

# Securing the Wired and Wireless Network

---

## Flexible Security for Networks

### Abstract

Many of today's WLAN security issues stem from a lack of integration with the underlying enterprise wired network. In these situations users and devices need to be independently monitored based on location and authentication method. Extreme Networks® unified wired and wireless security architecture provides flexibility without sacrificing network security. This network environment supports a wide variety of devices-wired and wireless-with many operating systems, radio types and drivers.



## The Security Balancing Act

Network security has always been a balancing act between ensuring the safety of corporate resources and maintaining the functionality needed. In the wireless domain, there is an added facet to this—a heightened concern about added potential for security breaches. There are tales of successful “war driving” through corporate parking lots to find open and unsecured Access Points (APs) into corporate networks.

There is also good news in that significant strides have been made to secure wireless access. On a technical level, in fact, the main security problems for wireless access have essentially been solved. If anything, the pendulum now swings the other way, replacing the security vacuum with numerous ways to adequately protect a wireless network. The standards now being rolled out use vastly improved encryption methods that are strong enough to be approved for use by the Federal Government.

Still, IT groups are realizing that although the issues surrounding wireless security (wireless encryption and authentication) are significant, it is only a single component of the overall security picture. Solving the problems related to protecting data privacy and network identity over the airwaves has removed a major barrier to widespread adoption, but IT administrators need more pieces to solve the entire security puzzle.

For wireless access to be practical in today’s enterprise network, it needs to satisfy several other requirements that are best addressed in a wired and wireless network architecture encompassing the wired network already in place. The security solution must address the functional requirements of the existing campus infrastructure, and must also be a flexible solution that can be implemented with the existing network.

## Fulfilling the Security Requirements of Wired and Wireless Infrastructure

Though the exact needs that come out of the security policy differ from one company to the next, there are definite core requirements essential to securing the network. These are summarized as follows:

**Authentication and Policy Requirements:** Allow the right people in the network and keep the unauthorized people out. Can users be allowed access to both wired and wireless networks in a single step? Can people be given different privileges based on who they are, where they are, or what time they’re trying to use the network? Does a given solution easily integrate with the existing backend infrastructure and not require a wholesale upgrade?

### Practical Considerations in Securing the Network

It is well established that wireless equipment vendors need to provide authorization and encryption for secure connectivity to

the enterprise. Other security requirements depend on unique business needs of the company, as well as realistic implications such as budget, operational impact and user education.

### Balancing Ideals with Realities

There are several questions to be considered when identifying business requirements for network security:

- Which network resources need to be protected (and to what degree)?
- Who should access these resources (can these requirements be generalized into user groups)?
- Are there other dependencies beyond identity (such as time and location) to be considered in granting access?

Then there are a few additional questions to consider from practical standpoints such as implementation, operations and budget:

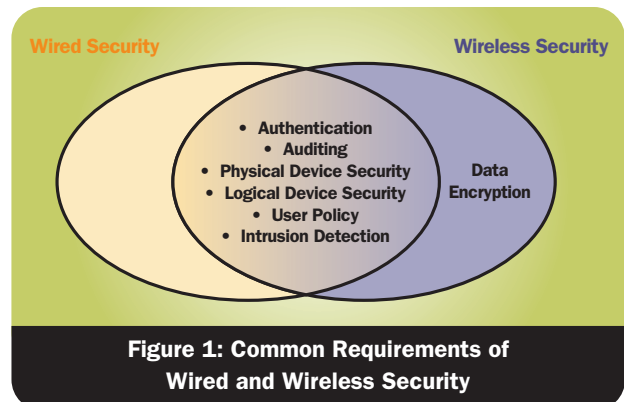
- Which operating systems and hardware platforms are currently deployed in the network?
- How much resource can be devoted to ongoing network management?
- To what extent can clients be upgraded to improve security?

To develop an adequately secure but flexible network that can be implemented, ideal and practical considerations need to be balanced. Once a workable set of parameters is established, they become the makings of the network security policy, which then sets certain requirements for the network vendor.

