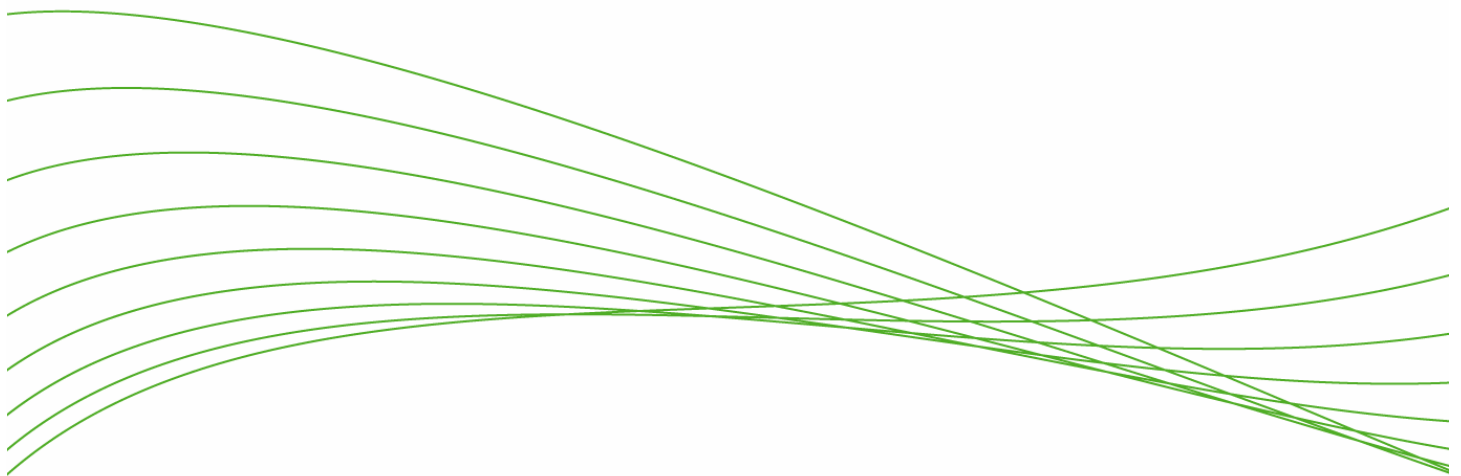


# Extending the Enterprise Network Through Mobility

The Adaptive EDGE Architecture and Mobility Infrastructure Solutions from ProCurve Networking by HP



Introduction .....	2
The Need for Enterprise Network Mobility.....	2
The Evolution of Enterprise Networks to Mobility.....	3
The ProCurve Adaptive EDGE Architecture .....	4
ProCurve Mobility Infrastructure Solutions .....	5
Choice and Flexibility .....	6
Unified Access Control and Management.....	7
Robust Data Privacy .....	7
Guest Access .....	8
Roaming .....	8
Resiliency .....	9
Solution Services .....	10
Enabling Business Applications .....	10
Summary.....	11
For more information.....	12

## Introduction

Connecting and sharing business intelligence in real time is essential for successful competition in today's business world. Many enterprises need seamless network access around the clock as their business borders extend across local area networks (LANs) and around the world.

Network managers address mobility either proactively by design or reactively by default. In some cases, network managers bring wireless access to the network in a controlled and managed way. In others, employees drive adoption by deploying rogue access points, causing administrators to scramble to manage the situation. Whatever the case, it is no longer feasible to delay deployment of mobile solutions. Increasing productivity through wireless connectivity without compromising network security is imperative for today's enterprises.

This paper explores the need for mobility in the enterprise network and the technology issues network managers must address as mobility solutions evolve from the cutting edge to the reality of mainstream use. It also provides an overview of ProCurve Networking by HP mobility solutions, which are highly available, secure and affordable. Based on the ProCurve Adaptive EDGE Architecture™, these solutions enable companies to effectively accommodate the evolution of the enterprise network into an anytime, anywhere resource that adapts to changing business needs with command from the center and control to the edge.

