How Vernier Networks Complements Cisco

The dramatic rise in wireless access to enterprise networks has amplified demand and increased complexity of network usage. Unwired users are more in touch with the network and thus use it more. Vendors, visitors and other guests also can drive up traffic and complicate security measures.

To prevent wireless users from overburdening the network core, securing and managing wireless access requires an evolution of the traditional strategy of handling authentication and enforcing access policies at the core. Today's architectures must utilize layered security at the network edge to provide secure, mobile, manageable access to multiple services on a single network—all while maintaining complete control from the network center

The Vernier Networks System™ is designed to complement existing wired network controls and allow administrators to control and manage wireless networks flexibly, simply, and cost-effectively. Vernier's solution brings control—and intelligence—to the network edge where users connect, while providing campus-wide security with support for seamless roaming. Vernier enables network administrators to precisely control wireless access by user, by location, and even by time of day, making the wireless network as secure as the wired network. This distributed architecture with centralized management allows administrators to apply network access policies appropriately.

Wireless roaming presents challenges for most existing wired networks because they were architected for fixed-location users in controlled access areas. Roaming represents an additional threat to the enterprise network, since wireless users may attach to uncontrolled public networks and pick up viruses or worms that can be then be introduced into the enterprise. Thus it's not surprising that using traditional wired networking methods to control, manage, and secure wired/wireless hybrid networks can result in rigid, difficult to manage, and costly designs that are potentially insecure. In addition, supporting wireless roaming can result in increased network traffic and an unsatisfying user experience.

The Vernier Networks System complements existing wired networks by providing fine-grained access control, centralized management, virus prevention, and hassle-free roaming for wireless users. The Vernier solution drops into existing architectures without requiring the kinds of architectural compromises that can result from using traditional methods. Thus, network managers can fill the gaps in their existing infrastructure and create an integrated, managed, comprehensive wired/wireless architecture. Adding the Vernier solution can enable companies to securely deploy and cost-effectively manage 802.11 networks ranging from tens to thousands of access points.

Go Beyond Traditional Wireless Security Recommendations

To see how Vernier complements existing network infrastructures, let's consider how our solution fits in with industry leader Cisco's product suite and wireless recommendations. Because they are architected to serve non-mobile users, Cisco-based and many other wired networks must rely on less than optimal designs for integrating wireless users. The result can involve the following expensive, complex, and hard to manage solutions:

- Deployment of expensive, non-scalable VPN concentrators
- An increase in broadcast traffic due to placing Access Points in a subnet overlaying the enterprise network
- Use of complex, resource-intensive MobileIP for roaming
- Extensive use of filtering due to increased unauthenticated traffic on the LAN
- Overloaded wireless Access Points

- Reliance on 802.1X with LEAP, which has been shown to be vulnerable to dictionary attacks
- No support for multicast or broadcast for wireless users

In the following discussion, you can see how Vernier's solution fills the gaps in Cisco's product line and leverages your existing investment in the command and control of your network. Compared with other solutions, Vernier greatly decreases cost while simplifying the setup, maintenance, and control of WLANs and improving users' wireless roaming capabilities and experience. Vernier also adds several important capabilities, including tiered levels of access control, intrusion prevention, a network-traffic-aware virus filter, 802.1q tagging, bandwidth management, and Power over Ethernet (PoE) support.

Improve Edge User Architecture

Cisco Recommendation: Cisco's basic approach to securing wireless LANs is to treat wireless traffic like dialup or other remote access from off network. They employ a VPN architecture in which wireless Access Points (APs) are sited in a single subnet outside the firewall in a DMZ. Cisco uses an IPSEC VPN to tunnel wireless traffic across the enterprise network to one or more VPN concentrators. The VPN concentrators authenticate the traffic and route it back into the enterprise network.