### Wired Versus WLAN Requirements

The requirements of wired and wireless access have a great deal in common. From a security perspective, the main difference is that a wired network is assumed to be safe from eavesdropping whereas in a wireless network, it is assumed that all bits are open for all to hear.

Most security requirements are common to your wired and wireless APs. Data encryption, of course, stands out as uniquely oriented to wireless, but the tools to address this must not preclude the many common requirements of authentication, intrusion detection and flexible policies (See Figure 1).



**Figure 1: Common Requirements of Wired and Wireless Security**

For example, when developing a security policy, a single, unified policy is needed—one that is relevant for both the wired and wireless components of the network.

**Privacy Requirements:** Make sure that the data sent over the network is not being intercepted and read by others.

- **Rogue AP Detection and Removal:** A wireless signal serves as an open invitation to those unwelcome individuals who—at a minimum—want a free ride on the Internet, but who could also steal corporate information and damage the organization in other ways. The network infrastructure needs to report these issues and give direction as to how to solve them. A part of this requirement also involves ensuring that the network is immune from Denial of Service (DoS) or intrusion attacks.
- **Scalability:** The solution needs to scale, especially in terms of being able to implement authentication and protocols for greater numbers of users. The policy solution should be easily implemented with the existing campus environment, and should readily handle changing proportions of wired and wireless users.
- **Physical Security of the Network Equipment:** What protections are in place to make publicly-exposed equipment difficult or impossible to steal?

The following sections discuss these principal requirements and the method Extreme Networks uses to handle them.

## Authentication and Policy

A network access authentication protocol uses identity to allow or deny access to a network (wired or wireless). The acute need for authentication support in wireless access is due to the fact that unauthorized individuals can attempt to gain access from all sorts of locations—the parking lot, for instance, or the coffee shop down the street.

## Types of Authentication Protocols

Before exploring the authentication offerings of the latest standards, consider the authentication options of the past:

- **None:** For most home wireless networks and many wired networks, this is what is used today. This is not to say that wired access to the network is completely open, because these networks often require Network Operating System (NOS) authentication (i.e. Microsoft domain access), which allows access to file servers and email. A recent survey found that over 40% of participants in a wireless conference did not turn on wireless security while at the conference.
- **MAC Filtering:** A MAC-based approach is not a true authentication protocol because access is based not on the user's identity but on the hardware (MAC) address of the device trying to connect the user to the network. Though MAC authentication seems simple, in reality it is very difficult to manage MAC lists; furthermore, MAC addresses can be easily spoofed.

As neither of these methods is secure enough for enterprise wireless access, 802.1x and the Extensible Authentication Protocol (EAP) provides a flexible framework for centralized, key-based authentication. 802.1x and EAP facilitate mutual authentication between a client and a RADIUS server, dynamic and secure encryption keys, and centralized control of policies.

Various EAP authentication methods include Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS) and EAP with Tunneled Transport Layer Security (EAP-TTLS). Table 1 describes these protocols, along with their uses, infrastructure requirements and supported platforms.

**Table 1: Authentication Protocols and Their Effectiveness**

Authentication Protocol	Security Rating	Network Infrastructure Requirements	Supported by Client Operating System
None	None	None	Yes
MAC	Easily defeated	None	Yes
802.1x/EAP-MD5	Defeatable in wireless (okay in wired)	RADIUS Server	Win2000, Win XP, Linux, third-party client software on the other platforms
802.1x/EAP-TLS	High	RADIUS Server, full PKI deployment (client and server digital certificates)	Win2000, Win XP, Linux, third-party client software on the other platforms
802.1x/EAP-TTLS	High	RADIUS Server, limited PKI deployment (server digital certificates only)	Third-party client software on the other platforms
802.1x/PEAP	High	RADIUS Server, limited or full PKI deployment	Win XP, Win2000, Linux, third-party client software on the other platforms

It is apparent that access authentication is required for wireless access, but it is quickly becoming a necessity for wired access as well. The proliferation of laptops and portable handhelds with wired Ethernet access means that anyone visiting the enterprise campus could easily attempt to “plug-in” and explore the network. Even if rogue users cannot authenticate into a NOS, they can still be given an IP address and be allowed to poke around the network. A unified security solution should integrate some form of EAP support into the authentication mechanisms employed by the traditional wired network.