## The Need for Enterprise Network Mobility

Today, mobile network connectivity includes both wired and wireless technologies. Wired connections include LAN ports throughout a building or campus, dial-up connectivity and secure Virtual Private Network (VPN) technology. Wireless LAN (WLAN) technology continues its unabated advancement as an essential enterprise resource.

According to Gartner, "Revenue from sales of WLAN switches and controllers almost doubled year on year (in 2006), to total \$609 million, equivalent to 44% of the market revenue."<sup>1</sup>

Many of the obstacles to widespread WLAN adoption – ease of management, quality of service (QoS), security and resiliency, to name a few – are being addressed with industry innovation and standards development.

"For the near term, because of the rapid evolution of the features of enterprise-class WLAN systems, unified WLAN switches — switches that tout command and control functionality over both the wired and wireless parts of the corporate network — will find their best applications in a subsegment of businesses that are looking to minimize system cost, footprint, and administration," says Jean Kaplan, Enterprise Networks research analyst with IDC. "However, as the features of WLANs become standardized over time and the processing power of networking equipment grows, it will become increasingly attractive to unify the wired and wireless parts of the network to drive manufacturing costs and complexity out of the LAN infrastructure."<sup>2</sup>

Network mobility, both wired and wireless, allows users to have access across a broad range of environments for a broad range of needs. Network mobility solutions provide several benefits, but also bring challenges that administrators must address with a unified, holistic network architecture. Some of the questions and challenges that surround enterprise network mobility include:

- Will data residing on the network and users accessing the network be protected from attacks by hackers and other potential abusers?
- With the addition of mobility, can the network correctly identify and provide access privileges to different types of users and traffic types?
- Can QoS be controlled and bandwidth optimization managed?
- Can the existing infrastructure be leveraged? Will it restrain deployment?
- Will the mobile network infrastructure be flexible enough to meet users' needs while accommodating change and growth?
- Can the mobile network infrastructure support emerging business applications without requiring extensive upgrades?

---

<sup>1</sup> Gartner "Market Share: Wireless LAN Equipment, 2006 (Preliminary Statistics)," February 2007.

<sup>2</sup> IDC, "Worldwide Unified WLAN Switch 2007–2011 Forecast," February 2007.

- How can wired and wireless network investments be consolidated and managed in a unified fashion?

WLANs present a host of benefits and challenges to every organization. Wireless networks are creating efficiencies and reducing costs for not only corporate enterprises, but also a wide array of targeted industries, such as healthcare, education and manufacturing. Although there are advantages and obstacles unique to each industry, there are generically applicable benefits for any organization seeking to deploy WLAN capabilities.

Increased productivity is the most commonly cited advantage of wireless network connectivity. Yet contrary to common belief, the productivity gleaned by WLAN deployments extends far beyond laptop users checking email during meetings. Wireless mobility can rapidly and positively change the way employees work and give them more control over their jobs. With users always on the network, problems can be solved in real-time and overall collaboration is improved. This applies to not only a company's campus workforce but also mobile and remote employees, guests, partners and suppliers.

Coupled with increasing workforce and business productivity, a WLAN deployment can extend a network to areas that were previously unattached to the enterprise infrastructure, such as warehouses and distribution centers. It can also bolster network functionality and enable the use of new applications, such as Voice over WLAN (VoWLAN) and location based services. By extending the enterprise infrastructure and improving network operations, user and business productivity is enhanced.

Despite the rapidly growing demand for mobile network services, there is still some reluctance among network administrators to install wireless or remote access to the enterprise network. Though aware of growing user demand and the potential benefits WLANs can provide, many either cannot justify the cost of deploying and managing a mobile network or are concerned about potential security threats. The reluctance to implement wireless access can also be attributed to concerns about supporting applications requiring advanced QoS support and network bandwidth utilization. In effect, next-generation applications require new levels of control and security as well as more sophisticated network allocation capabilities.

When considering the implementation of mobility capabilities, network managers have traditionally been caught between the proverbial "rock and a hard place." They can postpone adding wireless access to their networks and cope reactively with the security and traffic management problems caused by employee-driven mobile access. Or they can proactively implement mobile access and address issues such as security, reliability and technology evolution head-on.

