing and forwarding functions reside—from the control and management planes. Purpose-built appliances that preserve the benefits of central control are emerging, complementing intelligent access points that perform fast-path data switching at the network edge.

This next-generation architecture delivers more effective QoS and more economical scaling and is designed to meet a number of important criteria:

- **Rich service offerings**—Besides providing access to wired network services, the model enables a new class of business mobility applications. It supports real-time services with roaming, location-based applications and more. And it is open to integration with third-party applications.
- **Scalability**—The new architecture is flexible and modular enough to fit both centralized and distributed organizations and both large and small facilities.
- **High performance**—The architecture delivers the performance required to support not only demanding client applications but also emerging high-speed technologies like 802.11n and MIMO. Plus, it will provide a migration path to even higher performance applications and technologies in the future.
- **Reduced cost**—In order to make WLANs the "default" access technology in enterprise networks, the new model yields a TCO—including installation, operation and equipment costs—that is competitive with wired Ethernet.

By separating the data and control planes, this next-generation architecture also provides a steppingstone to the Unified Services Network, the ultimate merger of wired and wireless LAN switching into a single platform deployed throughout the access layer of an enterprise network.

WLAN Trends and Requirements

Rapid adoption of WLANs is driving the movement toward a new architecture in the enterprise. No longer an emerging technology or special-case solution, WLANs have become a standard business tool—a fact that places challenging new requirements on wireless networks:

- **True mobility**—Enterprise WLANs were first conceived to support nomadic use. Employees could expect wireless access to the corporate network while sitting in offices or conference rooms, but not while walking down the hall. Now a new generation of applications, with voice at the forefront, requires WLANs that support continuous real-time mobility. A WLAN must maintain reliable high-performance connections to wireless devices even while users move about the building.
- **User diversity**—To increase productivity and convenience, enterprises are opening their WLANs to more types of users. Besides giving employees access to internal applications, companies are granting visiting suppliers wireless access to the corporate extranet, giving contractors access to specific resources, and in many cases, allowing the public access to the Internet. In fact, enterprise WLANs often support more types of users and applications than wired LANs, making ease of use, tight security and stringent quality of service (QoS) more important than ever.

- **More devices**—Not only are more personal computers going wireless, but more types of wireless devices are appearing in enterprise environments. A growing population of voice handsets, PDAs, portable tablets, barcode scanners, etc. needs secure, responsive wireless access to the enterprise network.
- **Mass deployment**—The ultimate goal for enterprise WLANs is 100% coverage—wireless access for all users, all devices, and all company locations. WLANs must scale to support large, diverse user populations at a mix of both small and large sites.
- **Application integration**—Integration with other network devices can foster valuable new WLAN capabilities. An IP PBX, for example, could check WLAN bandwidth availability before putting a voice call through to a wireless handset. Modern WLAN systems, therefore, should include an open interface to third-party developers.
- **Affordability**—First and foremost, enterprise WLANs must be cost-effective, with a total cost of ownership (TCO) that competes with wired Ethernet. Initial deployments should be reasonably priced, and upgrades to add capacity or to support new services should come in affordable increments.

Outdated Switch-centric WLANs

Over the last two years, the industry has settled on a model for enterprise WLANs that comprises “thin” access points (APs) and a central WLAN appliance or switch. The APs handle radio frequency (RF) connections to laptop computers and other wireless devices. The switch handles everything else: WLAN management and control, fast-path data forwarding, security and QoS. MAC layer processing is split between the switches and the APs. Traffic between the APs and the switch tunnels through multiple hops as it moves from the network edge to the enterprise network equipment center, where the switch is typically installed. Since the central switch makes all packet-forwarding decisions, all WLAN traffic must pass through the switch on its way between clients and servers (Figure 1).