Unifying wired and wireless network access keeps the user experience in sync, and better secures the wired network. Like its wireless counterpart, wired authentication seamlessly logs into the NOS as well—maintaining the convenience of a single sign-on.

Given these options, a good rule of thumb is to consider 802.1x with PEAP; in most cases, this will provide the best authentication with the widest set of platforms supported.

### Authentication Options for Wired and Wireless Networks

A major concern about deployment of advanced authentication protocols is whether the client stations are ready for it. Extreme Networks security features allow all users, regardless of operating system or different versions of NIC drivers, to authenticate themselves to the network. Customers can choose between Extreme Networks highly secure (and no upgrade) Network Login with SSL for legacy clients and 802.1x (with PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) whenever client support exists.

This provides maximum flexibility for IT managers to choose the best method for the scenario at hand. Furthermore, these authentication types are supported in both the wired and wireless ports, allowing network users to have a common experience, regardless of the media they use to log in. IT managers only need to create a single authentication infrastructure.

A Captive Portal transaction (Figure 2) provides secure authentication to clients with a standard IP stack by redirecting the user to a SSL encrypted browser login form.

This is an excellent choice for environments—such as a university campus or a conference room with visitors—where access to the network is given to users but have no control over the laptop.

Although authentication into the network has focused on the one-dimensional aspect of identity, equally valid qualifiers for access are location and time. For example, a hospital visitor may have the rights to use the wireless network for Internet browsing in a conference room, but nowhere else. On a corporate level, users may be allowed wireless access during normal business hours, but not after hours.

As administrators of medium to large networks know, making a strategic choice about what the client technology the user base should use is an important step in establishing a cohesive and consistent security policy. There is always a migration period, as there is no “flash cut” for the edge of the network. Given this reality and the heterogeneous user base, it makes sense to choose a wireless access vendor that allows for all authentication methods to be used. With its unified wired and wireless architecture, Extreme Networks provides multiple authentication types on the same wired and wireless ports.

### Policy

The need for a security policy to take into consideration that there are many different types of users in a network is based on the fact that network access and authentication rights do not fall neatly into “yes, you can have network access” or “no, you cannot have network access” categories; there is a need to provide a continuum of network resource access depending on who the user is, and how much you trust the authentication and encryption method used by the user.

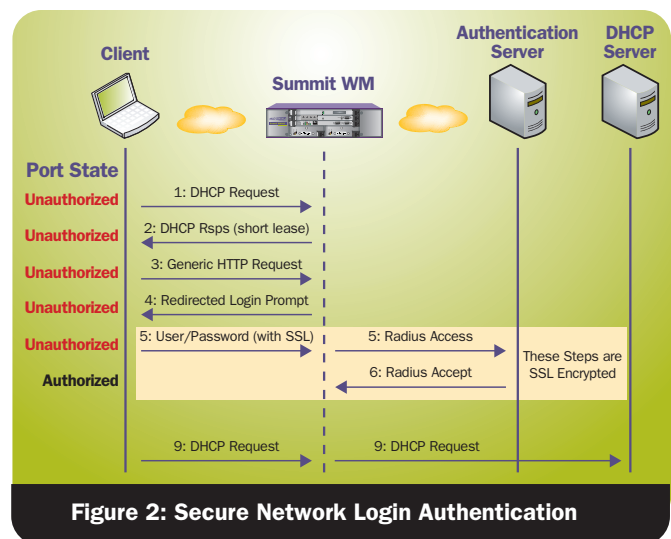


Figure 2: Secure Network Login Authentication

Policy networking has two components: trigger mechanisms and enforcement methods. The policy trigger mechanisms are parameters or conditions that a switch watches for, in order to classify the user for subsequent appropriate treatment.

The types of variables that may be used as a policy trigger are described in Table 2.