Fortunately, new technologies are available that solve the dilemma of if and when to formally implement mobility, enabling enterprises to deploy WLAN capabilities in a cost-effective manner and ensure the protection of information assets. To that end, network managers must maintain control from the center of their network to the edge, regardless of whether access is wired or wireless.

## The Evolution of Enterprise Networks to Mobility

The evolution of the enterprise network – specifically Ethernet – is moving into new geographic domains such as metropolitan area networks (MANs), mobile wireless connectivity and new classes of converged applications, such as Voice over Internet Protocol (VoIP). This evolution is changing the enterprise network from a file and print sharing tool to a communications platform and, perhaps most important, an anytime, anywhere resource. Each evolution-enabling innovation is typically accompanied by specific technical and operational challenges that must be addressed if the innovation is to become viable.

Today's successful mobility implementations should enable workers to roam from location to location, across subnets with session persistence and without requiring user re-authentication. To do this, the enterprise network infrastructure must incorporate solutions that are reliable, easy to use, affordable, secure and well integrated. The ability to provide and support technology convergence is a necessity, with seamless, standards-based interoperability. Organizations need to work with reliable vendors that understand this new, emerging mobile enterprise network and have the ability to support it.

One telling result of the immense amount of recent and ongoing industry innovation is a network administrator's ability to choose different wireless deployment frameworks for a variety of physical environments. Standalone access points, the most popular framework deployed to

date, are effective and sufficient for smaller, individual cell deployments. The desire to implement mobility capabilities in larger areas with more widespread coverage has recently fueled the inception and evolution of the “coordinated” deployment model: lightweight access points with little capability beyond providing robust radio connectivity, reliant on centralized radio frequency (RF) management capabilities housed upstream in the network. While both of these deployment schemes are valuable for specific physical environments, one big challenge for network administrators is how to effectively manage these different deployment models as they may often need to co-exist in the same business network, as in the case of a campus headquarters with numerous smaller satellite branch offices connected through a wide area network (WAN).

As the range of mobile frameworks and digital appliances continues to diversify and proliferate, the integration, management and security challenges they bring with them are forcing network managers to look for new command and control solutions. Today’s wired and wireless networks are faced with the challenge of integrating new classes of applications requiring QoS, traffic conditioning and rate limiting so that they all coexist on one network.

Maintaining the integrity of the application in a mobile environment is the next logical step as remote access becomes more prevalent and the distinction between wired and wireless networks becomes increasingly blurred. Wireless access points serve as the point of entry for employees, guests and at times unwelcome users. These wireless access points are tasked with simple permission or denial access control and have limited abilities in determining user access rights. They may be aware of four or five active devices, but are not able to manage overall traffic loads or accommodate the needs of other users on the network. This is particularly important when network resources need to be assigned or realigned to meet application or user requirements.

As mobile computing matures, the network is extending its reach to provide mobile connectivity with local wireless technology, public high-bandwidth wireless hotspots and digital cellular. Enterprises need solutions that span these multiple infrastructures to maintain seamless connectivity. Decisions about network access, traffic prioritization, traffic flows and bandwidth optimization can no longer be centralized. As new applications become pervasive, more functionality must move to the edge of the network to effectively support users while making efficient use of the network resources. By understanding how to maintain command from the center with control to the edge, enterprises can enable mobility while maintaining application integrity, bandwidth allocation and network security.

## The ProCurve Adaptive EDGE Architecture

ProCurve is being recognized as a leader and primary challenger in the networking industry due to an unrelenting emphasis on making advanced networking technology affordable and driving innovation in the critical areas of network security, mobility and convergence.