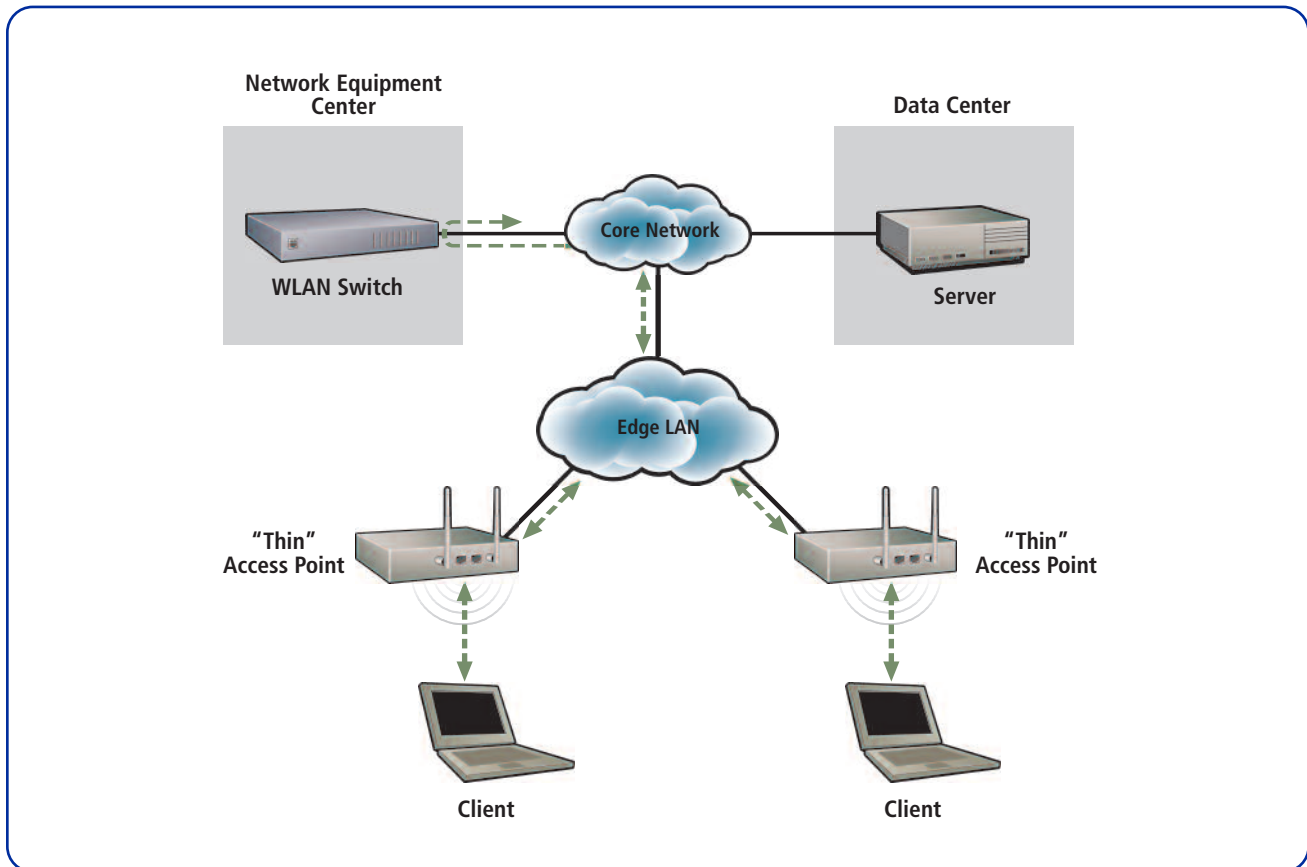


Figure 1: With switch-centric WLANs, all traffic passes through the WLAN switch.

Centralized management and control make it easy to deploy and operate these switch-centric WLANs. Security, QoS, RF tuning and other features can be managed from a single point, rather than dealing with each AP separately. And central control makes it easy to manage the handoff as a wireless device roams from AP to AP. On the other hand, sending all wireless traffic through a central switch has significant drawbacks:

- **High entry cost**—The monolithic central switch imposes a high entry cost on the WLAN, making it too expensive for small sites. And since the APs cannot operate without the WLAN switch, the enterprise must pay for redundant switching capacity to ensure non-stop operation.
- **Expensive scaling**—As wireless traffic increases, the central switch becomes a bottleneck. The only way to increase packet-forwarding capacity is to buy and install another switch. But the performance “sweet spot” for most WLAN switches is around 36 to 128 APs, resulting in scaling increments that are too large for some situations and too small for others. Moreover, the inclusion of control logic in every switch imposes a “tax” on WLAN scaling. Every time the enterprise adds more packet-forwarding capacity, it pays for more control logic as well. The resulting amortized cost is over \$1,000 per AP.
- **Weak QoS**—Quality of service policies are applied to WLAN traffic at the switch, not at the APs. Often, the WLAN switch is deployed in a network equipment center several “hops” away from the APs. If there is congestion between the APs and the switch, delay-sensitive traffic can suffer, since the tunnels used to carry WLAN packets across the wired LAN hide QoS markings contained in the user flows and prevent the wired LAN from acting upon them.
- **Traffic re-engineering**—Tunneling traffic to a central switch introduces a different traffic pattern than the distributed switching that most enterprises use to handle traffic from wired clients. This causes aggregation links along the path between access points and the central WLAN switch to be upgraded to handle the increased traffic load.
- **Limited future**—The closed, one-size-fits-all design of today's WLAN switches severely limits network growth and enhancement. The switches can't scale to cover highly distributed environments or to cope with an increasing traffic load. In fact, the enterprise will likely have to buy new WLAN switches to support future high-speed standards like IEEE 802.11n. And lacking open interfaces, most WLAN switches can't be controlled from or share information with external devices, precluding valuable new applications.