**Table 2: Policy Triggers**

Policy Trigger	Why This is Important
User Credentials (e.g., user/password, digital certificate)	This is the fundamental trigger traditionally used.
Location	Allows the set up "policy hot-spots," where certain users can use the wireless network and others are blocked.
Time	Allows establishment of time based access.
Authentication Type	Not all pathways into the wireless network are totally secure. For the less secure entry points (such as WEP or Open Access), make sure users are allowed in, but appropriately restricted.

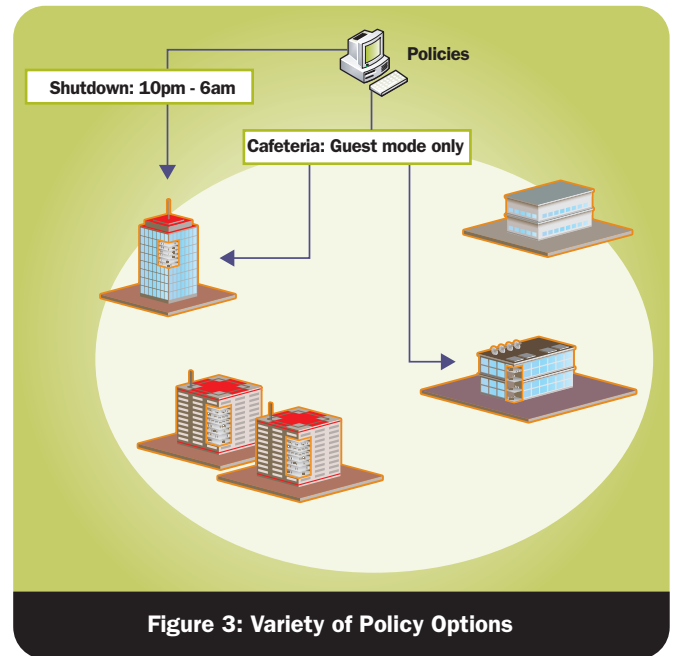
The second component of policy networking, policy enforcement methods, defines the actions and privileges allowed to a user once a trigger condition has been met. These actions include creation of VLANs, Access Control Lists (ACLs), end-to-end Quality of Service (QoS) settings, and rate limiting. These tools and their uses are discussed in Table 3.

### Policy Networking Solved

Extreme Networks unified access implementation is designed to provide less secure users with appropriate network access, while fully trusted users are given the access that they need. Upon authentication, users can be placed into pre-configured VLANs with established ACLs, or

**Table 3: Policy Enforcement Methods and Reasons for Their Existence**

Policy Method	Why This is Important
VLAN Placement	Depending on the policy triggers met, the user can be set in a trusted or non-trusted VLAN.
Layer 2 – Layer 4 ACLs	Based on the policy, restrict or allow access to network resources.
QoS	Based on the policy, certain users can be given higher priority than others.
Rate Limiting	Based on the policy, certain user groups can have bandwidth limited to protect consumable resources, such as wireless capacity and Internet access.



**Figure 3: Variety of Policy Options**

Policy Manager by EPICenter® can apply per-user policies complete with individual ACL, QoS, and priority values (See Figure 3).

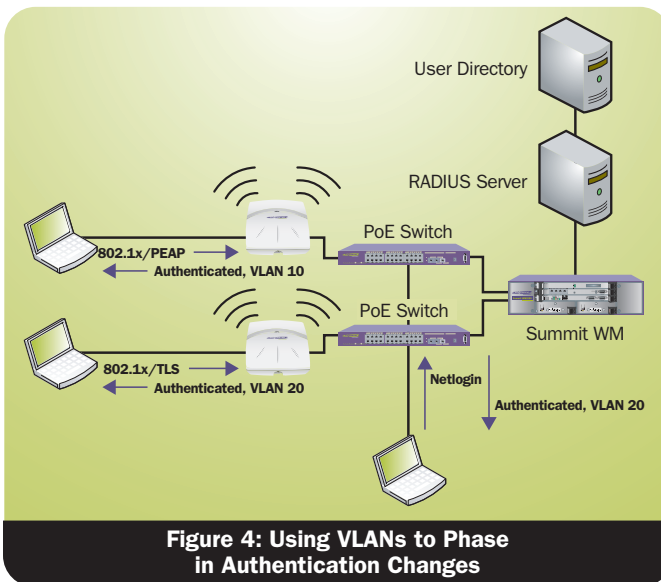
With unified wired and wireless, a user can be placed into a VLAN based on the security of the authentication type. For instance, users authenticating with WPA or WPAv2 are in a different level of medium encryption as those authenticating using WEP, NetLogin or Wi-Fi Protected Access Pre-Shared Key (WPA-PSK); the latter group would thus be segregated into VLANs with fewer access privileges. Of course, if those same users logged in using a higher level of authentication and a stronger encryption method, they would be given full network access (See Figure 4).