According to Gartner, “Any enterprise replacing a LAN infrastructure that is more than seven years old must have ProCurve Networking from HP on their evaluation list. Also, enterprises looking for an open convergence-ready infrastructure for any site with less than 5,000 nodes should have ProCurve on their shortlist. Highly distributed solutions with a lot of smaller sites are ideally suited to the ProCurve product family.”<sup>3</sup>

The ProCurve Adaptive EDGE Architecture is an innovative approach to designing next generation networks, based on the two key principles of command from the center and control to the edge. It provides intelligence at the edge of the network where users connect and control the behavior of that intelligence by configuring it from a central database. Adaptive EDGE Architecture-enabled solutions can enforce security and bandwidth allocation policies and enable QoS when and where needed, all while maintaining session persistence as mobile users move across subnets.

---

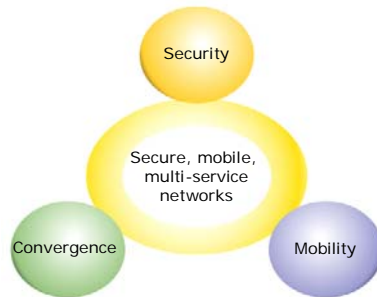
<sup>3</sup> Gartner, “Magic Quadrant for Global Campus LAN, 2006,” October 2006.

---

## A new, unified approach is required

"Built-in" not "bolted on"

*A unified holistic approach*  
to secure, mobile,  
multi-service networks



- Network functionality must migrate to the *edge where users connect*
- Network functionality must be cost effective and manageable
- Network functionality must support all current and future traffic types

Figure 1. ProCurve Adaptive EDGE Architecture.

---

Based on the Adaptive EDGE Architecture, ProCurve mobility devices are designed to enable mobile users to move from one location to another, preserving the connection (potential security and productivity issues) and application (potential QoS issues) as appropriate across wired and wireless zones. ProCurve switches can immediately recognize who the user is and the types of services and access they are authorized to have, thus personalizing the network at the point of entrance. This also means that any unauthorized traffic is stopped at the point where it is trying to connect, not after it has entered the infrastructure, making the network less vulnerable to attack.

The standards-based nature of ProCurve solutions makes it possible for network managers to implement today's mobility solutions while also having the ability to accommodate emerging technologies. It also provides the industry's only holistic architecture for security, convergence and mobility services. This is particularly important as network managers integrate mobility into their networks today with an eye toward the next generation networks of tomorrow. Being able to easily deploy and enable mobility as just another secure, integrated service on an intelligent edge network, rather than as a completely separate overlay is a very powerful capability of the Adaptive EDGE Architecture.

## ProCurve Mobility Infrastructure Solutions

ProCurve Mobility Infrastructure solutions combine ProCurve products, services and support to enable reliable, secure wireless connectivity for a wide range of business environments:

- Hardware, including standalone access points, wireless services modules for intelligent edge switches, coordinated radio ports and standalone secure access appliances
- Software, including integrated device and user-based network management tools
- Wireless services and support, including partner provided site assessment and deployment and a unique lifetime warranty for most ProCurve products

Key solution elements also support third party authentication systems, clients, switches and access points for maximum flexibility and cost savings.



Figure 2. HP ProCurve Mobility Infrastructure solution framework

Based on the ProCurve Adaptive EDGE Architecture, ProCurve Mobility Infrastructure solutions address customer requirements and provide peace of mind by ensuring:

- Choice and flexibility to serve a wide range of physical environments
- Unified access control and management, with consistent application and enforcement of security policies across wired and wireless connections
- Robust encryption for data privacy
- Flexible guest access capabilities
- Seamless roaming
- Network resiliency
- Best-in-class service and support
- Business application enablement

## Choice and Flexibility

One challenge a network architect faces is how to deploy mobility in an optimized yet consistent fashion for different physical environments. Oftentimes, a business may have a campus headquarters site, with many smaller branch or remote sites connected via WAN interface. The ProCurve Adaptive EDGE Architecture addresses this issue by establishing an “intelligent edge” where the network behaves consistently regardless of whether a user connects at the campus site or a remote site. In addition, by consistently managing and applying security policies and access control wherever the intelligent edge resides, ProCurve mobility solutions reduce complexity and increase security.

