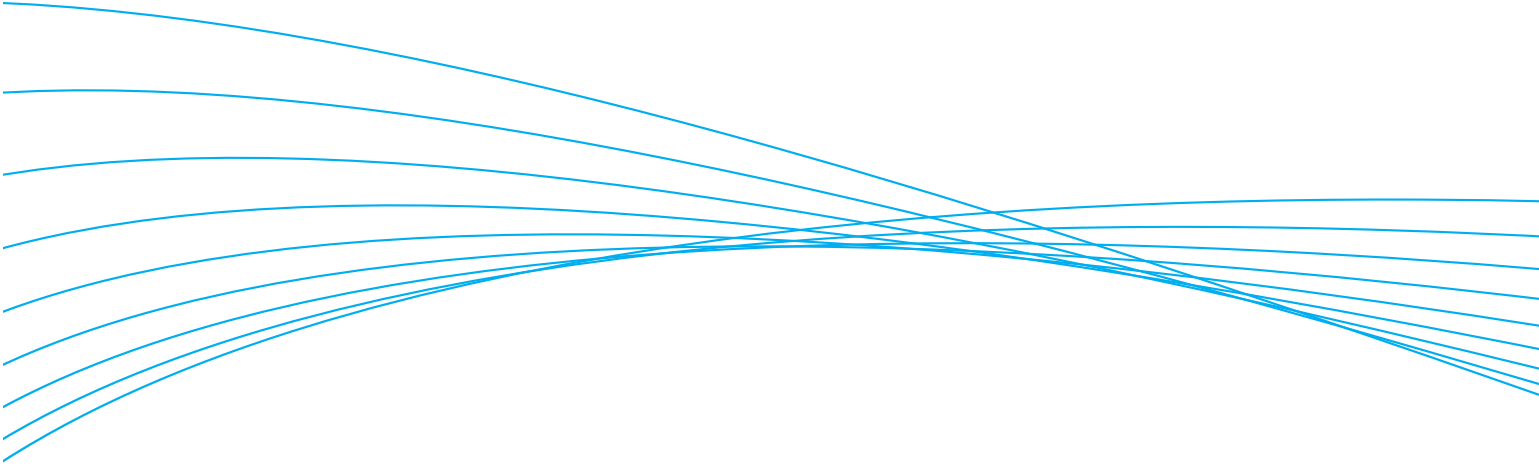


HP ProCurve Networking

Network Access Control—ProCurve and Microsoft[®] NAP Integration



Abstract	2
Foundation	3
Network Access Control basics	4
ProCurve Identity Driven Manager overview	5
Microsoft Network Access Protection overview	7
ProCurve IDM and Microsoft NAP integrated	9
Conclusion	11

Abstract

Keeping important services and data available can be critical for the success of a company. One of these measures helps with reducing the risk from internal threats: Network Access Control. By using Microsoft's expertise in clients and servers, along with ProCurve's expertise in networking, it is possible to create an integrated solution for Network Access Control that provides personalized, appropriate network access to users and clients, without hindering their productivity.

Microsoft Network Access Protection (NAP) provides a mechanism to test a client for company policy compliance, such as requiring that up-to-date antivirus software or firewall software is running. NAP also includes capabilities to automatically bring a client back into compliance.

HP ProCurve Identity Driven Manager (IDM) provides a mechanism to set user-based performance and security settings on switches and access points, based on the user identity, the user's location, connection time, and device ID.

This document describes ProCurve IDM and Microsoft NAP, and how the two products integrate to provide a complete Network Access Control solution.

Foundation

Before deploying any security solution, it is important to help ensure that the infrastructure itself is secure. The security of an environment is as strong as its weakest link. Choosing the right components for the right task will help produce a secure foundation.