Extreme Networks assigns fully trusted users (i.e., ones that have authenticated via WPA or WPAv2) to their specific VLAN regardless of where they are in the network, or how they access the network (wired or wireless). VLAN information—such as credentials and passwords—can be stored together on a RADIUS server or in an attached directory. Once the user logs in through 802.1x, the VLAN associated with the user is loaded from RADIUS and applied to the wired or wireless port. Thus, a member of engineering or marketing feels at home from a network perspective, whether logged in as a wired or wireless user.

**Table 4: VLAN Assignment Based on Authentication Method**

Authentication Method	VLAN Directed To	Application
None	“Guest VLAN”	This is appropriate for providing convenience Internet service for users in a corporate lobby.
Network Login	“Guest VLAN”	Provides a “Guest” service but requires a user login.
WEP	“WEP VLAN”	WEP’s security holes are well documented.
WPA-Pre-Shared Keys (WPA-PSK)	“PSK VLAN”	Though WPA is a solid standard, the reliance on static keys makes it unacceptable for true security.
WPA (aka TKIP/RC4)	User Based VLAN	VLAN placement is based on user or group profile.
WPAv2 (aka CCMP/AES)	User Based VLAN	VLAN placement is based on user or group profile.

Figure 4 shows how this allows flexible migration; authentication changes are phased in on a per-VLAN basis.



**Figure 4: Using VLANs to Phase in Authentication Changes**

Another facet of policy networking is applying customized treatments to the VLAN, thus ensuring that users who are not trusted are properly restricted—usually with ACLs—in their access privileges. Summit® WM provides fully qualified ACLs—called filters—that can be applied to any VLAN and user.

For service differentiation, users can also be tagged with 802.1p priority assignments. This tag enables strict prioritization in the wired network, or for implementing rate limits for certain user classes.

## Encrypting for Privacy

The concept of encrypting data traffic in the enterprise is new with wireless; in traditional wired Ethernet, data is transported over physical wires or fibers, hidden from all but the most ambitious snoopers. In contrast, wireless is a shared medium open for everyone to hear; data encryption is paramount, and that is where privacy protocols come in. A privacy protocol is a method of encrypting traffic to ensure that people cannot intercept and read the information. The overall security of a privacy protocol depends not only on the strength of the encryption algorithm, but also on the method by which the secret keys are exchanged.

### Privacy Protocols

There are several choices in privacy protocols; the ones most likely to be relevant are broken down as follows:

- **No Encryption:** No security.
- **Wired Equivalent Privacy (WEP):** The “Shared System Access” defined in 802.11. WEP uses the RC4 encryption algorithm (the same one used in SSL), but because WEP makes it easy for a snooper to recover the keys, this protocol is easily cracked.
- **Temporal Key Integrity Protocol (TKIP):** Designed as a software upgrade for most WEP systems, it patches most of the holes in WEP and is considered to be fairly good security, as long as dynamic keys are used.
- **CCMP/AES:** The holy grail (thus far) of privacy protocols. The AES encryption algorithm is expected to serve the encryption community for the next 30 years and is NIST approved standard used by all government agencies. Incidentally, this is a resource-intensive protocol that will perform much better on hardware with built-in AES encryption.

