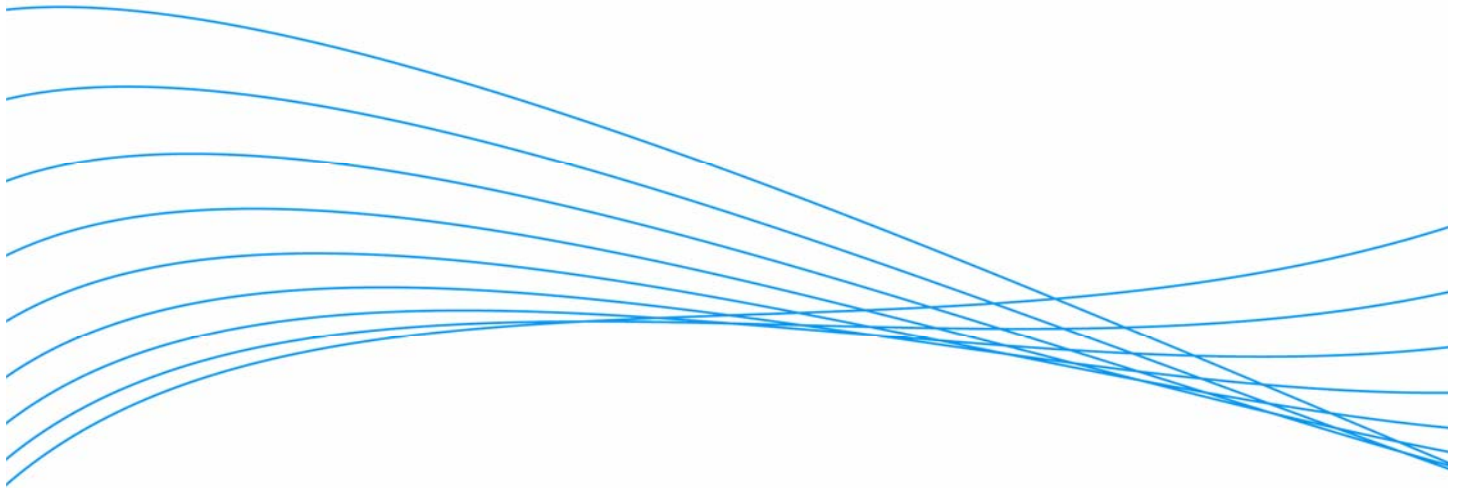


Identity Driven Management Technical Brief



| | |
|--|---|
| Introduction | 2 |
| Transitioning Networks from a Technology Resource to a Business Resource | 2 |
| Intelligent Network Access through Identity Driven Management (IDM) | 3 |
| ProCurve's IDM Solution | 3 |
| ProCurve Identity Driven Manager 2.0 | 3 |
| Utilizing IDM | 4 |
| How IDM Works | 5 |
| IDM Architecture and Implementation | 6 |
| Summary | 7 |
| For more information | 8 |

Introduction

Just as network infrastructures are evolving from a pure technology resource to a utilitarian business resource, so too are strategies associated with network management and access control.

Traditionally, network management's principal responsibilities have been facilitating the discovery of devices, ensuring they are properly configured and establishing the linkage between those devices and the services residing on the network. Largely disregarded, however, have been the unique needs and business objectives of those using the network.

A new approach is to push intelligence to the edge of the infrastructure to enable Identity Driven Management (IDM). ProCurve Networking by HP is a leading enabler of intelligent EDGE networks and offers robust IDM functionality for an advanced, dynamic, adaptive and easy-to-manage infrastructure.

This paper discusses the transition to IDM and highlights ProCurve's IDM solution. It also describes how the solution integrates with a company's existing security and access framework to improve workforce productivity, enhance network security, management and performance, and better serve overall business needs.

Transitioning Networks from a Technology Resource to a Business Resource

Enterprise networks have historically been more of a technology tool than a business tool. The primary areas of focus have been connecting user devices with the enterprise infrastructure and preventing network downtime. Static, simple configuration has been employed for static, simple connectivity across multiple domains, with more complex functions, such as traffic routing, security and performance, left to core routing switches.

With this traditional model, networks behave uniformly no matter what user is connecting to the network, whether it is a guest or a CIO. In fact, the network has historically been unable to distinguish among different users.

This strategy of network management, with limited or non-existent access control, not only hinders workforce productivity, but also creates several problems and limitations associated with network security, management and performance. Traffic is allowed on the network before it can be identified, creating security concerns; new edge devices, applications and traffic types require tedious network reconfigurations; and traffic routing is inefficient, oftentimes creating unnecessary traffic that can impact core router performance.