Microsoft Windows® Server 2008 and Microsoft Windows Vista® both include security features to reduce the risk that servers or clients will become compromised. Some of the new technologies and features available include:

- **Address Space Layout Randomization (ASLR)**, which loads system files at random addresses in memory. This helps prevent most remote execution attacks by preventing “Return-to-libc” buffer overflow attacks.
- **Data Execution Prevention (DEP)**, which can flag certain parts of memory as containing data instead of executable code. This prevents overflow errors from resulting in arbitrary code execution.
- **Windows Service Hardening**, which prevents Windows Services from performing file system, registry, or network operations they are not supposed to do.
- **Improved integrated firewall**, which helps to keep out attackers at the client level.
- **Network Access Protection (NAP)**, which will be discussed in more detail in this document. NAP tests clients to determine if they comply with the corporate policy.

These and other security features can be configured centrally by using Active Directory with Group Policies, simplifying management.

ProCurve LAN and wireless LAN (WLAN) products, such as the ProCurve Switch 5400zl Series and the Wireless Edge Services zl Module, include features to strengthen the security of the network and reduce the risk that the network devices will become compromised, as well as to protect clients and servers on the network. Some of the built-in technologies and features available include:*

- **Virus throttling**, which detects traffic patterns typical of worm viruses and can be configured to take action such as throttling or blocking the interface.
- **Secure management access**, which secures all access methods by encrypting through Secure Shell Version 2 (SSHv2), Secure Sockets Layer (SSL), and/or Simple Network Management Protocol Version 3 (SNMPv3).
- **Multiple user authentication methods**, such as IEEE 802.1X (discussed in more detail in this document), Web-based authentication, and MAC-based authentication, provide security and flexibility for guest users and non-IEEE 802.1X capable clients.
- **Rogue access point detection**, which alerts the IT administrator when there are non-authorized access points on the network.
- **User-based security settings**, which will be discussed more in detail in this document, allow the network to configure itself to provide personalized, appropriate network access for each user.

By using HP ProCurve Manager Plus and its plug-ins, security features can be managed network wide from one interface, simplifying management.

Correctly implementing and configuring the security features available in Microsoft Windows Server 2008, Microsoft Windows Vista, and ProCurve network equipment can dramatically reduce the attack surface, giving hackers less of an opportunity to break security. Both ProCurve and Microsoft have security-specific products to further enhance overall network security.

* Not all features and technologies are available on all ProCurve devices.

Network Access Control basics

IT infrastructure is becoming more and more important for most companies. Even to the extent that any interruption in service or loss of data may cause a huge financial impact, or may even result in bankruptcy if the interruption is long enough. So it makes sense to reduce the risk of this happening from multiple avenues. Some examples are:

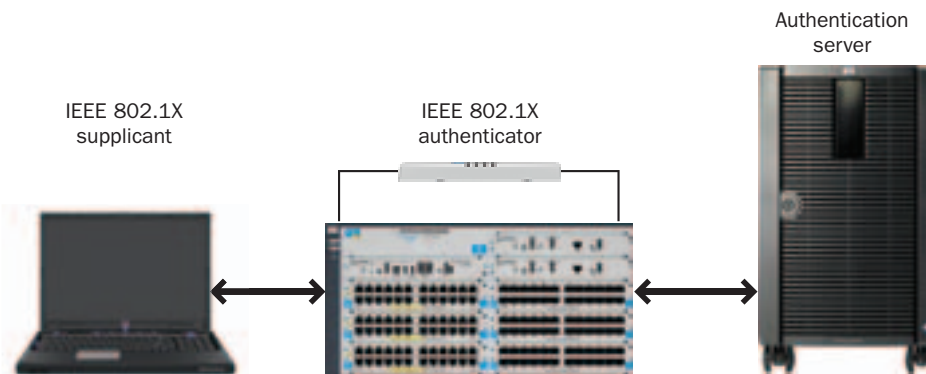
- Having a sound backup strategy
- Having a workable disaster recovery plan
- Having a redundant infrastructure
- Protecting against external threats
- Protecting against internal threats

This white paper discusses protecting networks from internal threats and, more specifically, identifies the first line of defense against internal threats as Network Access Control.

