

HP ProCurve Networking Access Control Security Solution

Technical Brief



Introduction.....	2
Business and IT Needs/Benefits.....	3
Figure 1: Comparison of Access Control Paradigms	4
Figure 2: HP ProCurve Access Control Security solution architecture	5
Figure 3: HP ProCurve Networking Access deployment examples	6
Access Control Best Practices	6
Solution Value	7
Figure 4: The HP ProCurve Security solution framework.....	7
Detailed Configuration	8
Network Management Software	8
HP ProCurve Manager	8
HP ProCurve Manager Plus.....	8
HP ProCurve Access Control Client Software	8
Wired Infrastructure Products.....	8
HP ProCurve Switch 2500 Series	8
HP ProCurve Switch 2800 Series	9
HP ProCurve Switch 4100gl Series.....	9
HP ProCurve Switch 2600 Series	9
HP ProCurve Switch 5300xl Series	9
Wireless Infrastructure Products.....	10
HP ProCurve Wireless Access Point 420	10
HP ProCurve Wireless Access Point 520wl	10
HP ProCurve Secure Access 700wl Series	10
HP ProCurve Access Control Security Solution Services.....	10
Summary	11
For more information.....	12

Introduction

Network administrators know how hard it is to construct an effective access control system. In fact, many of them see a huge gap between where their organizations are currently and where they need to be to effectively manage the security risks that arise from unauthorized or malicious access to corporate Local Area Networks (LANs).

A corporation would not allow intruders to come through its front door and roam freely throughout its office space. Yet that is exactly what many corporations do when it comes to controlling access to their internal LANs. The results aren't surprising. The 2003 Search Survey indicated that one-third of network violations were internal breaches.

Insider abuse

Insider abuse was the second-highest form of network abuse cited in the 2003 FBI/Computer Science Institute Computer Crime and Security Survey. Eighty percent of corporations reported internal incidents.

A comprehensive approach to access control isn't a particularly new or revolutionary concept, but it's critical because in today's corporation authorized users are not only employees but also customers, partners and vendors. To protect its LANs, corporations must build electronic "doors" that lead authorized users into appropriate "zones" of information and services – and nowhere else. Those doors and zones should have levels of user access that can be changed at any time.

So how do you get there from here?

Built on the HP ProCurve Networking Adaptive EDGE Architecture™, the HP ProCurve Access Control Security solution helps provide the most secure LAN environments available today. The HP ProCurve approach is based on two principles:

1. Access is controlled at the LAN edge – intelligent switches deal with user authentication individually and rely on commands from a central server to set authorization levels before a user is granted access.
2. The network is commanded from the center – access control policies are stored at a central server, from where they can configure the various switches at the network's edge.

While it's not new, a comprehensive approach structured this way represents a fundamental change to the way most networks are designed. This paper will outline how the HP ProCurve Access Control Security solution based on the Adaptive EDGE Architecture solves the real customer problem of protecting corporate LANs from unauthorized use while leveraging an organization's current infrastructure and providing a clear migration path to the 802.1X standard.

The HP ProCurve approach addresses the authentication of end users through the use of 802.1X and remote authentication dial-in user service (RADIUS) technologies implemented on edge switches. This approach is the first step toward creating a truly intelligent network and for administrators looking for the best possible access control architecture; it's how they get there from here.

Business and IT Needs/Benefits

“The new model for controlling access to a network calls for protecting data wherever it is and trusting no one completely wherever they are.”¹

Typically, corporations are at one of four levels when it comes to controlling access to their corporate LANs:

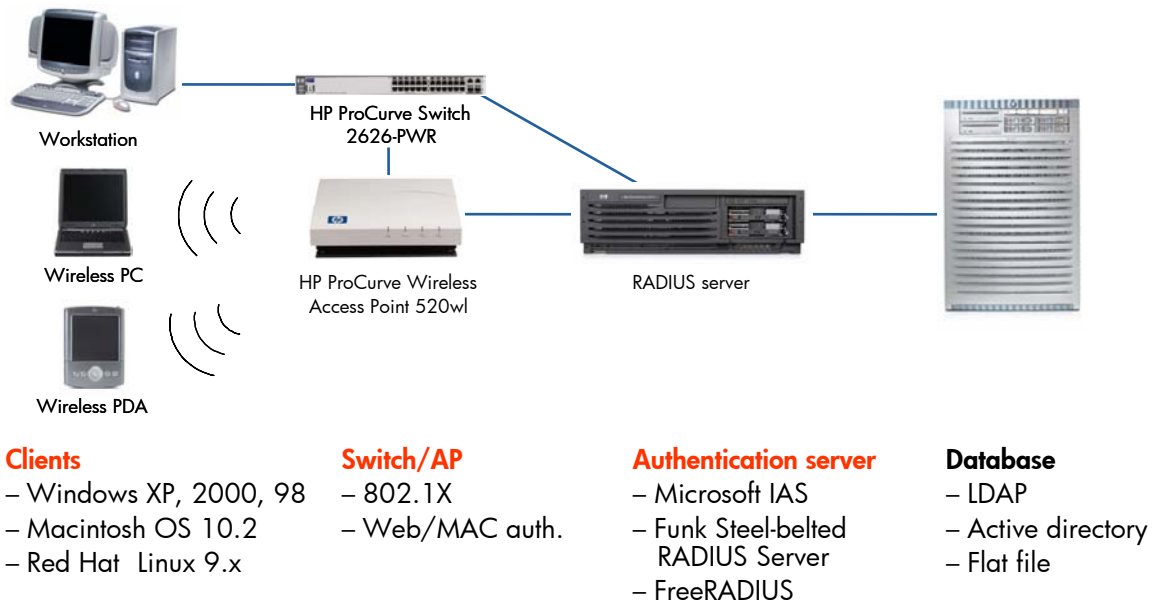
1. **No controls** – the corporation has no measures or monitoring systems in place. The 2003 FBI/CSI survey found that 15 percent of companies simply “don’t know whether there was any unauthorized use of their computer systems last year.”
2. **Device-specific controls** - the corporation has Layer 2 MAC-address based access controls, tying specific machines to the network. Tying devices to the network prevents unauthorized devices from accessing the network but can be difficult to set up and maintain. In addition, it’s not possible to automate wireless encryption key assignments.
3. **Web-based controls** – the corporation has a web-based access control system. This means Web-based authentication dynamically ties the user and the individual MAC address to the network. Tying users and computers together to the network helps deter attacks but problems remain in the inability to automate wireless encryption.
4. **Holistic 802.1X controls** – the current gold standard of access control, 802.1X provides the corporation with the ability to manage access control on multiple levels, wired or wireless, with full support for automating wireless encryption and an audit trail for authenticated users.

¹ Suzanne Gaspar, “The New Security Battle Plan” Network World, Sept. 30, 2002

Figure 1: Comparison of Access Control Paradigms

Paradigm	None	MAC-based	Web-based	802.1X
Security	None	Low	Medium	High
Advantages	No deployment cost	<ul style="list-style-type: none"> • Transparent to end-user • No need for client software 	<ul style="list-style-type: none"> • True user authentication • Capitalizes existing user security information • Leverages web browser ubiquity 	<ul style="list-style-type: none"> • True user authentication • Capitalizes existing user security information • Integrated into traditional log-on process • Automated encryption key assignment (wireless)
Disadvantages	Completely insecure	<ul style="list-style-type: none"> • Overhead of MAC address management • Device specific, not user • Spoofing opportunities • No automatic key encryption rotation (wireless) 	<ul style="list-style-type: none"> • End-user behavior modification • No automatic encryption key rotation (wireless) 	<ul style="list-style-type: none"> • Requires client supplicant technology (possible deployment /support issues)
Client Products	n/a	n/a	n/a	<ul style="list-style-type: none"> • HP ProCurve Access Control Client Software
Wired Products	n/a	<ul style="list-style-type: none"> • Switch 5300xl series • Switch 2600* series 	<ul style="list-style-type: none"> • Switch 5300xl series 	<ul style="list-style-type: none"> • Switch 2500 series • Switch 2600 series • Switch 2800 series • Switch 4100gl series • Switch 5300xl series • Switch 6108 • Routing Switch 9300m series
Wireless Products	n/a	<ul style="list-style-type: none"> • Access Point 420 • Access Point 520wl • Secure Access 700wl series 	<ul style="list-style-type: none"> • Secure Access 700wl series 	<ul style="list-style-type: none"> • Access Point 420 • Access Point 520wl • Secure Access 700wl series