Maximum choice and flexibility can be provided with specific mobility deployment approaches optimized for different physical environments. For example, at small branch offices where client populations are low, it is most effective to deploy highly intelligent standalone access points, which have the ability to perform key services such as authentication locally should a WAN link fail. Conversely, for campus headquarter sites where more dense coverage and service to more users is required, fast roaming and self-healing are essential. These capabilities are best addressed utilizing centralized RF management and coordinated radio ports (lightweight access points). ProCurve’s approach to this hybrid environment is unique, providing consistent

“command from the center” device and access control management uniformly across both standalone and coordinated mobility deployments, as well as the ProCurve wired environment.

## **Unified Access Control and Management**

Multiple standards-based approaches to network access security can be applied and coexist, including 802.1X, Web-based authentication and state-of-the-art wireless data privacy with virtual private networks (VPNs) or 802.11i implementation. In conjunction, these approaches deliver enhanced wireless functionality while ensuring utmost security and flexibility. They also enable robust network operations, seamless integration and roaming through interoperability and scalability, which can contribute to an organization's productivity.

Further enhancing wireless functionality are the secure network access, access management and roaming capabilities made possible by ProCurve mobility devices. By providing control to the edge with intelligent switches, wireless services modules and coordinated radio ports, as well as highly intelligent standalone access points, and then using command from the center to define who gets access to specific applications, services and information, network behavior can be driven by a variety of factors. These include organizational structure, mission, business needs, job descriptions, customer profiles and more.

ProCurve mobility devices provide centralized security configuration and policy management for all users of the wireless network. Centralized policy management allows quick and efficient updating of user rights, consolidated into one location. ProCurve mobility solutions seamlessly integrate into a network infrastructure, leveraging existing authentication services to authorize user access. These solutions maintain constant communication with the appropriate access control enforcement device (standalone access point, switch port or coordinated access point) to coordinate all user activity. They can also update network access rights based on the user's policy privileges, physical location or time of day. The result is a high degree of control and management of various users and their unique access rights, consistently and uniformly applied. Network access can now be fine-tuned on a per-user basis, not only addressing whom the user is and whether or not they should have access, but what they should have access to, when and where they should be allowed access and how much bandwidth they should be provided.

With the Adaptive EDGE Architecture, network edge devices (standalone access points, edge switch ports, wireless services modules and access control modules) all have the capacity to enforce centrally defined, user-based policies for access control rights, bandwidth and QoS. User-based policies are defined once (centrally) in the network and then applied consistently wherever an intelligent edge device exists. This enables an extremely scalable framework; as new capacity is required for additional users, new intelligent edge devices can be added with the centrally defined policies applied in lock step with the existing devices. This framework inherently reduces operational expense since network administrators are freed from repetitious tasks such as redefining access control policies. Wireless overlay networks and poorly integrated wired/wireless approaches available from other vendors require duplicate (or in some cases triplicate) and fragmented effort, resulting in additional operational expense as well as heightened risk of security flaws, which can be targets for exploit.

## **Robust Data Privacy**

In addition to access control, data privacy is a chief concern for businesses entertaining a WLAN deployment or wrestling with an existing, older generation deployment. Technology and standards related to WLAN data privacy have evolved rapidly over the past several years, resulting in robust, standards-based encryption schemes such as WiFi Protected Access version 2.0 (WPA2.0) and utilizing 802.1X as an authentication fabric. ProCurve Mobility Infrastructure solutions support the latest in standards-based security protocols, allowing administrators to architect very robust WLAN solutions for greenfield deployments.

Despite the advancement of data privacy standards, many corporate networks still render it too easy for unwanted users to get onto the WLAN. Although recent security protocols and technologies are available, deploying them across all aspects of a network (client, infrastructure, etc.) takes time and resources. As a result, many businesses today are still reliant on Wired Equivalent Privacy (WEP) encryption, which has known data privacy issues. In addition to utilizing the latest in standards-based data privacy encryption and authentication protocols, ProCurve also offers solutions providing VPN termination capability for legacy environments.