Network Access Control is a mechanism to help ensure that only appropriate users, who use only appropriate clients, can obtain appropriate access rights to the network. This helps defend against intentional and unintentional threats. Intentional threats can include unauthorized users trying to access any data or authorized users trying to access data they should not have access to. Unintentional threats can include authorized users that have a virus-infected laptop.

Network Access Control works by evaluating multiple criteria of a user that tries to connect to the network, before setting the appropriate access right, or by denying access completely. Company policy dictates which criteria are used, and the network administrator can configure the network infrastructure to reflect this. Depending on which equipment and software are used, there can be different possible criteria.

The framework used to achieve this is called IEEE 802.1X, which is an open standard developed by HP and Microsoft, among other companies. In the most basic setup, three components are needed:



- **IEEE 802.1X supplicant**—the entity requesting access to the network, such as the supplicant integrated in many Microsoft Windows versions
- **IEEE 802.1X authenticator**—the entity requiring authentication from the supplicant, such as ProCurve switches and access points
- **Authentication server**—the entity providing verification of the credentials provided by the IEEE 802.1X supplicant, usually a RADIUS server, such as Microsoft Network Policy Server

When a client connects to an IEEE 802.1X-enabled network—either wired or wireless—the following steps take place (the steps listed here are simplified; for complete details of the process, please reference RFC 3580):

- At first, only IEEE 802.1X traffic is allowed between the supplicant and the authenticator. Any other traffic the client sends will be dropped.
- The authenticator will request authentication from the supplicant.
- The supplicant provides the authenticator with its credentials.
- The authenticator forwards the credentials to the authentication server.
- The authentication server verifies the credentials and returns either an accept or a reject message to the authenticator.
- The authenticator will either allow or deny network access based on the message.

ProCurve Identity Driven Manager overview

ProCurve Identity Driven Manager (IDM) is a plug-in for ProCurve Manager Plus (PCM+) that extends the functionality and capabilities of a basic IEEE 802.1X setup, as mentioned earlier. Besides the provided credentials, IDM is also capable of using other criteria to make decisions. With IDM, the result can be more detailed than a simple reject or accept.

The criteria IDM can use are the following:

- **User identity, including group membership.** Using a user directory, such as Microsoft Active Directory, IDM can differentiate between users and/or groups, such as John and Jane or Finance users and Research users.
- **Time.** Configured by an administrator, IDM can differentiate between times, such as working days from 9 a.m. to 5 p.m., holidays, or any other configured times, including start and end dates.
- **Location.** IDM can differentiate between different locations as specific as a single port on a switch or an access point, or as broad as a building, a site, or the entire network and everything in between.
- **Device ID.** Defined as the Media Access Control (MAC) address of a device, allowing users to be tied to clients, such as specific computers or PDAs.

Each criterion can be used separately, in combination with others, or not at all, providing flexibility in differentiating between situations that need different network access rights. For example, John from Finance working at 10 a.m. from the third floor needs different network access than Jane, who is a guest to the company and is checking her e-mail wirelessly from the company cafeteria.