At present, CCMP/AES is considered the best bet for privacy. These attributes are summarized in Table 5.

**Table 5: VLAN Assignment Based on Authentication Method**

Protocol	Security	Standardized	Requires Hardware Assistance	Client Driver Support Available
No Encryption	None	NA	No	NA
WEP	Easy to Crack	Yes	No	Yes
TKIP/RC4	Secure	Newly	Probably Not	Increasing
CCMP/AES	Highest	Nearly	Yes	Not Yet

## Extreme Networks Privacy Options

Extreme Networks supports all types of 802.11 standards-based security. Our implementation allows for existing users—with their existing drivers—to use the network. Encryption is achieved using either WEP within the framework of WPA/TKIP, for simple devices such as phones and scanner guns, or AES (from 802.11i) for stronger encryption going forward. Extreme Networks is ready for the most advanced and strongest form of security: CCMP with AES.

Encryption is done directly in Altitude APs, so Summit WM can handle up to 200 APs per Summit WM with full AES encryption.

## Rogue AP Detection

Wireless networks are notoriously interesting targets for hackers. Although most culprits are probably just seeking a free ride on the Internet, a smaller group has the more destructive goal of disrupting network operations, destroying corporate data, or perhaps worst of all stealing sensitive corporate secrets.

Though numerous things can be done to prevent intruders from ever getting into the network, many aspects of network security are inherently at the mercy of the individual user; passwords, for example, can always be stolen if not properly secured. Therefore, a security solution needs to have sufficient support to protect against intrusion.

A “rogue” can be either a person or device that is attempting (or succeeding) in gaining unauthorized access to the network. There are a number different varieties of rogues, including employee-installed APs for the purpose of getting wireless access outside of IT’s guidance, or APs installed by malicious individuals for the explicit purpose of luring authorized users to it, to perpetrate a “man-in-the-middle” attack. A totally separate wireless network is also considered a rogue network, not because it compromises enterprise data security but because it can cause radio interference with the authorized corporate network. Rogue wireless users will try to connect to an employees’ wireless card if the card is configured in ad hoc mode (i.e., Peer-to-Peer network mode for wireless).

For protection against rogues, a way is needed to detect their radio signatures. This can be done by physically walking the campus with a wireless sniffer, or installing a separate wireless sensor network for the exclusive purpose of constantly listening for rogues. Alternatively, an active scanning mesh could be created, using the AP network to flesh out both rogue APs and ad hoc networks.

Another aspect of hacker handling is the ability to restrict users from entering the network from (for instance) the parking lot, and being able to determine if multiple users

are logged in using the same password. Finally, there is the question of simple device hacking, and how to protect wireless devices from the same types of DoS attacks that plague the rest of the network.

## Extreme Networks Offerings to Handle Hackers

With a security solution from Extreme Networks, IT managers set policies and thresholds to detect rogue APs and provide users with selective “allow” or “lockdown” capabilities for stricter authentication. Flexible lockdown is important in a large enterprise, where legitimate third-party vendor devices coexist with rogue APs. Rogue APs can immediately be isolated while allowing uninterrupted operation of legitimate APs.

In essence, an IT manager “secures the air” in the same way that a physical port is secured. This helps protect corporate resources, regardless of the medium (wireline or wireless) used for intrusive access. With more flexible authentication and encryption services available, tunneling approaches such as Virtual Private Networks (VPN) are no longer necessary.

Extreme Networks Altitude wireless ports can form a mesh of rogue AP detectors. This is an inexpensive way to pro-actively scan and probe the air to detect any rogue APs or ad hoc users in the neighborhood.

Rogue detection is efficiently implemented so that minimal time is spent away from serving legitimate users; it can be initiated on request or scheduled at intervals, and you can control the amount of time that Altitude spends looking for rogues.

Once the AP has scanned its frequency range, results are reported to EPICenter®—the unified wired/wireless element manager from Extreme Networks—which sorts through the list of discovered APs, subtracts the ones that it already knows about, and then alerts IT staff of additional or new rogues (see Figure 5).