## Guest Access

Enabling appropriate guest access is a powerful capability for a wide range of businesses. ProCurve offers a host of guest access services depending on customer needs. ProCurve products provide “Virtual Lobby” capabilities, enabling organizations to host guest users on the secure enterprise LAN and give them access to only the resources and services they need, such as the Internet, printing and email. Network zones are created on the enterprise network – using Virtual LAN (VLAN) technology – that are essentially open to a corporation’s public users but not to the general public. The “Virtual Lobby” can be extended across the entire enterprise to provide guest users with services where, when and how an enterprise wants to provide them. This can include meeting rooms for customers, conference and seminar facilities for partners and human resource information for job applicants and contractors across the enterprise campus – all of which can be customized to provide a variety of rich user services and the appropriate view of the enterprise for different types of guests.

ProCurve’s approach to enabling guest access is unique, since guests can be treated simply as another user profile. As such, appropriate access is defined and enforced for that profile across all edges of the corporate network, consistent with how access and user policies are defined and enforced for all other users of the network. Regardless, guest access can either be provided as an integrated capability, with switches and wireless services modules, or as an added, specialized solution to meet demanding client environments, where client configuration is not an option. ProCurve also provides guest access administration capabilities, to allow the network administrator to delegate guest access administration to a help desk or building lobby attendant, to more easily and efficiently enable secure guest access for businesses.

## Roaming

Different environments and deployment needs demand different roaming capabilities. ProCurve provides a host of roaming capabilities to effectively enable a wide variety of business applications.

For mainstream environments such as floors of an office building, ProCurve provides seamless fast roaming with pre-cached authentication credentials for wireless users. This is accomplished by utilizing centralized RF management that is integrated into intelligent edge switches via a wireless services module as well as coordinated access points. The approach provides a streamlined, easily scalable solution by leveraging the switching infrastructure and consistently defined and enforced user policies.

For very large demanding environments requiring seamless roaming across multiple subnets, ProCurve wireless services modules track and forward the active session from module to module as a user moves between locations, keeping the session live and uninterrupted. As the session is forwarded among host modules, each module checks with the module that initially authenticated the user and ensures the authentication information is passed to the current module allowing the session to continue anywhere in the network, across multiple subnets. Multiple subnet roaming is also available as a capability on the ProCurve secure access series solution, specifically designed for the ProCurve Switch 5300xl series. All of these options add up to providing additional flexibility for securing and controlling mobile access to network resources.

Figure 3 represents a typical business environment with campus and remote sites, illustrating how ProCurve Mobility Infrastructure solutions can be utilized to address key concerns facing network administrators. Guests and employees are granted secure, appropriate network access, while unwanted users are prevented from accessing the WLAN.