Above all, with an overriding emphasis on enabling connectivity and maintaining network operation, users' varying access, application, bandwidth and quality of service (QoS) needs are largely disregarded. This creates roadblocks to continually improving workforce productivity, information security, network resiliency and overall business efficiency.

Fortunately, network technologies have matured and companies are realizing their infrastructures can better serve organizational and user needs. This realization has spawned a transition from device- and connection-oriented networks to user- and business-oriented networks.

In order to make this transition, organizations face several business and information technology (IT) challenges.

Key business challenges:

- Enabling users to access just the right network resources to achieve a business result
- Simplifying the management of network privileges to people across the business
- Facilitating real-time network adaptation in accordance with changing business needs and the deployment of new applications

Key IT challenges:

- Adapting network behavior based on the “appropriate” business need of the user
- Implementing an industry-standard way to control network behavior for each user
- Establishing a single pane of glass to configure and administer policies across the network
- Simplifying and automating the administration of privileges and policies

Intelligent Network Access through Identity Driven Management (IDM)

Pioneered by ProCurve, a new model of network management and access facilitation is to push intelligence from the center of the network to the edge, where users connect and policies are enforced. In doing so, organizations can employ intelligent network access through IDM.

IDM helps companies maximize network resources and improve productivity by enabling automatic configuration of the network edge through security and performance policies defined on a centrally administered management server. IDM solutions make this possible by allowing network administrators to define network access policies which dynamically apply security and performance settings as users connect to the network. These policies are defined based on user, device, location, time and other variables and are applied to all ProCurve adaptive-edge devices: both wired and wireless. The result is a unified management infrastructure and a more secure, mobile, multi-service network.

IDM is the groundwork for creating an intelligent network that is able to prevent unauthorized use and deliver an adaptive, user-friendly experience for a more productive workforce while securing important business information from prying eyes.

ProCurve’s IDM Solution

ProCurve is a leader in enabling business-driven networks that behave uniquely and appropriately for every user. The foundation of such a network is the ProCurve Adaptive EDGE Architecture™, which facilitates ProCurve’s command from the center (ProCurve Manager Plus and IDM) with control to the edge (intelligent edge devices).

With intelligence pushed to the edge, security is enhanced, traffic prioritization is improved and users can connect anytime, anywhere with a consistent view of the network. With Command-from-the-Center, companies have centralized control of network configuration, making it easier to implement new applications and support new network services across the enterprise.

More importantly, with Command from the center and control to the edge, the network is able to adapt dynamically to business and user needs.

ProCurve Identity Driven Manager 2.0

Building upon the foundation of the Adaptive EDGE Architecture, ProCurve now offers breakthrough IDM functionality with ProCurve Identity Driven Manager 2.0 (IDM 2.0).

IDM 2.0 software dynamically manages network devices to provide appropriate, optimized network access that increases productivity and overall efficiency while enforcing security. It automatically applies security, access and performance settings to network infrastructure devices based on user, device, health of the device, location and time. IDM 2.0 manages wired

and wireless connections in conjunction with RADIUS authentication servers and is able to synchronize users and group membership from existing enterprise directories.

IDM 2.0 enables command from the center by automating the configuration of intelligent edge devices to provide unique behavior for every individual or group. It provides control to the edge by ensuring switch and access point features make the correct decisions and enforce policies at the perimeter of the network. This creates the ability to easily manage and facilitate:

- Access Control – Based on users' business needs.
- Access Rights – Based not only on the individuals and their group associations, but also on the device they are using (i.e., PC, laptop, PDA, or VoIP phone), day, time and location.
- Policy Enforcement – On a per-user, per-session basis.

IDM 2.0 is an add-on module to ProCurve Manager Plus, a complete, Windows-based network management solution for companies using ProCurve products. ProCurve Manager Plus allows users to discover, configure, monitor and troubleshoot ProCurve devices and offers advanced features such as configuration management, VLAN management, in-depth traffic monitoring, group and policy management and automated software updates.

Utilizing IDM

IDM 2.0 enables the edge of the network to adapt to each user individually. Whether the user is a guest, employee or special high-priority person, he or she receives a unique, albeit consistent, network experience. The network behaves appropriately according to each user's particular access rights, no matter where or when they access the network or what device they are using.

Figure 1 illustrates the typical IDM user experience. After the network administrator establishes the appropriate users, groups and access rules, the network is able to dynamically and automatically configure itself on a per-user, per-session basis.