The New Generation: Colubris TriPlane™ Architecture

The Colubris TriPlane Architecture is leading the way to the next generation of enterprise WLAN solutions. Its innovative design allocates separate resources to management, control, and data forwarding and distributes network intelligence to the wireless edge (Figure 2). By combining the operational efficiency of centralized management and control with the scalability, versatility and enhanced QoS of distributed intelligence, the TriPlane Architecture preserves the strengths of today's switch-centric WLANs while eliminating the weaknesses.

As its name implies, the TriPlane Architecture assigns management, control and data forwarding functions to separate “planes,” each with dedicated processing resources. In a Colubris Intelligent MultiService System (CIMS), the data plane is implemented in InReach™ MultiService Access Points (MAPs), the control plane in InMotion™ MultiService Controllers (MSCs), and the management plane in the InCharge™ Colubris Network Management System (CNMS). The design of each device is optimized for its role in the WLAN system.

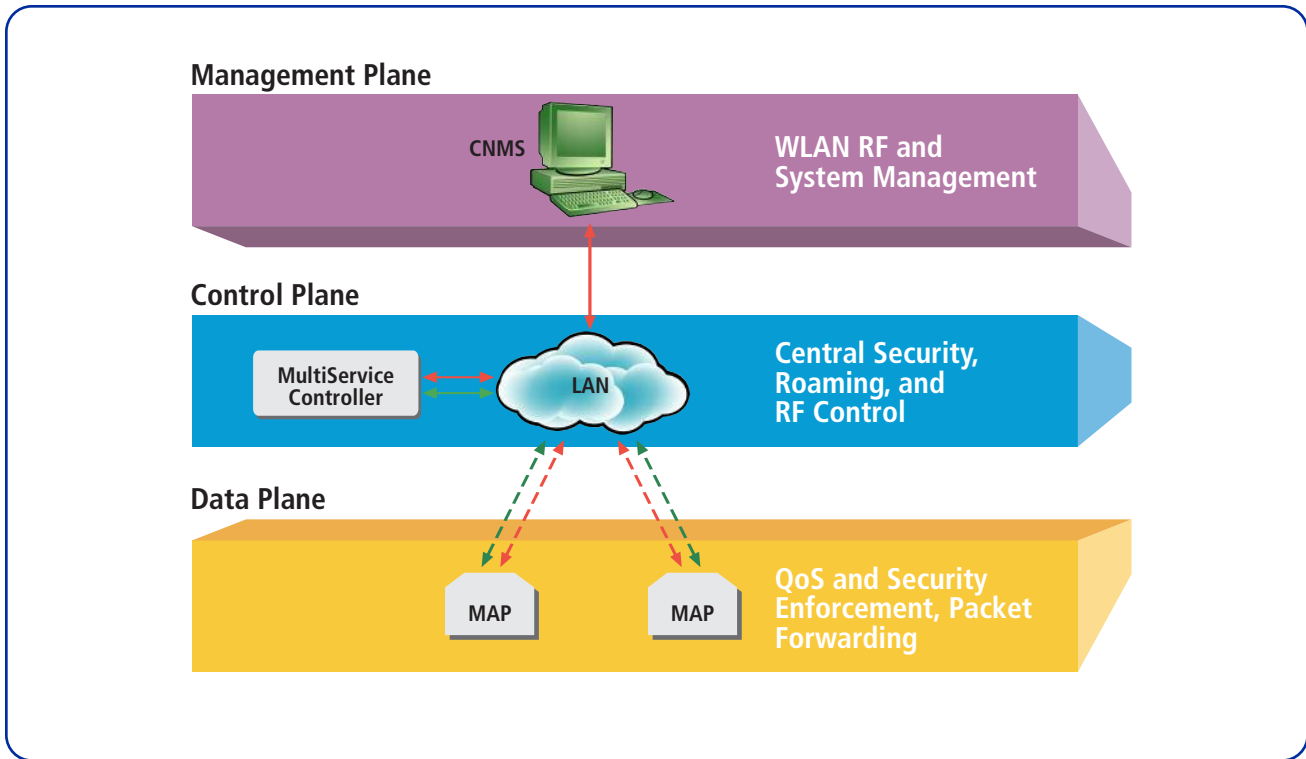


Figure 2: The Colubris Tri-Plane Architecture allocates separate resources to management, control, and data forwarding.