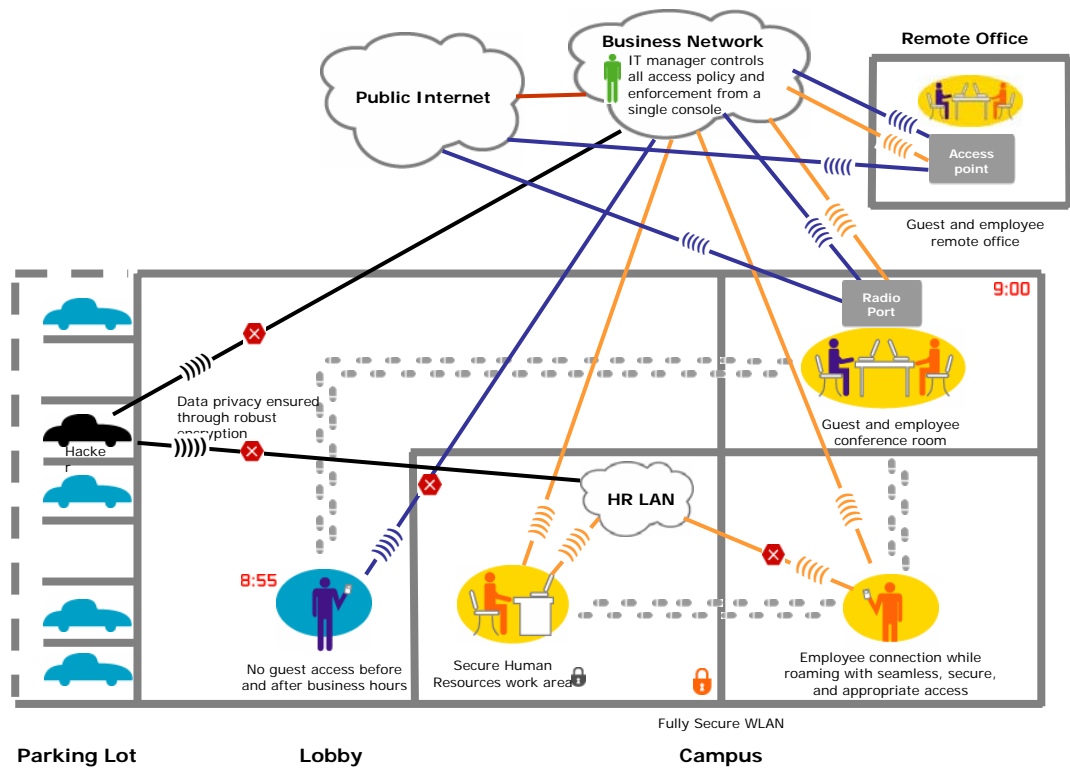


Figure 3. Wireless deployment utilizing ProCurve Mobility Infrastructure solutions

ProCurve Mobility Infrastructure solutions are available as end-to-end ProCurve deployments and as overlays to existing 3<sup>rd</sup> party WLANs. For a legacy WLAN environment which does not support the latest robust encryption standards, advanced data privacy capabilities ensure unwanted users cannot “sniff” or capture any company data in the RF spectrum. The ability to schedule access (i.e. before 9 a.m., no WLAN access is permitted in the lobby area) via centralized control eliminates the possibility of a hacker attempting to gain access outside normal business hours. In this scenario, when a guest arrives in the lobby before 9 a.m., no access is possible. However, when the guest is called into the conference room at 9 a.m., scheduled guest access is enabled, increasing meeting productivity and collaboration.

In addition, WLAN connectivity can now be completely secured in particular locations, such as the Human Resources (HR) work area. Policy attributes to employee classifications can be assigned centrally and enforced at every connection point, thus granting HR LAN access to HR employees only. Policy control extends beyond the “who” to facilitate access based on “what,” “where” and “when.” Access to the HR LAN is not only limited to HR employees, but also the physical confines of the restricted HR work area and the time of day the LAN is accessible.

Several flavors of ProCurve Mobility Infrastructure solutions can also be implemented to provide session persistence across subnets. As approved employees roam to various buildings or conference rooms, their connection is maintained and productivity enhanced. No time or effort is spent re-authenticating, reconnecting or reloading applications. Using the above scenario, HR employees would not have access to the sensitive HR LAN while in the conference room, per the centrally dictated policy. By providing unified access control and policy enforcement at every edge of the network, guest and employee network services are delivered identically at a remote branch office site and at the headquarter campus. This assures that users have a consistent experience and security policies are uniformly enforced and maintained.

## Resiliency

Select ProCurve switches and access control devices offer unique bandwidth management capabilities, helping contain and mitigate viruses, worms and other malicious agents that threaten enterprise networks.

The most common method of protecting wired and wireless networks is to implement anti-virus software on each individual client. These solutions utilize signature recognition to identify the physical characteristics of a documented virus and, once recognized, prevent it from entering the network. Unfortunately, these tools are fundamentally reactive and only effective when dealing with known viruses. They are not able to recognize or stop the new threats that sprout daily.

Connection-rate filtering based on virus-throttling technology is an effective and unique ProCurve-developed solution that addresses these concerns. Virus-throttling is unique in that it identifies the behavioral characteristics of a network under attack (i.e. the number of connections a computer is attempting to make per second) instead of the physical characteristics of a known virus (i.e. program code). In doing so, it is able to automatically discover attacks by previously unknown threats and hamper them by immediately restricting bandwidth, giving network managers the time necessary to implement a response.