Disadvantages: Using VPN concentrators for wireless traffic is an architectural compromise, using a component that was primarily designed to handle high density/low throughput dialup traffic to route traffic from within the enterprise outside for authentication and access. VPN concentrators are not designed to handle the traffic of medium density/high throughput WLANs and thus scaling for performance can be a challenge. Couple this with the fact that concentrators are not scalable in a granular manner, with capacity upgrades typically done in bundles of 5,000 users, and you can have price/performance challenges. But the biggest problem with this approach is an architectural one: VPN concentrators are designed as a single point of entry (and therefore a bottleneck and a single point of failure) and do not fit a broad user edge model that modern networks should embrace if they are to enable efficient management of wireless users. Using VPN concentrators for wireless users also means creating large broadcast domains, which is contrary to traditional, highly subnetted network design.

Adapting an architectural model designed for a class of users (dialup) that have very different characteristics from wireless users represents an architectural compromise rather than state of the art. Plus, VPN concentrators provide no value add specific to WLANs (for example, they don't do virus containment and cleanup).

The Vernier Advantage: Vernier complements Cisco's centralized command and control functions while simplifying wireless LAN management and security by siting wireless **Vernier Access Managers™** at the edge of the network as part of an integrated network edge architecture. Designed to handle WLAN rather than dialup speeds, these edge devices offer centralized, granular access control and management functions without the complexity of a VPN concentrator architecture. By allowing enterprises to terminate VPNs at an Access Manager at the edge rather than through a costly VPN concentrator, Vernier eliminates the need to tunnel traffic across your enterprise network and simplifies troubleshooting. Plus, Vernier's solution is easily scalable: Need more capacity? Add another **Vernier Access Manager™**. Vernier's solution also adds value by providing virus containment and cleanup features (see below for details).

Easily Support Mobility

Cisco Recommendation: Cisco supports wireless mobility using MobileIP, a complex architecture that can result in extra traffic on the enterprise network and an unsatisfactory user experience due to increased latency and other complications. With MobileIP, each user has his or her current effective or "care-of" IP address and a static "home" address. All traffic to and from the user is routed through the home address, which may add one or more network hops and redundant data paths.

Disadvantages: Using MobileIP necessarily increases the amount of traffic on your network, as much as two to three times. This solution also complicates management since move, add, and change implementations now must change a user's home address and VLAN, and relevant ACLs must also be updated. Using MobileIP also requires the installation of client software, with its attendant distribution and update headaches. Finally, due to the complexity of MobileIP, it can take a significant amount of time to complete roaming.

The Vernier Advantage: The Vernier Access Manager doesn't require the use of MobileIP or client-side agents for roaming, instead supporting session persistence across subnets without requiring re-authentication as users move among coverage zones. The Vernier Networks System also adds dynamic tunneling to a Cisco-based architecture. Using Vernier's firewall type NAT translation, only existing session-based traffic from a roaming user is tunneled; all new user sessions are handled directly by the Access Manager. This NAT capability has important benefits for multicast traffic, as you can see below. Administrators can ensure that network sessions are preserved long enough to maintain connections for session-based applications using Vernier Network System's linger timer, which defines how long a session should persist once a connection has been lost due to the user temporarily moving beyond the wireless network's coverage zones. In addition, security association and policy roam with the user. Thus you can accomplish moves, adds, and changes simply by switching users from one access group to another.

Support Multicast and Broadcast for Wireless Users

Cisco Recommendation: One result of Cisco's recommendations is that multicast and broadcast are not supported for wireless LAN users. Although Cisco APs and wireless client cards support multicast, their VPN concentrator does not.

The Vernier Advantage: Vernier augments Cisco solutions by offering Mobile Multicast Support via IGMP version 3.0, which enables WLAN users to have full access to multicast applications even while roaming. The Vernier Access Manager minimizes disruption when roaming by proactively rejoining multicast groups so users don't need to wait 60 seconds to respond to the "all groups" query.

Control Access Without VLANs and Multiple ACLs

Cisco Recommendation: Cisco recommends the use of multiple VLANs with attendant ACLs to segregate wireless traffic. In addition, they recommend placing all wireless APs on the same subnet.