Rogue AP Address	Manufacturer	SSID	Encryption Method	Location
00a2168bc612	Cisco	15	None	Sw A; Port 15
130065f7d219	NetGear	1	WEP	Sw J; Port 43
093d442e0a35	D-Link	1	None	Sw S; Port 8

**Figure 5: Rogue AP Report**

Because EPICenter is a unified access element management system, it also searches the wired network to find out if the suspected rogue AP is connected to a wired port. The IT administrator only has to disable the port, and the rogue AP is inactive. EPICenter also watches out for multiple login sessions of the same user. If it detects multiple users using the same password, an alert is passed up to the IT staff.

Every Altitude AP keeps a record of every end station it sees, whether it is associated with that AP or not. These tables are sent to EPICenter, which dutifully removes all the end-stations that are legitimately associated somewhere, and the resulting list is the set of stations that are active from a radio sense, but are not logged into the network.

Enterprise wireless networks are typically designed so the entire building receives good signal coverage. The only place where signal strength falls off is outside the building—places where the legitimacy of the user trying to connect is more suspect. EPICenter can be programmed to alert IT staff if it finds people trying to associate who are below a certain signal strength level. As the data that connects to an AP is directly related to the signal strength, Extreme Networks Summit WM can be configured so that it will not allow lower data rates. This effectively cuts off network associations in places where there is bad coverage.

Finally, Extreme Networks provides a variety of ways to record events as they happen. Not only are security and authentication-related items being set up to the robust alarm management system in EPICenter, but Syslog and SNMP traps can also be issued to a variety of IT specified destinations (such as advanced correlation engines or dedicated event managers such as NetCool).

For advanced intrusion detection and prevention, Extreme Networks suggests that IT staff consider implementing tools such as SpectraGuard® Enterprise from AirTight® Networks

## Scalability

Though securing an individual device may be very straightforward, individually securing hundreds of them is unmanageable and lends itself to security compromises because something was missed—therefore, a security solution has to scale in order to be effective. Though wired and wireless network access have areas of differing requirements, the ultimate goal for scaling network access security is to unify wired and wireless security under a single security umbrella.

When securing wireless networks, solutions that seem appropriate at first eventually fail when cast against scalability requirements. For instance, VPN methods originally designed for allowing remote access into the corporate network through the Internet present tremendous scaling issues when they are used as the secure tunnel for wireless clients. The sheer numbers of mobile devices on the hori-

zon—such as tablet PCs, PDAs and wireless IP phones—indicate that any encryption has to scale in a way that traditional VPNs and their rigid tunneling techniques do not.

Extreme Networks unified wired and wireless security implementation is scalable both in terms of encryption and management. As the AES or RC4 encryption is performed in hardware directly on Altitude APs, factor in terms of the number of authentication and encryption does not become the limiting APs for Summit WM even when all the APs are running the highest level of encryption.

The effectiveness of any security implementation is directly tied to the number of physical devices that need to be secured. As Extreme Networks unified architecture centralizes Altitude management in Summit WM, you can manage wired/wireless security worth 2 Gbps of bidirectional capacity with a single device.

## Physical Security of the Network Equipment

Physical protection is not such a large issue with wired devices because they are typically locked in wiring closets, and are basically inaccessible; however, APs are exposed in a public area, so physical security is a much more serious issue.

For this reason, all the necessary protections must be in place to make this equipment difficult—or at least undesirable—to steal. Areas of concern include the following:

- How accessible is the AP?
- Can the AP be physically secured to a permanent structure?
- What type of information is on the AP if it is stolen?
- Is there management access available on the publicly accessible devices?
- Can network access be achieved through the network cable connected to the device?

An Altitude 350 -2 AP is protected in several ways to mitigate the key problems caused by its exposed nature.