By utilizing the switching infrastructure as much as possible for deployment of mobility services rather than a separate dedicated overlay, a greater degree of resiliency is achieved. The ProCurve switches that host the various mobility services modules have been designed with high availability in mind and feature fully redundant, hot swappable power supplies, resulting in higher service uptime. Redundant modules are also available to provide immediate failover capability should a primary module fail.

While ProCurve has mobility solutions which can be deployed in consistent fashion from core to edge - based on customer preference, ProCurve recommends deploying RF management intelligence (including self-healing) for coordinated deployments at the edge of the network that inherently boosts resiliency. If a services module fails at the edge, the potential effects are limited to the number of clients associated through that particular module, minimizing business impact. Other approaches available in the market deploy RF management intelligence at the core of the network, with all wireless clients for an entire site funneled back to a single point. If this service fails at the core, an exponentially larger number of client associations may be affected, resulting in a substantially more severe impact to the business. Furthermore, building in redundancy at the core of the network is traditionally a much more expensive undertaking than building in redundancy at the edge.

## **Solution Services**

ProCurve understands it is imperative to have a WLAN implemented quickly and effectively, and recommends organizations utilize a ProCurve Elite Partner to assess, deploy and maintain a ProCurve Mobility Infrastructure solution that best fits their unique needs. ProCurve Elite Partners are trained in ProCurve Mobility Infrastructure solutions and offer services designed to integrate a new WLAN solution into an existing network.

ProCurve Elite Partners have a comprehensive understanding of networking and offer a broad suite of product and application services, including systems integration and network design, installation, configuration and optimization and network lifecycle support. ProCurve Elite Partners are required to have achieved the highest level of certification in network solutions planning and design as recognized by ProCurve. Committed to excellence, quality and integrity, ProCurve Elite Partners are the deployment vendors of choice for ProCurve's most demanding customers.

With a ProCurve Elite Partner, organizations are assured of having a dependable partner and advisor to deliver best-in-class solutions that will effectively address IT requirements and business needs.

## **Enabling Business Applications**

Many businesses are looking beyond wireless email and mobile access to the corporate intranet when considering how to glean business benefit from a WLAN deployment. A host of business applications are emerging, including Voice over WLAN (VoWLAN) and location services, which hold the promise of raising the return on WLAN investment substantially higher than current expectations, especially for specific vertical segments. ProCurve Mobility Infrastructure solutions host built-in capabilities and technologies to help foster business application enablement, without requiring significant network upgrades when an organization decides to deploy the application.

## Summary

ProCurve Mobility Infrastructure solutions enable businesses to deploy wireless networks with protection and management at the forefront, whether they are for small and focused sites like classrooms or throughout an entire global organization. The architecture is designed to give network managers control at the edge of the network down to the level of who gets in, what network resources they are able to access, what they are allowed to do as well as when, where and for how long they are allowed to do it. Only control to the edge provides the robust functionality needed to support secure mobility for current and future applications and traffic types.

Whether the connection is remote or local, wired or wireless, ProCurve Mobility Infrastructure solutions emphasize a unified security scheme for network access, management and roaming. With consistent network performance and management as well as choice and flexibility to optimize wireless capabilities for a variety of environments, the overall cost of mobility is reduced.

Between the client and the network edge – before access is granted – through use of industry standards and key protocol capabilities, the Adaptive EDGE Architecture permits secure, fast and appropriate access. In addition, new offerings enable organizations to integrate advanced mobility capabilities such as fast roaming, session persistence across subnets, self healing and flexible authentication methods as they deploy mobile networks as an extension to an existing wired networking infrastructure.

By extending the wired network to mobile users with secure, reliable and appropriate access, ProCurve enables users to effectively communicate anytime, anywhere.

## For more information

To learn more about ProCurve Networking solutions, contact your local ProCurve sales representative or visit the company's Web site at [www.procurve.com](http://www.procurve.com).

For a list of ProCurve Elite Partners that can provide ProCurve mobility solutions, go to [www.procurve.com](http://www.procurve.com).

To find out more about  
ProCurve Networking  
products and solutions,  
visit our web site at

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



© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-0542ENW, 4/2007