Figure 2: HP ProCurve Access Control Security solution architecture

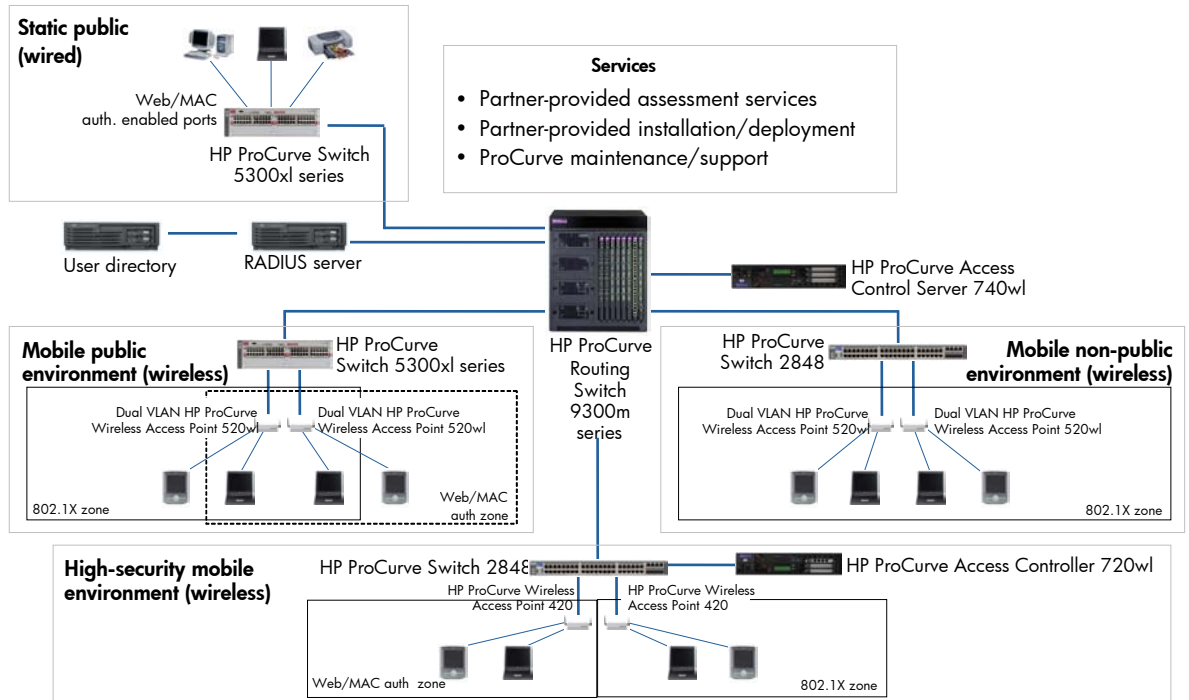


Any access control architecture is made up of several steps (Figure 2), which typically happen in the same order. When an end user connects to an HP ProCurve switch or access point, it will recognize a connection state change. The system will update its internal structure that represents the physical connection state and will check if the physical interface is configured as an 802.1X authenticator or supplicant. For non-802.1X interfaces, the initialization process continues as usual by bringing up the logical interface.