The Data Plane

In the Colubris TriPlane Architecture, the data plane is responsible for data forwarding, QoS enforcement and security enforcement. Sitting at the wired/wireless boundary, intelligent InReach MAPs forward packets directly between clients and servers, rather than shunting everything through a central WLAN switch (Figure 3). Local 802.11 MAC protocol processing, hardware-assisted data encryption, and RADIUS authentication eliminate most dependencies on a central resource. By applying security policies, MAPs stop unauthenticated traffic at the network edge. And by eliminating special WLAN client traffic tunnels, the intelligent MAPs leverage the QoS and security features of the wired infrastructure.

The data plane also performs real-time WLAN intrusion detection and prevention. Dual radio models of the InReach product line provide the first line of WLAN defense by detecting and de-activating rogue devices before their traffic can pose a threat to the enterprise network.

The Control Plane

The control plane is the key to the TriPlane Architecture. By maintaining centralized control over the distributed data plane, the control plane ensures consistent service support across the entire WLAN, but without the shortcomings of a central WLAN switch.

As the WLAN is deployed and expanded, InMotion MSCs and InReach MAPs automatically discover each other and establish a secure layer-3 communications tunnel for the exchange of WLAN control information. Mutual X.509 authentication and encryption between the MAPs and the MSC eliminate any security risk and high availability features built into the configuration and control protocol ensure continuous MAP-MSc connectivity.

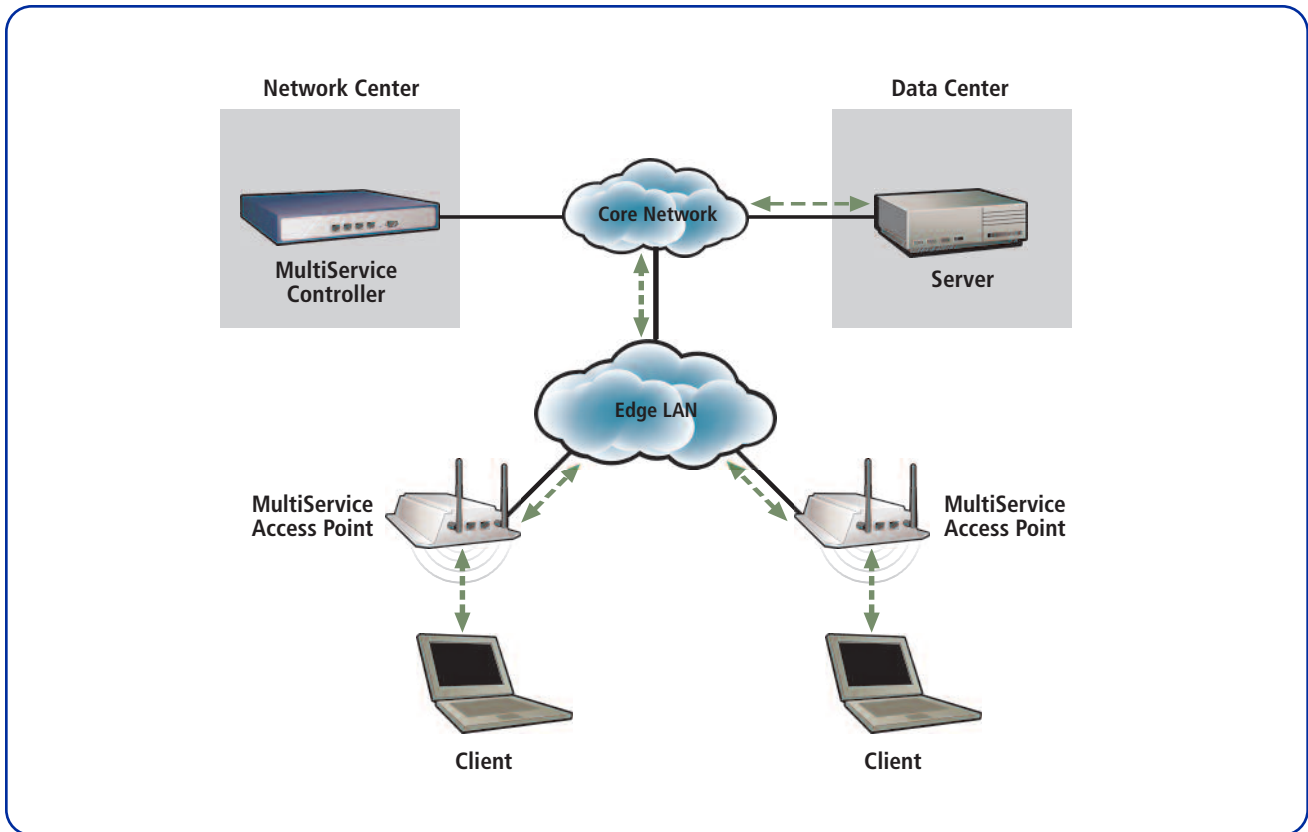


Figure 3: With the Colubris Tri-Plane Architecture, intelligent Multi-Service Access Points forward traffic directly between clients and servers.