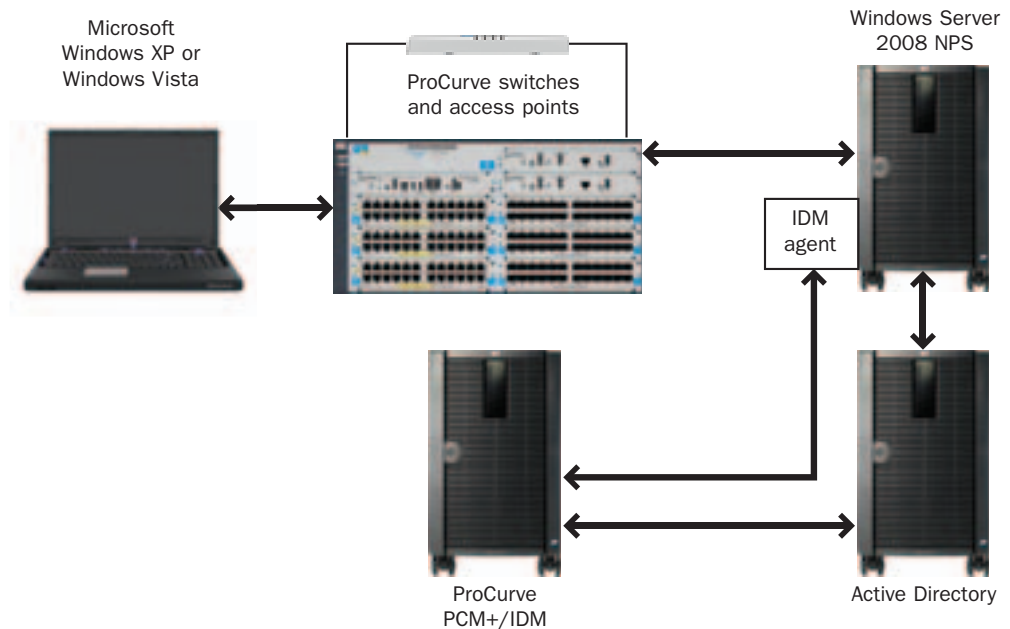
To complement this flexibility, IDM allows the IT administrator to tailor network access based on the criteria mentioned. To achieve this, IDM is capable of the following per-user security and performance settings, in addition to allowing or denying access completely:

- **Virtual local area network (VLAN)**—logically group clients that have similar network needs, such as segregating Finance and Research users
- **Access Control Lists (ACLs)**—per-user ACLs allow access to network resources to be controlled at the entry point of the user—from either a switch port or access point, such as denying access to the Finance server or permitting traffic to the Internet
- **Quality of Service (QoS)**—setting the priority of the traffic originating from a user, such as setting a lower priority for guest users
- **Rate limits**—limiting the available bandwidth, such as limiting the bandwidth for guest users that only need to check their e-mail

Each per-user setting can be used separately, in combination with others, or not at all, providing appropriate network access for each user in each situation.

IDM uses an agent on the RADIUS (authentication) server for evaluating all criteria and for setting all per-user settings. Each IDM agent can work independently from the IDM server, allowing redundancy to be achieved with multiple RADIUS servers, rather than with multiple RADIUS servers and multiple IDM servers. The IDM server is used as a graphical front-end for configuration, event logging, and reporting.

IDM is also capable of using other frameworks besides IEEE 802.1X, namely Web-authentication and MAC-authentication. But these are outside of the scope of this document. When using IDM, the setup is extended from the basic setup and now has the following components:



- **Microsoft Windows Vista**—The client trying to access the network is running Windows Vista and uses the built-in supplicant for the authentication.
- **ProCurve switch**—The switch is the authenticator and will require authentication from the client.
- **Microsoft Network Policy Server (NPS)**—The RADIUS (among other things) server provided with Microsoft Windows Server 2008 will act as the authentication server.
- **Active Directory**—The user directory that holds all user information, such as group memberships and credentials.
- **IDM agent**—The part of IDM that evaluates the criteria and controls the per-user settings.
- **PCM+/IDM**—The part of IDM where configuration changes are made, events are logged, and where the network administrator can create reports.

When the client connects to this network, the following steps occur (simplified here):

- At first, only IEEE 802.1X traffic is allowed between the Windows Vista supplicant and the ProCurve switch. Any other traffic the client sends will be dropped by the switch.
- The ProCurve switch will request authentication from the Windows Vista supplicant.
- The Windows Vista supplicant provides the ProCurve switch with its credentials.
- The ProCurve switch forwards the credentials to the Microsoft NPS server.
- The Microsoft NPS server verifies the credentials against the Active Directory.

- The IDM agent evaluates the other criteria: group membership, time, location, and MAC address.
- The IDM agent returns the appropriate per-user settings to the Microsoft NPS server, such as VLAN, ACLs, QoS, and rate limits.
- The Microsoft NPS server sends the ProCurve switch the results.
- The ProCurve switch sets the per-user settings and allows the appropriate access.
- The IDM agent sends an event to the IDM server.