If the port is configured to run an 802.1X authenticator, the system will require a supplicant to authenticate before logically bringing up the interface. Before this time, the port will be logically down and will not learn the MAC address of the attached supplicant nor forward packets to or from the port. This means at a base level that all ports are shut, which is inherently a higher level of security.

The port will direct certain packets (STP, FEC, GARP, 802.1X or LDBAL) with several specifically programmed MAC addresses to the switch CPU. A packet containing the 802.1X-assigned MAC address (one of the special 16 bridge protocol data unit (BPDU,) addresses set aside by the 802.1X standard) will be one of those packets. Any packet received on the port that is not one of the above special packets is discarded.

Figure 3: HP ProCurve Networking Access Control solution deployment examples



HP ProCurve solutions and the access control architecture (Figure 3) provide a multi-vendor standardized framework using industry standard RADIUS authentication servers, something many corporations already have as part of a remote access solution. HP ProCurve solutions also support multiple methods of end user authentication, including passwords, digital certificates and smart cards. Finally, in wireless networks the 802.1X standard allows encryption keys (WEP and WPA) to be automated on a per-user, per-session basis.

Access Control Best Practices

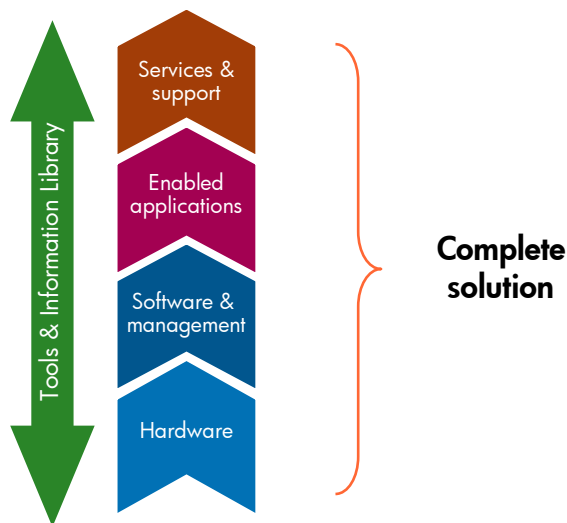
- **Think Big** – a comprehensive approach to access control is essential because there are multiple elements that need to integrate correctly to effectively secure a network. Technology enables such an approach but corporate practices, procedures and plans all play key roles in building a truly intelligent network. Successful access control begins in the executive suite.
- **Push Control to the LAN Edge** – intelligent networks stop unauthorized traffic and users right at the network edge, keeping undesirables out and monitoring authorized users. The overall level of security is markedly increased when unauthorized traffic is segregated immediately. This is a basic premise of network access control but one that currently isn't incorporated into a lot of corporate LANs.
- **Have a Roadmap** – it's important to have a clear migration strategy from a corporation's current infrastructure to the current gold standard of access control, which is based on the 802.1X standard. Implementing a state-of-the-art access control solution requires that solution to co-exist with and build on existing technology in an evolutionary approach. For example, passwords should be used initially but can be augmented in subsequent stages by additional security, including smart cards, digital certificates, public key encryption and even biometrics.

- **Control the Ports** – every network port must either allow or disallow access. Open ports are a haven for hackers and can allow even authorized users free reign over a network. An 802.1X access control solution can control ports and restrict access so even an authorized user can't log on using a different network port unless permission to do so is written into the user's profile.
- **Establish Explicit Usage Policies** – corporations must have clear policies that define network access and segregate users based on various pre-defined factors. These parameters form the "central command" of policies. Other policies should include a clear reporting mechanism and infrastructure to respond rapidly to end user issues.
- **Deliver Quantifiable Technical ROI** – investing in access control will contribute to the technical efficiency of networks, mitigate clear risks to corporations and save a lot of money. Documenting those savings back to the executive suite is essential.
- **Embrace Industry Standards** – insisting that vendors deliver flexible solutions that can work with equipment and software from other vendors is an important part of a long-term access control strategy.
- **Equipment Lockdown** – ad hoc implementations, rogue downloads, PDAs and Wi-Fi networks can impact the overall security of networks. Every piece of equipment added to a network must be channeled through IT and the process must be streamlined so end users participate.