Disadvantages: Not only is creating VLANs an additional cost to the enterprise, it complicates access control by requiring extensive use of static ACL filters to restrict access to VPN traffic only, resulting in complex implementations and high maintenance overhead. In addition, use of VPNs generally locks the enterprise into a single VPN client. Placing all APs on a large broadcast domain is an architectural compromise that increases the load on your network and can choke your APs. Using the VPN/VLAN architecture makes it harder to granularly control the type of access permitted, for example, guest, contractor, and employee. Implementing VLANs is also very complex. Administrators must set them up on every port and every switch.

The Vernier Advantage: VPNs can be terminated at the **Vernier Access Manager™** which controls access at the network edge, eliminating any need to route traffic elsewhere for access control. The device also offers misconfigured service management and proxy redirection that allows secure, transparent login for guests or users who have changed their configurations. Vernier supports any VPN client, including ones based on IPSec, PPTP, and L2TP/IPSec. Vernier adds features including guest access, clientless Web logon, and a number of VPN mechanisms.

Go Beyond LEAP and 802.1X For Authentication

Cisco Recommendation: Cisco recommends using LEAP and 802.1X for authentication and dynamic WEP key management.

Disadvantages: All elements across the network must run the same implementation and version of LEAP, and there are many emerging wireless devices that do not support the protocol, including scanners and Wi-Fi telephones. For Layer 2 roaming within a subnet, LEAP can take longer to roam compared with static WEP. Additionally, Cisco's LEAP protocol has been shown to be vulnerable to dictionary attacks (see sidebar). In addition, the Cisco solution opens a door to the entire network if security is compromised (hacking, identity theft, etc).

The Vernier Advantage: The Vernier Networks System™ supports 802.1X with various EAP extensions including LEAP. Plus, Vernier adds tiered levels of granular access control for greater access flexibility so that not all users are equal. Vernier provides a user-based mobile policy to restrict access to only certain network resources, down to the application level. If the network is compromised, an intruder can only see a small part of the network. Thus damage is limited and the intruder can't use the compromised account as a platform to launch attacks.

Vernier's Complementary Solution

The Vernier Networks System™ fills the holes in Cisco's solution and thus is complementary to a Cisco-centered network.

Vernier provides a distributed thin Wireless Access Layer by siting wireless access managers at the edge of the network, allowing enterprises to terminate VPNs at the edge rather than through a VPN concentrator. The **Vernier Access Manager™** and **Vernier Control Server™** devices transparently integrate with existing network architecture and infrastructure elements and support a wide range of 802.11 equipment. There's no need to build a separate network or security structure just for wireless usage.

Vernier allows for authentication and access control at the edge, while maintaining command at the core of the network. Rather than using multiple static, inflexible ACLs, Vernier's edge-based ACLs enable you to create finely grained levels of access to network resources based on user, group, location and time.

In addition to simplifying wireless LAN management and security, Vernier also offers several value added features that enhance any wireless network, such as:

- 802.1q tagging
- Virus filtering
- Web session redirection
- Bandwidth management
- Expanded support for Power over Ethernet (PoE), including support for Cisco's proprietary PoE scheme

Vernier's advanced **802.1q tagging** allows for tagging and forwarding based on user, group or location to allow you to better manage your network.

Vernier's devices **monitor the network for virus-like behaviors** and can prevent bad packets from getting on to main network, effectively stopping the spread of worms and denial of service attacks. Using Vernier's robust session logging, network administrators can not only see which devices are infected, but also the MAC address, user ID, time, and type of traffic involved.

Once infected users have been identified, an administrator can simply create a user group for the users, deny them access to network resources, and **redirect Web sessions** to a custom web page informing them of the infection and offering links to fixes. Vernier's session logging also enables effective network audits, forensics, trend spotting, and capacity planning.

Vernier's bandwidth management features offer additional control of **network bandwidth utilization** by allowing priority queuing and bandwidth limits to be part of specific user rights enforced by the Access Manager.

Power over Ethernet (PoE) reduces deployment costs and Total Cost of Ownership of Access Points. Vernier's PoE implementation provides remote power and power cycling supporting the IEEE 802.3af draft standard and Cisco's power scheme through built in (not added on) power injectors. Vernier provides support for up to 12 powered Access Points per Access Manager with up to 15W of power per port, enough to power Cisco's power-hungry Aironet 1200 dual mode APs.