The IDM server receives events from the IDM agents, such as logon and logoff events. These events contain a lot of detail about the user logging on or off, including the time, location, MAC address, and bytes sent and received. This allows the network administrator to see who is connected to the network currently, including their details. Information about these sessions is stored, so it is also possible to view previous session details. With this historic data available, it is possible to generate reports from within IDM. There are multiple reports that are predefined, such as bandwidth usage (top users) and per-user session reports.

Microsoft Network Access Protection overview

Microsoft Network Access Protection (NAP) was introduced with the release of Microsoft Windows Server 2008. It provides functionality to control access to network resources based on a client's identity and compliance with corporate governance policy. NAP is capable of providing this functionality for the following types of network access communication:

- IEEE 802.1X-authenticated network connections
- Internet Protocol Security (IPSec)-protected traffic
- Remote access Virtual Private Network (VPN) connections
- Dynamic Host Configuration (DHCP) address configurations
- Terminal Services Gateway connections

This section focuses on how NAP extends the basic IEEE 802.1X setup with determining the degree of compliance of a connecting client. The other methods are outside of the scope of this document. The server components of NAP run on Microsoft Windows Server 2008, whereas the client component is available on Microsoft Windows Server 2008, Windows Vista, and Windows XP Service Pack 3.

NAP determines the level of compliance by validating the client's health state against the health requirement policies, as defined by the administrator. NAP includes the following configurable health requirements for Microsoft Windows 2008, Windows Vista, and Windows XP Service Pack 3:

- The client computer has firewall software installed and enabled
- The client computer has antivirus software installed and enabled
- The client computer has current antivirus updates installed
- Microsoft Update Services is enabled on the client computer
- The client computer has all recent software security updates installed of a configurable severity
- The client computer has antispyware software installed and enabled (only for Windows Server 2008 and Windows Vista)
- The client computer has current antispyware updates installed (only for Windows Server 2008 and Windows Vista)

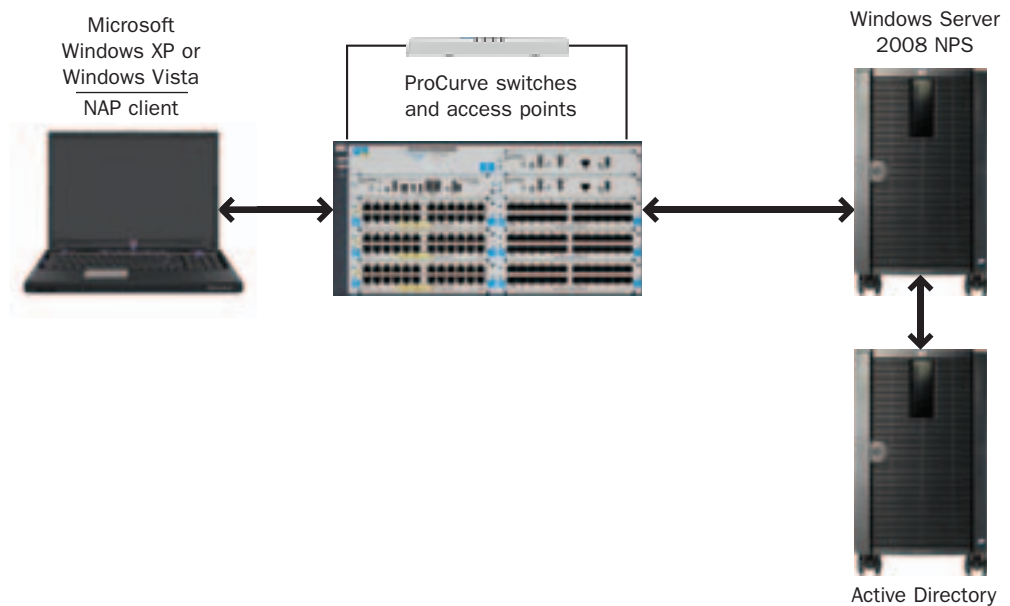
With NAP, Microsoft also released an API, which allows third-party software vendors to create their own health requirements, extending the possibilities of what a client can be checked for.

