



Unified Wired and Wireless Visibility and Control

There is nothing more important than our customers.

Unified Wired and Wireless Visibility and Control

Enterprise Wireless LANs (WLAN) deliver significant business advantages; including increased knowledge worker productivity, enhanced virtual collaboration and the facilitation of next generation unified communications. However, because WLAN networks are almost always deployed alongside existing wireline infrastructures, it is essential to unify wired and wireless access management and policy controls in order to achieve these advantages. This is particularly the case as organizations rollout Network Access Control (NAC) and Security Information and Event Management (SIEM) solutions, and as Voice over IP handsets become WiFi enabled.

Key issues to address when deploying an enterprise class WLAN that integrates with, and enhances, your existing network and security infrastructure are:

- Implementing Authentication and Policy Based Control
- Migrating to Wireless Switch based WLANs
- Building a Scalable, Future Proof Solution
- Using Location Services for Security and Management
- Controlling Rogue Access Points
- Finding Vendor Expertise in both LAN and WLAN Solutions

This Whitepaper reviews the business and operational challenges faced by the IT team when planning a WLAN rollout to enhance the existing LAN infrastructure. It proposes some highly effective methods for controlling LAN access and leveraging edge-based traffic control policies for system-wide security. And it recommends some best practice implementations, based on Enterasys' long heritage of developing integrated LAN and Wireless LAN solutions.

Authentication and Policy Based Control

When planning a scalable, enterprise-class Wireless LAN, the primary objective should be to deploy a WLAN solution that has been designed and built for seamless integration with the existing wireline network. Specifically, this solution should use the same directory authentication, management software and policy-based control mechanisms for both LAN and WLAN infrastructures. Both sides of the network should be effectively managed as one contiguous entity to greatly simplify security, management oversight and troubleshooting. The solution should enable the easy deployment of Network Access Control, enforce Acceptable Use Policies and audit network activity – regardless of the method used for network access.

In reality, the differences between the LAN and WLAN control systems are enough to prevent the WiFi components from utilizing the same authentication directory and policy management platforms. In this scenario IT operations must implement and maintain a separate back-end directory and policy management control system designed specifically for the WLAN. The capital investment, ongoing costs and management complexity of operating parallel control systems can quickly get out of hand.

Enterasys RoamAbout WLAN products address these authentication and policy based control challenges. RoamAbout uses the same policy “triggering mechanism” (known as the FilterID RADIUS return attribute) as Enterasys' Secure Networks™ switches and management applications – so that the WLAN and LAN infrastructures can truly be managed as a single system. Mobile users have the same priorities and privileges regardless of whether they connect wired or wirelessly. Enterasys Secure Networks offers business-oriented, policy-based visibility and control of users and applications; in contrast to competitive approaches which require technology-oriented manual configuration of access control lists (ACLs) on each device for individual ports and VLANs.

Migrating to Wireless Switch Infrastructure

Recent years have seen the development of an entirely new type of WLAN. Traditional “Thick Mode” WLAN Access Points (APs) operate by making traffic switching, forwarding, policy, management and other decisions independently. While these solutions provided effective mobile connectivity, management challenges plagued operations, and scalability was limited. Specifically rogue access point detection, traffic load balancing, inter-subnet roaming, location-based services and various self-healing capabilities all proved challenging with thick mode deployments.

In response to these limitations many vendors developed “Thin Mode” WLAN architectures which allow access points to operate in a collective framework that is coordinated from central “controller” devices. In this case access points are able to work together as a single system, to alleviate the management and operational issues mentioned above.

Using the Thin Mode architecture all traffic to and from a particular Access Point travels back and forth through the central controller, regardless of traffic type (e.g. voice, video or data) or destination (same Access Point, different Access Point or wireline device). This produces a suboptimal traffic flow with potential single points of failure. A solution to these problems is a “Hybrid Mode Architecture” that leverages the best attributes of both Thick Mode and Thin Mode WLANs. In hybrid mode, control-plane management traffic goes to the controller while voice/video/data payload traffic communicates directly between the source and destination once the flow/connection has been established. Hybrid mode also ensures the throughput and latency of the entire wireless infrastructure is not constrained by the capacity of the controllers.

Enterasys RoamAbout offers a complete portfolio of Thick, Thin and Hybrid mode WLAN solutions that are designed for interoperability with one another, and with Enterasys Matrix and SecureStack switches. The solution uses an integrated suite of management applications to simplify configuration and operations. Many of the components - including Access Points, antennae and network management software – are used in thick or thin mode to greatly simplify the seamless migration from one mode to another.

Building a Scalable, Future-Proof Solution

As with any technology deployment, Wireless LANs should be implemented in a manner that ensures scalability – and protects investments over time – by adapting to new business realities. Some emerging WLAN technologies include location-based asset tracking, VoIP via WiFi-enabled handsets, cellular convergence, and high speed IEEE 802.11n class networks. Each of these technologies promises productivity gains and cost savings, so it makes sense to ensure that your WLAN deployment is “future proofed”. Every WiFi investment made today must protect your financial and knowledge investments into the future.