In support of real-time mobility, the MSC ensures fast, seamless handoffs as wireless devices roam from MAP to MAP. The MSC knows which MAPs are neighbors, so it can anticipate handoffs. Pre-shared PMK caching allows WPA re-association and proxy Mobile IP supports inter-subnet handoffs in less than 50 milliseconds with complete client transparency.

By dedicating separate resources to WLAN control, the MSC also enables the next major step in access network evolution: the Unified Services Network. In a Unified Services Network, LAN access switches are replaced with unified LAN/WLAN access switches that apply advanced QoS and security controls to both wired and wireless traffic. The MAPs and MSC remain, although in some implementations the MSC may be integrated with the unified switch or tucked away in a LAN core switch. For dramatically simplified network operations, a unified management system oversees both types of traffic. See the Colubris *Unified Services Network* white paper for details.

The Management Plane

In the management plane, the InCharge Colubris NMS supports classic fault, configuration, accounting, performance, and security (FCAPS) functions:

- **Policy management**—Network operators can define services and set policies for the entire WLAN. A friendly user interface simplifies the configuration process, while the CNMS automatically pushes configuration and policy information to the MSC and MAPs.
- **Troubleshooting**—Troubleshooting tools and automatic firmware updates aid quick problem resolution.

- **Capacity planning**—Performance analysis and trending tools assist in WLAN capacity planning.
- **Remote management**—Standard web, SNMP, and XML management interfaces enables rich, straightforward remote management.
- **RF Security**—configuration of security policies to be monitored and enforced by MAPs, plus ongoing auditing to ensure policies are always up-to-date.

TriPlane Architectural Benefits

By dedicating separate resources to management, control and data forwarding and by distributing intelligence to the wireless edge, the TriPlane Architecture delivers benefits that earlier, switch-centric architectures cannot achieve.

- **Unprecedented performance and scalability**—Separation of the control and data planes dramatically increases WLAN performance and scalability, but without sacrificing the convenience and control of centralization. A WLAN can start at the right size and cost for any situation and then grow to serve more users or to reach more sites simply by adding more MAPs. The MAPs automatically discover the MSC and configure control protocols. A single CIMS can grow to include thousands of MAPs and support tens of thousands of users.
- **Superior QoS**—By enforcing QoS at the wired/wireless boundary, the TriPlane Architecture creates a superior foundation for sensitive voice and multimedia applications. Forwarding packets directly toward their destination instead of detouring them through a WLAN switch eliminates the jitter and latency of at least one network hop and leverages the QoS features of the wired network. Intelligent MAPs apply QoS to the RF links, ensuring that voice and other delay-sensitive traffic is prioritized end-to-end. Central coordination by the MSC ensures consistent, balanced QoS enforcement from MAP to MAP.
- **Real-time mobility**—Intelligent MAPs, coordinated by the MSC, support real-time mobility. Wireless clients can move throughout the WLAN footprint, maintaining secure, continuous connections with intra- and inter-subnet handoffs in under 50 milliseconds.
- **Integrated client security policy enforcement**—The TriPlane architecture exposes individual user flows to wired Ethernet access switches, enabling their security features to analyze and act upon the WLAN traffic. This allows client security policies to be consistently enforced for wired and wireless LAN users alike. It eliminates the expense associated with a specialized WLAN infrastructure for antivirus and network admission control.
- **Scalable RF Security**—The distributed data plane performs real-time IDS/IPS on 100% of the WLAN traffic, enabling it to detect threats that are unique to WLANs. Unlike WLAN switches that centralize all RF security functions along with client packet processing, the TriPlane architecture forwards only threat information from MAP to MSC. The threats can then be correlated and subjected to additional analysis. This hierarchical RF security approach is more scalable and eliminates the heavy network traffic load associated with centralized RF security solutions.
- **Service reliability**—Distributed data plane intelligence increases WLAN service reliability, since the failure of a MAP doesn't affect other network elements. Because MAPs are intelligent, they continue to forward client packets and accept new connections normally, even if an MSC were to fail.
- **LAN-like TCO**—Separation of the data and control planes significantly reduces WLAN TCO since the enterprise no longer pays a controller tax each time it adds packet-forwarding power (Figure 4). Amortized cost of the controller and MAPs drops to nearly \$600 per MAP, as much as 40% lower than earlier architectures. The TriPlane Architecture protects the WLAN investment by allowing the addition of next-generation MAPs—to support 802.11n, for example—without requiring an MSC upgrade. And operations costs stay low since the CNMS scales to manage thousands of MAPs as a single system.