When the level of client compliance is determined, NAP can allow unrestricted access, limited access, or no access. There are two ways that NAP can restrict network access:

- Using a VLAN
- Using an user-based ACL

This allows the administrator to configure access to only certain resources, such as remediation servers. For example, remediation servers can be servers that hold the antivirus updates or antispyware updates, so the client can automatically update itself to become compliant again. NAP also has the capability to automatically remediate a client, such as enabling the firewall or enabling automatic updates.

When using NAP, the setup is extended from the basic setup and now has the following components:



- **Microsoft Windows Vista**—The client trying to access the network is running Windows Vista and uses the built-in supplicant for the authentication.
- **NAP client**—The built-in NAP client is responsible for collecting the system health information of the client.
- **ProCurve switch**—The switch is the authenticator and will require authentication from the client.
- **Microsoft Network Policy Server (NPS) running NAP**—The RADIUS (among other things) server provided with Microsoft Windows Server 2008 will act as the authentication server and the health policy server.
- **Active Directory**—The user directory that holds all user information, such as group memberships and credentials.

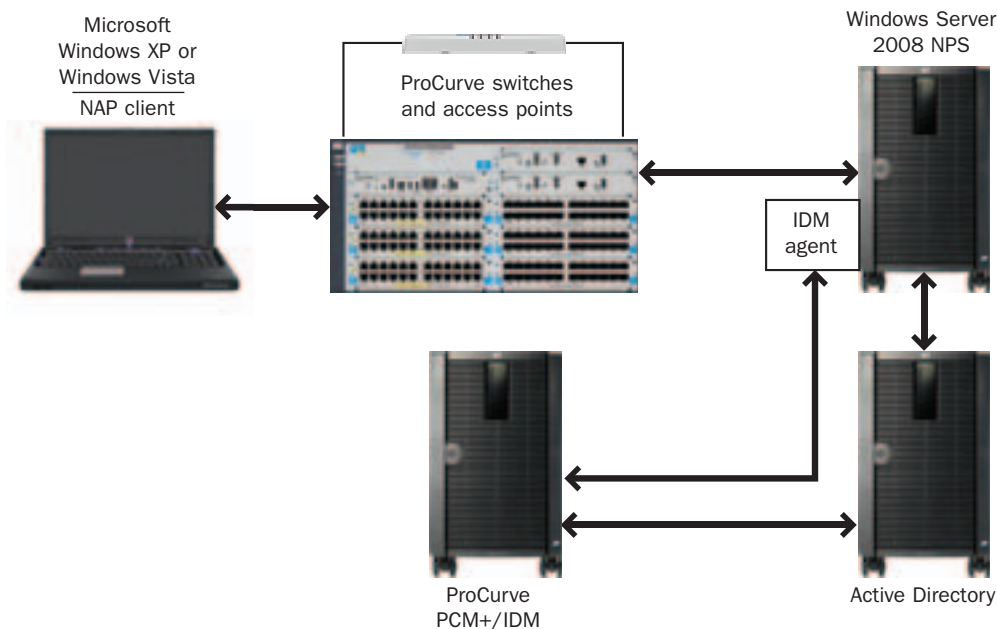
When the client connects to this network, the following steps occur (simplified here):

- At first, only IEEE 802.1X traffic is allowed between the Windows Vista supplicant and the ProCurve Switch. Any other traffic the client sends will be dropped by the switch.
- The ProCurve switch will request authentication from the Windows Vista supplicant.
- The Windows Vista supplicant provides the ProCurve switch with its credentials.