With 15 years of wireless networking experience, Enterasys is distinguished not only in terms of knowledge and expertise, but also in terms of innovation and thought leadership. Enterasys was the first and only vendor to provide unified identity-based controls across the wired and wireless network. Other industry firsts include first dual-band Access Points, first WLAN SNMPv3 support, first 128-bit encryption and first Power over Ethernet powered Access Points.

RoamAbout is made to meet future business requirements. Every RoamAbout wireless switch controller has the capability to support the forthcoming IEEE 802.11n high-speed standard with a simple software enhancement. RoamAbout’s Direct Path Forwarding feature offers significant advantages in traffic-flow efficiency and low latency for voice/video applications. Enterasys WLAN solutions preserve the financial and knowledge investments of our customers through an architecture that delivers long technology lifecycles.

User Location Services for Security and Management

On a wired LAN locating a specific user or device is a relatively straightforward procedure. For a WLAN there is no physical connection between the user and the Access Point, so a user may be located anywhere within range of the AP. Technologies such as RF triangulation and automated topological mapping may be used to locate end systems. Then, depending on the accuracy of site surveys and RF propagation calculations, end systems may be pinpointed to within several meters. Results can be unreliable, creating problems for applications such as retail inventory tracking, healthcare medical cart tracking, and E911 emergency location services.

Enterasys RoamAbout offers both integrated and partner-sourced technologies for user, device and asset location services. RoamAbout includes native capabilities to pinpoint the location of WiFi enabled devices as well as rogue Access Points. RoamAbout Switch Manager (management software) can even compile a precise physical “heat-map” to display the whereabouts of a given target entity. In addition, RoamAbout supports tight integration of RFID location services from a number of technology partners including EKAHAU, AeroScout and Newbury Networks.

Controlling Rogue Access Points

Sometimes users (employees, students, contractors) seek to build a personal WLAN by connecting inexpensive consumer-grade Access Points to the organization's LAN or WLAN infrastructure. This action creates major security and management headaches for the IT Operations team. Most organizations forbid these maverick Access Points, but locating and neutralizing them can be a major challenge. It is essential for system-wide confidentiality and information integrity that rogue APs are proactively detected and automatically disabled.

There are two approaches used to implement rogue AP detection and suppression for an enterprise class WLAN: construction of a parallel overlay network, and integration of rogue AP control measures into the existing WLAN infrastructure.

- **Parallel Overlay** – This technique builds a completely separate WLAN within the same physical area as the primary WLAN. The overlay network is a passive system whose mission is to listen for rogue APs. When a rogue device is detected the overlay network coordinates various countermeasures to block users from connecting to the rogue AP, and to notify the network operations staff of its existence. Overlay networks are very effective in countering the rogue threat, but at a significant additional cost.
- **Integrated Rogue Control** – A far less costly approach, and just as effective if implemented correctly. However the technology necessary to effectively integrate rogue detection and suppression into an operational WLAN is not widely available today.

Enterasys RoamAbout's rogue AP control leverages the best attributes of both overlay and integrated methods. Implementation typically involves the deployment of a small overlay network, augmented by the primary network Access Points which may be temporarily reconfigured to locate and suppress a rogue device. RoamAbout solutions offer industry leading rogue detection and suppression capabilities whether deployed as parallel overlay networks, fully integrated rogue detection and suppression, or as a hybrid of both.

The Need for Vendor Expertise in both LAN and WLAN Solutions

When evaluating WLAN solutions seek out a vendor with proven experience and expertise not only in wireless systems, but also in wired Ethernet infrastructure. As we have discussed, these networks are complementary and security / management / deployment interoperability challenges must be addressed in order to deliver a seamless user experience. Wired and wireless networks are not entirely self-contained, and the quality of professional services and troubleshooting assistance is directly correlated to the knowledge and experience of the selected vendor.

Enterasys has in-depth experience and a long track record in deploying LAN infrastructure, WLAN infrastructure, and seamless LAN / WLAN solutions. Our Engineers and Global Technical Assistance Centers have extensive knowledge of both LAN and WLAN systems. Enterasys leverages this history and experience to provide customers with the best LAN / WLAN technical support in the industry.

In Conclusion

Enterasys has designed RoamAbout WLAN solutions to address each of the challenges outlined above. Enterasys has created a comprehensive LAN and WLAN product portfolio that provides seamless integration in a manner that is practical, achievable and delivers rapid time to value.

Enterasys RoamAbout is a complete WLAN solution that delivers continuous identity-based security and priority controls regardless of thick, thin, or hybrid modes – fully integrated with the wired infrastructure. Enterasys has a proven track record of “industry-firsts” in every aspect of wireless technology. RoamAbout is ready for 802.11n and will adapt to meet new requirements over time.

Let us show you how we can protect the confidentiality, integrity, availability and performance of your wireless infrastructure and the business users that rely on it.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



Thought Leadership

Over 500 global patents

© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.



Delivering on our promises. On-time. On-budget.