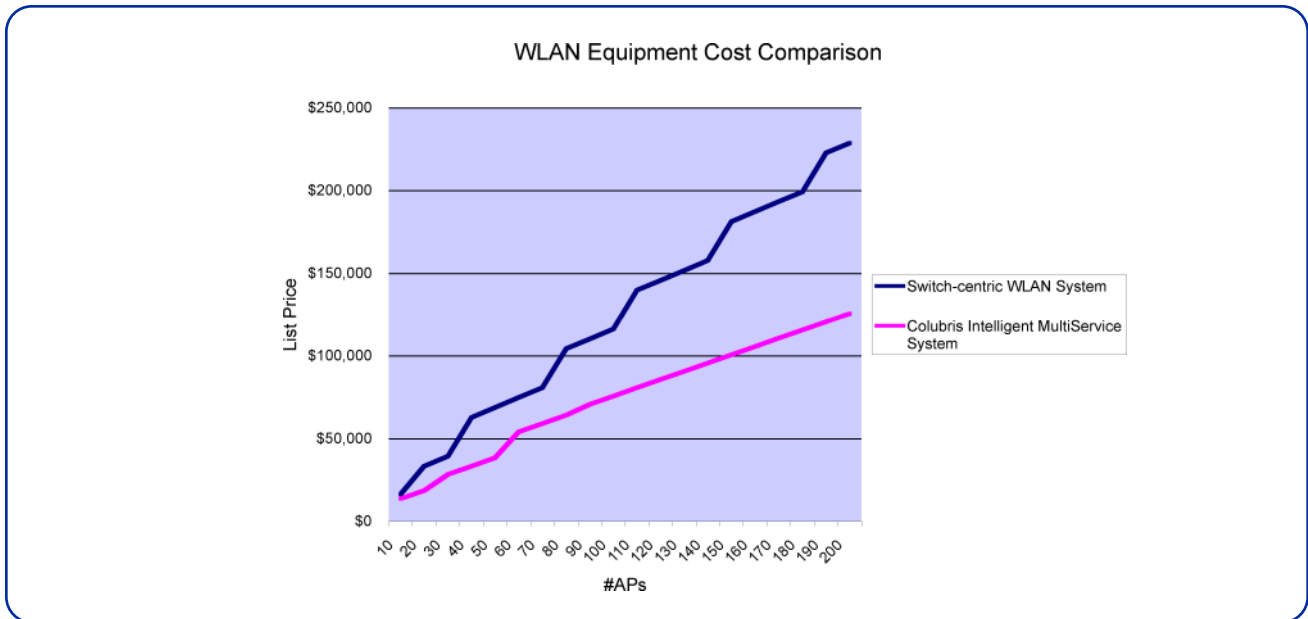


Figure 4: The price of a Colubris WLAN is as much as 40% lower than switch-centric WLANs.

An Extensible Architecture

The Colubris TriPlane architecture is implemented in software, giving it the flexibility to support advanced enterprise features as optional software upgrades. The Colubris roadmap includes MSC clustering that will provide N+1 redundancy and enables an enterprise to scale MSC capacity in affordable increments. Advanced RF management features will coordinate RF channel allocation, power and load balancing across MAPs. By controlling the overall RF footprint, the MSC ensures consistent coverage, performance and resiliency and makes it easy to deploy and expand the WLAN.

Separation of the data and control planes also ensures a smooth migration to the Unified Services Networks of the future. With WLAN control centralized in the MSC, enterprises can deploy unified WLAN/LAN access switches and integrated management for consistent, fully capable wired and wireless access to best-in-class business services.

Conclusion

By dedicating separate resources to management, control and packet forwarding and by distributing network intelligence to the wireless edge, the Colubris TriPlane Architecture eliminates the cost and service limitations of today's switch-centric WLANs without sacrificing the benefits of central control. With the Colubris TriPlane Architecture, wireless LANs take their place beside wired LANs as ubiquitous elements of the enterprise network, while enterprises enter a new era of flexible, secure, economical business-class wireless networking and begin the migration to the Unified Services Networks of the future.