Solution Value

Corporations need the right combination of hardware, software, services and support to deliver a strategic access control solution – and that's what HP provides (Figure 4).

Figure 4: The HP ProCurve Security solution framework



The HP ProCurve Access Control Security solution offers a complete solution by combining HP ProCurve products with services, support and tested third party products to ensure a secure, scalable, standards-based access control architecture.

The HP ProCurve family of products includes layer 2 through layer 4 switches, robust, enterprise-class wired and wireless mobility and secure access products, plus industry leading service and support. The entire product family is designed to provide high-performance, no-compromise functionality at affordable prices. The HP ProCurve family also features several products that come with lifetime warranties.

The key components include HP ProCurve wired and wireless infrastructure devices, HP ProCurve Manager, and the HP ProCurve Access Control Client Software for Windows, Linux, and Macintosh platforms. The third party component that completes the solution is an interoperable RADIUS server that can either be a Microsoft IAS, Funk Steel-Belted, or Linux FreeRADIUS server.

Detailed Configuration

Elements required to configure a secure 802.1X access control architecture include:

Network Management Software

HP ProCurve Manager

HP ProCurve Manager is a Windows-based network management solution that is included in-box with all controllable HP ProCurve devices, wired and wireless, providing a unified management platform. It provides mapping and polling capabilities, device auto-discovery and topology mapping, device configuration and management, and troubleshooting data and alerts for an HP ProCurve network.

HP ProCurve Manager Plus

HP ProCurve Manager Plus is a complete, Windows-based network management solution that provides both basic and advanced management features for HP ProCurve LAN devices. It allows users to discover, configure, monitor and troubleshoot HP ProCurve devices. HP ProCurve Manager Plus includes features such as configuration management, VLAN management, in-depth traffic monitoring, group and policy management and automated software updates.

HP ProCurve Access Control Client Software

HP ProCurve Access Control Client Software provides a single source for all elements of an access control solution. It is a multi-platform 802.1X supplicant – including Microsoft Windows 98, 2000, XP, Red Hat Linux and Apple Mac OS – and includes an enterprise deployment tool for Windows 2000/XP environments. The client software has been fully qualified with HP ProCurve infrastructure products that support 802.1X and Microsoft IAS, Funk Steel-Belted, and Linux FreeRADIUS authentication servers.

Wired Infrastructure Products

All HP ProCurve wired products below include 802.1X authenticator functionality with support for EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP authentication methods. Additionally, all switches support 802.1X and the 5300 series supports web and MAC authentication.

HP ProCurve Switch 2500 Series

The HP ProCurve Switch 2500 Series are low cost, stackable, managed 24- and 12-port switches with 10/100 auto-sensing per port and 2 open transceiver slots for Gigabit or 100Base-FX. The HP ProCurve Switches 2524 and 2512 offer HP Auto-MDIX on all 10/100 and 100/1000 ports and high-availability features. These switches are ideal for low-cost migration to 10/100 managed switching with uplinks. Pertinent access control features include 802.1X authenticator and supplicant capability. The 802.1X authenticator can be coupled with dynamic VLAN (up to 30) assignment via RADIUS.

HP ProCurve Switch 2800 Series

The HP ProCurve Switch 2800 series consists of two switches: the 24-port HP ProCurve Switch 2824 with 20 10/100/1000 ports, and the 48-port HP ProCurve Switch 2848 with 44 10/100/1000 ports. In addition, each switch has 4 dual-personality ports for 10/100/1000 or mini-GBIC connectivity. Ideal for medium to large networks, the Switch 2824 and Switch 2848 cost-effectively offer the maximum in bandwidth performance with 10 times the speed of 100 Mbit switches. Migrating to Gigabit switches allows corporations to take full advantage of their existing high-performance, Gigabit-enabled PCs, laptops, and servers—and see noticeably improved application response and file transfer times. The HP ProCurve Switch 2800 includes 802.1X authenticator and supplicant capability. The 802.1X authenticator supports dynamic VLAN (up to 60) assignment via RADIUS.