One aspect is AccessAdapt™ technology built into Altitude. Altitude, by design, lacks any persistent storage. Once it is disconnected from the PoE switch, it loses all configuration and images (however, once you plug it back in, it recovers its configuration from the Summit WM controller). Therefore, an individual stealing an Altitude AP in the hopes of gaining any stored passwords or network configuration will be sorely disappointed. This feature has implications in vertical markets such as healthcare; for instance, where AccessAdapt helps ensure HIPAA compliancy by removing any threat that a patient's records might be stolen along with an AP.

There are a couple of additional security features for Altitude 350-2 as well. Altitudes are never managed individually and there is no console port on Altitude. The only connection to the AP is the powered 10/100 Ethernet connection. Therefore, there is no way for someone to hack into Altitude and interfere with normal network operation. Altitude also comes equipped with a locking tab, so it can be locked to the mounting bracket.

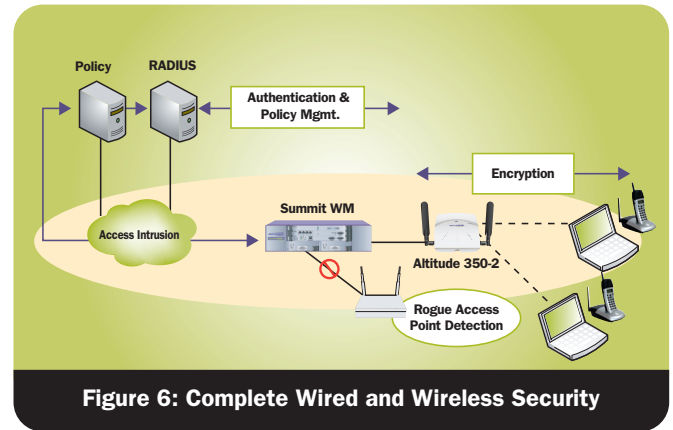
If Altitude 350-2 is going to be placed in a truly compromised area or public location, you can employ a detachable antenna so the Altitude itself is locked in a box with only the antenna exposed.

Finally, a clever individual may try to use the Ethernet cable connecting Altitude 350-2 to Summit WM in hopes that this link is less secure. Because Summit ports act like normal 10/100 ports if not connected to Altitude, the ports are secured from intrusion by 802.1x.

## Conclusion

Securing a network is essentially a solvable problem at this point given the technology currently available; the only remaining issue is how to implement the solution. Extreme Networks integrated security solutions offer secure access that is seamlessly migrated into an existing campus security solution. The techniques for managing wired and wireless access are integrated, and security functionality is robust and easy to administer.

Extreme Networks unified wired and wireless security architecture was built for flexibility. The emerging network environment will contain a wide variety of devices (wired and wireless) with many operating systems, radio types and drivers. Extreme Networks provides simultaneous access to all flavors and types without sacrificing network security.



**Figure 6: Complete Wired and Wireless Security**

- The combination of authentication and encryption mechanisms—with remote AP detection and leading hacker handling capabilities—make Extreme Networks unified wired and wireless security solution a complete arsenal that integrates into the existing security architecture. This scalable solution also minimizes the effect of scalability concerns or physical device protection, as the mobile user base is integrated into the traditional wired campus.
- Unified wired and wireless access control techniques are available based on the unique rules of the enterprise. These include authorization and authentication, cryptographic encryption, perimeter defenses via intrusion detection and monitoring and the auditing of network resources to identify anomalies in their use. This allows legacy security technologies to be incorporated with the new opportunities and challenges presented by mobile access.



[www.extremenetworks.com](http://www.extremenetworks.com)

email: [info@extremenetworks.com](mailto:info@extremenetworks.com)

**Corporate and North America**  
Extreme Networks, Inc.  
3585 Monroe Street  
Santa Clara, CA 95051 USA  
Phone +1 408 579 2800

**Europe, Middle East, Africa and South America**  
Phone +31 30 800 5100

**Asia Pacific**  
Phone +852 2517 1123

**Japan**  
Phone +81 3 5842 4011

© 2007 Extreme Networks, Inc. All rights reserved. Do not reproduce.  
Extreme Networks, the Extreme Networks Logo, AccessAdapt, EPICenter, and Summit are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries.  
Specifications are subject to change without notice.