The Colubris Intelligent MultiService System

The Colubris Intelligent MultiService System (CIMS) offers an unprecedented level of flexibility, scalability, service quality and economy. A range of configurations and form-factors makes the CIMS economical to deploy at any location (Figure 5). For small sites, integrated MultiService Controller/Access Points provide a turnkey WLAN solution that is easy to deploy and manage. In large venues, the CIMS leverages the existing wired infrastructure to create pervasive wireless service at low cost. In any environment, the system scales smoothly while protecting the enterprise's initial investment.

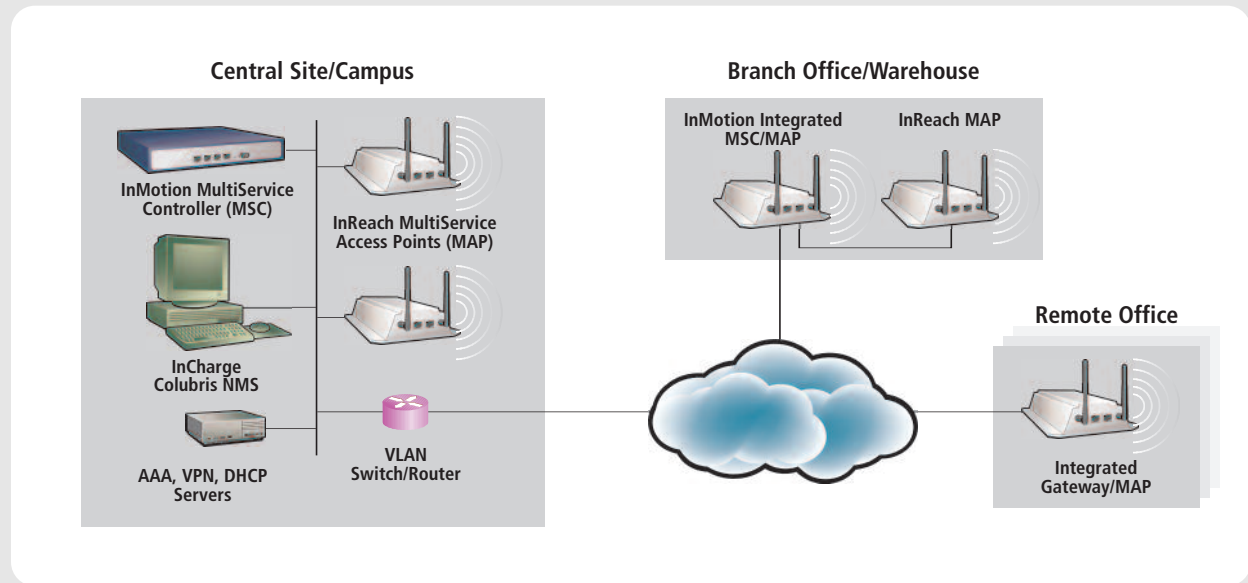


Figure 5: The Colubris Intelligent MultiService System offers an unprecedented level of flexibility, scalability, service quality, and economy.

InCharge Colubris Network Management System

The InCharge CNMS is available in versions that manage from 50 to 4,000 APs.

InReach MultiService Access Points

The InReach MAP is available in two models:

- **MAP-320:** An intelligent 802.11a/b/g access point with multi-service support, fast-path data forwarding, layered security and enterprise-class QoS. It is available in plenum-rated indoor, or outdoor enclosures.
- **MAP-330:** An 802.11a/b/g dual-radio access point with all the features of the MAP-320. Each radio is independently configurable to operate in AP mode for wireless access, WLAN monitor mode for troubleshooting and rogue AP detection, or wireless distribution system (WDS) mode for wireless backhaul. It is also available in plenum-rated indoor, or outdoor enclosures.

InMotion MultiService Controllers

The InMotion MSC is available in four models, including two with integrated access points:

- **MSC-5500:** A high-performance 1U rack-mount appliance that provides central control for as many as 200 InReach MAPs. The MSC-5500 boasts capacity for 2,000 public/guest access users.

- **MSC-5200:** A 1U rack-mount appliance that supports as many as 25 InReach MAPs and has capacity for 500 public/guest access users.
- **MSC-3200/3300:** An integrated multi-service controller and access point in an easy-to-deploy enclosure. The MSC-3200 includes a single software-configurable 802.11a/b/g radio, while the MSC-3300 offers dual radios for increased RF flexibility. Ideal for small offices, retail locations and Internet hotspots, these models have capacity for 100 public/guest users. Both models are available in plenum-rated indoor, or outdoor enclosures.