- The ProCurve switch forwards the credentials to the Microsoft NPS server.
- The Microsoft NPS server verifies the credentials against the Active Directory.
- If the credentials are valid, the NAP server requests the health state from the NAP client.
- The NAP client sends its health state to the NAP server.
- The NAP server evaluates the health state and determines if the client is compliant.
- The NAP server returns the result to the NAP client and sets the appropriate parameters on the ProCurve switch.

ProCurve IDM and Microsoft NAP integrated

ProCurve IDM integrates seamlessly with Microsoft NAP to provide a complete Network Access Control solution. IDM is capable of interpreting the compliance state that the NPS server returns and using it as one of its criteria to determine which per-user settings to configure on the switch or access point. When IDM and NAP are integrated, the setup has the following components:



- **Microsoft Windows Vista**—The client trying to access the network is running Windows Vista and uses the built-in supplicant for the authentication.
- **NAP client**—The built-in NAP client is responsible for collecting the system health information of the client.
- **ProCurve switch**—The switch is the authenticator and will require authentication from the client.
- **Microsoft Network Policy Server (NPS) running NAP**—The RADIUS (among other things) server provided with Microsoft Windows Server 2008 will act as the authentication server and the health policy server.
- **Active Directory**—The user directory that holds all user information, such as group memberships and credentials.
- **IDM agent**—The part of IDM that evaluates the criteria and controls the per-user settings.
- **PCM+/IDM**—The part of IDM where configuration changes are made, events are logged, and where the network administrator can create reports.

When the client connects to this network, the following steps occur (simplified here):

- At first, only IEEE 802.1X traffic is allowed between the Windows Vista supplicant and the ProCurve switch. Any other traffic the client sends will be dropped by the switch.
- The ProCurve switch will request authentication from the Windows Vista supplicant.
- The Windows Vista supplicant provides the ProCurve switch with its credentials.
- The ProCurve switch forwards the credentials to the Microsoft NPS server.
- The Microsoft NPS server verifies the credentials against the Active Directory.
- If the credentials are valid, the NAP server requests the health state from the NAP client.
- The NAP client sends its health state to the NAP server.
- The NAP server evaluates the health state and determines if the client is compliant.
- The NAP server returns the result to the NAP client.
- The IDM agent evaluates the other criteria: group membership, time, location, and MAC address, including the client's compliancy.
- The IDM agent returns the appropriate per-user settings to the Microsoft NPS server, such as VLAN, ACLs, QoS, and rate limits.
- The Microsoft NPS server sends the ProCurve switch the results.
- The ProCurve switch sets the per-user settings and allows the appropriate access.
- The IDM agent sends an event to the IDM server.

Because NAP and IDM share a lot of the same components, there is no need for redundant configuration tasks or even redundant software installations. There is, for example, no need to have two clients on the user's computer, and both NAP and IDM use the same Active Directory. This allows for administration from a single interface, once initial configuration is completed. Getting an overview of which current users are online, getting a detailed report about a user that includes bandwidth usage and login times, or changing per-user performance and security settings can all be done from within the IDM application, including generating reports on company policy compliancy of clients. Integrating IDM and NAP is as easy as installing the IDM agent on the NPS server.

Conclusion

Integrating Microsoft Network Access Protection and ProCurve Identity Driven Manager allows for a complete Network Access Control solution. Appropriate security and performance settings can be configured based on the user's identity, location, time, MAC address, and client's compliancy. IDM and NAP are built on IEEE 802.1X, an open standard that allows flexibility and cooperation between vendors. NAP also includes an API that allows software vendors to create their own health checks. Because of the tight integration between IDM and NAP, administration overhead is minimal. With Microsoft NAP and ProCurve IDM working together, the risks from internal threats are greatly reduced. The network will not allow unauthorized users to have access, but grants appropriate access to authorized users. Appropriate access also means limited access if the user's client does not comply with company policy.

For more information

To find out more about ProCurve Networking products and solutions, visit our Web site at **www.procurve.com**

© Copyright 2008 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.

Microsoft, Windows, and Windows Vista are U.S. registered trademarks of Microsoft Corporation.

4AA2-1544ENW, August 2008