HP ProCurve Switch 4100gl Series

The HP ProCurve Switch 4100gl series is convergence-ready and easy to use in compact 8-slot and 4-slot modular form factors. Based on HP Fast Path Technology, these switches provide reliable, high-performance, high-density 10 Mbit, 100 Mbit, or Gigabit connectivity for a growing network. The Switch 4100gl series is the low-cost, modular alternative to stackable switches and includes a lifetime warranty. Pertinent access control features include 802.1X authenticator and supplicant capability. The 802.1X authenticator supports dynamic VLAN (up to 30) assignment via RADIUS.

HP ProCurve Switch 2600 Series

The HP ProCurve Switch 2600 Series is a collection of low-cost, stackable, multi-layer, managed 50- or 26-port switches with 48 or 24 auto-sensing 10/100 ports and 2 dual-personality ports for 10/100/1000 or mini-GBIC connectivity. The HP Switch 2650-PWR and 2626-PWR are IEEE 802.3af compliant for Power over Ethernet (PoE) and provide up to 15.4W per port. A redundant and external power supply is also available as an accessory. The HP ProCurve Switch 2600 includes 802.1X authenticator and MAC-address² based authentication with support for dynamic VLAN (up to 30) assignment via RADIUS. An onboard 802.1X supplicant can be used to authenticate switch-to-switch links to create a fully secure network fabric.

HP ProCurve Switch 5300xl Series

Designed to accommodate the most demanding network needs, the HP ProCurve Switch 5300xl series offers scalable layer 2, 3, and 4 switching in compact 4- or 8-slot modular form factors. These convergence-ready switches provide flexibility, high port density, free software updates, and a lifetime warranty. The easy-to-use Switch 5300xl series provides the latest in technology with unparalleled investment protection and superior return on IT. The HP ProCurve Switch 5300xl series includes 802.1X authenticator, MAC address, and web-based authentication with support for dynamic VLAN (up to 256) assignment via RADIUS. An onboard 802.1X supplicant can be used to authenticate switch-to-switch links to create a fully secure network fabric. Furthermore, ACL capabilities provide layer 3 (IP) and layer 4 (TCP) access control filtering.

HP ProCurve Routing Switch 9300 Series

The HP ProCurve Routing Switch 9300m series delivers a new level of high-performance capabilities and investment protection for medium and large enterprise networks. By providing high-performance throughput from the wiring closet into the data center and out to the edge of the WAN, the Routing Switch 9300m series' non-blocking architecture enables network managers to build scalable and highly available network designs. Pertinent access control features include 802.1X authenticator with dynamic VLAN assignment via RADIUS. Also, ACL capabilities provide layer 3 (IP) and layer 4 (TCP) access control filtering.

² MAC-address based authentication support slated for Summer 2004 timeframe; Check www.hp.com/go/hpprocurve for software updates

Wireless Infrastructure Products

HP ProCurve Wireless Access Points and Secure Access products provide all of the components necessary to deploy a wireless network with secure, scalable, and standards-based network access controls.

All HP ProCurve wireless access points include 802.1X authenticator functionality with support for EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP authentication methods. The secure access 700wl series supports EAP-MD5 and EAP-TLS in 802.1X monitored login mode.

HP ProCurve Wireless Access Point 420

The HP ProCurve Wireless Access Point 420 is a full-featured IEEE 802.11g, single-radio access point ideally suited to support the MAC-based authentication or 802.1X-based network access control paradigms.