The Colubris Operating System

Resident in all CIMS components, the Colubris Operating System (COS) brings together the distributed intelligence of the TriPlane Architecture to create a rich multi-service WLAN system (Figure 6). Standard Utility Services provide the basic “plumbing,” including multi-layer security, QoS, RF management and virtual LAN extension. Modular Value Services furnish higher-layer capabilities such as public/guest Internet access, secure virtual private networks, multimedia transport and mobile business applications. Tunable parameters let network operators configure WLAN support for still-valuable legacy devices.

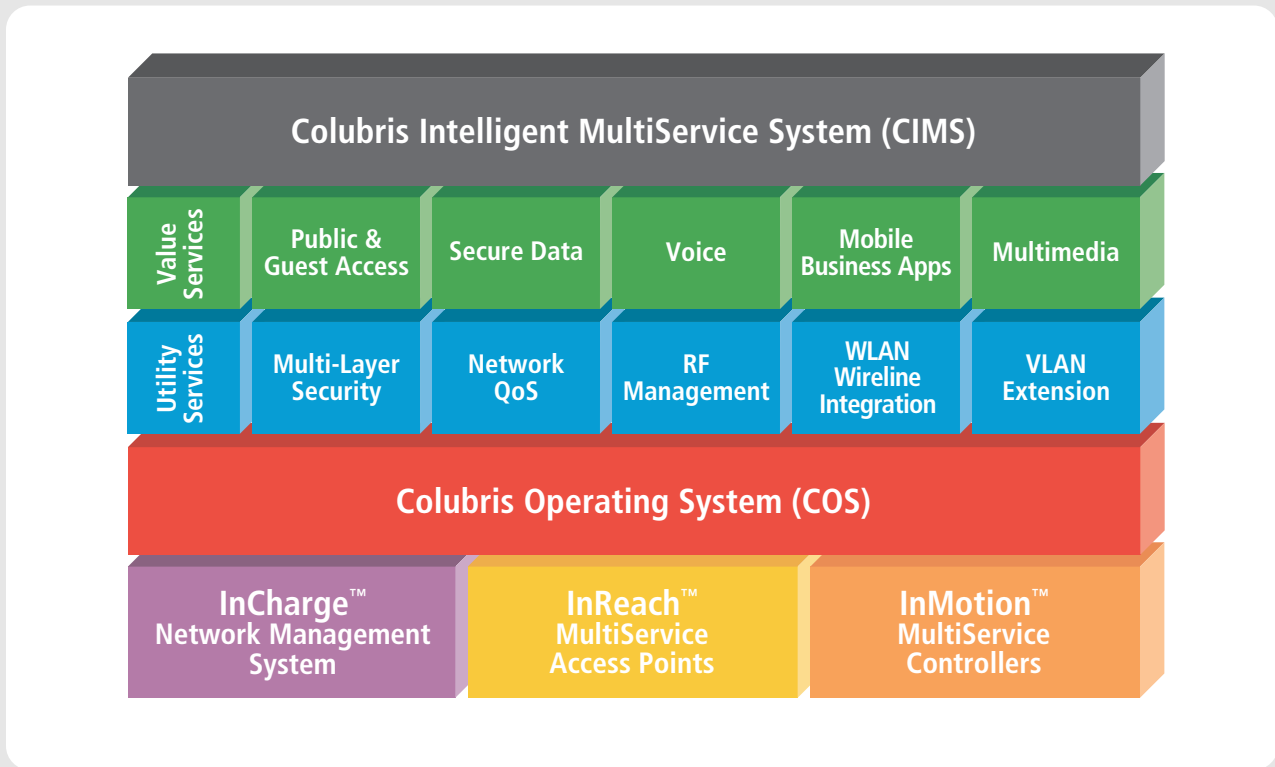


Figure 6: The Colubris Operating System creates a rich multiservice WLAN system.

COS features an XML/SOAP-based API that allows third-party applications to monitor and control WLAN operation. An IP PBX, for example, could retrieve real-time performance and QoS information and gracefully refuse a voice call if the RF signal is too weak or the AP is too busy with other calls. The PBX could also access location information for an E911 call. A PBX could even instruct the WLAN to preempt existing traffic and force through an emergency call.



200 West Street
Waltham, Massachusetts 02451
Phone: +1 781 684 0001
Fax: +1 781 684 0009
E-mail: sales@colubris.com

www.colubris.com

Copyright © 2000-2005, Colubris Networks, Inc. All rights reserved.
All trademarks are the property of their respective owners.