HP ProCurve Wireless Access Point 520wl

The HP ProCurve Wireless Access Point 520wl is a full-featured dual-radio capable access point. It is also suited to support the MAC-based authentication or 802.1X-based network access control paradigms. The 520wl's security features include MAC-based access control and support for the 802.1X authentication method capability.

HP ProCurve Secure Access 700wl Series

The HP ProCurve Secure Access 700wl series products offer an extremely powerful and flexible extension to base access control technology present in HP ProCurve access points. The 700wl series of products supports all three access-control paradigms and has ability to enforce access policies based on location, network access, and time of day. Furthermore, users can roam across wireless subnets without disruption.

The 740wl and 720wl work together to provide a highly scaleable system for controlling the network edge for wireless users. The 740wls provide centralized policy management while the 720wls enforce those authentication, access control, roaming, and bandwidth control policies at the network edge. The 760wl combines the functions of the 740wl and 720wl into a single unit for smaller deployments.

HP ProCurve Access Control Security Solution Services

Because robust network security is such a high priority to you, HP recommends that you have an HP ProCurve Elite Partner assess, deploy, and maintain the HP ProCurve Access Control Security solution to fit your needs. HP ProCurve Elite Partners, trained in HP ProCurve Access Control Security solutions, offer services designed to integrate your new Access Control Security solution into your existing network.

HP 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, optimization as well as network lifecycle support. HP ProCurve Elite Partners are required to have achieved the highest level of certification in network solutions planning and design as recognized by Hewlett-Packard. HP ProCurve Elite partners are the partners of choice for our most demanding customers.

With an HP ProCurve Elite Partner, you are assured of having a partner and advisor that you can depend on and trust to deliver a best in class solutions that will effectively address your IT requirements and ultimately, your business needs. HP ProCurve Elite Partners are committed to excellence, quality and integrity.

For a list of HP ProCurve Elite Resellers that can provide HP ProCurve Access Control Security solutions near you, go to www.hp.com/go/hpprocurve.

Summary

The need for comprehensive access control solutions has never been more urgent. Comprehensive access control isn't about having a faster switch or a bigger router. It's about taking technology that largely already exists and carefully constructing an intelligent network.

That network will protect corporate data wherever it resides and will trust no end user completely, wherever they are. Segregating users and data this way makes a corporate network more secure and more efficient than the vast majority of LANs are today. In the future, well constructed, intelligent networks will have access control systems that prevent 95 percent of attacks and drastically cut the risk from external or internal sources by providing a clear authorization process and audit trail that's commanded from a central server, yet controlled by switches at the edge for rapid authentication and authorization.

Migrating your current network infrastructure to a solution based on these principles may take time, and that's why an evolutionary approach is necessary, one that will be prepared to accommodate an array of future access control technologies as they become ubiquitous – passwords, encryption, smart cards, even biometrics.

So how do you get there from here?

The HP ProCurve Access Control Security solution is the first comprehensive offering from HP ProCurve that addresses the authentication of end users to a LAN using 802.1X standard and RADIUS technology implemented on edge switches. This solution, part of the Adaptive EDGE Architecture, is the first step toward "getting there from here" and creating a truly secure, intelligent network.

HP ProCurve was instrumental in establishing and ratifying the 802.1X standard in June 2001. With more than 25 years experience in network infrastructure, HP understands what corporations need to develop intelligent networks that can help manage the risks associated with access control. Controlling access to networks is a huge, complicated task. The HP ProCurve Access Control Security solution is part of the Adaptive EDGE Architectural approach that provides price/performance leadership, outstanding QoS, a lifetime warranty and, ultimately, a partner companies can trust.

For more information

To learn more about HP ProCurve Networking solutions, contact your local HP sales representative or visit our website at: www.hp.com/go/hpprocurve.

For a list of HP ProCurve Elite Resellers that can provide solutions based on the HP ProCurve Access Control Security solution, go to www.hp.com/go/hpprocurve.

© 2004 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.

5/2004