A "guest" logging in from the conference room receives Internet-only access, with a limit of 2Mbps. An "employee" logging in has access to the corporate server as well as the Internet. Users whose PCs do not comply with business policies are given access only to servers that will allow them to bring their system into compliance. For example, they might need to run virus software or install required software or patches. In addition, users designated as higher priority have their traffic is tagged with appropriate priority bits.

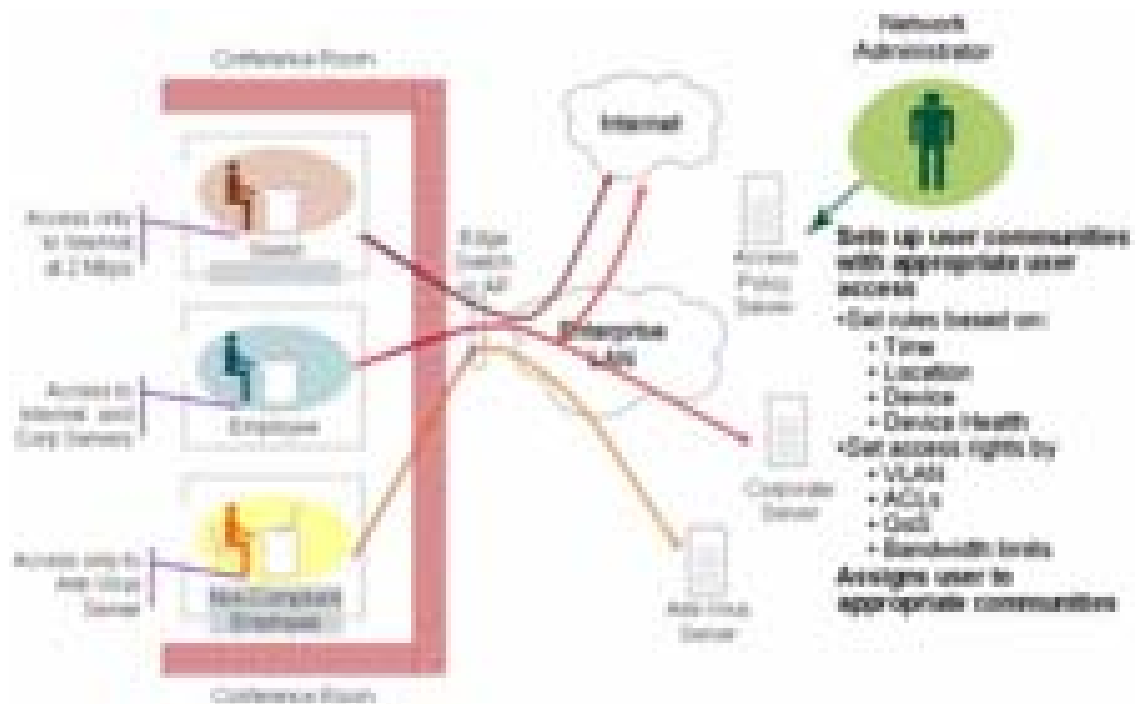


Figure 1. IDM User Experience

How IDM Works

IDM 2.0 operates within the general concept of “Realms,” which are also sometimes called “Domains.” Realms are typically large organizational units and every user belongs to one – and only one – Realm. Many companies utilize only a single Realm.

The fundamental configuration model of ProCurve’s IDM solution goes two steps further to create specificity based on Users and Groups. Every User belongs to a Group (called an Access Policy Group). Each Access Policy Group has an Access Policy defined for it, which governs the access rights that are applied to its Users as they enter the network.

The Access Policy is defined using a set of Access Policy Rules. These rules consider several inputs:

- Location – From where is the user accessing the network?
- Time – What time is the user accessing the network?
- Device – From what device is the user accessing the network?
- Device Health – Is the device running the company required software?

Using these input parameters, IDM 2.0 evaluates each of the rules. When a matching rule is found, the Access Rights (called an Access Profile) associated with that rule will be applied to the user. The Access Profile defines the VLAN, Access Control Lists (ACLs), QoS and bandwidth rate-limits that will be applied to the user as they access the network.

IT personnel need define only the Access Policy Groups and establish an Access Profile for each Access Profile Group. Users can be automatically assigned to groups based on information in the existing company directory, or assigned to groups by the administrator. Once users are assigned to an appropriate group, IDM 2.0 automatically handles the remaining access and service tasks. Based on the rules defined for the Access Policy Group, the user will get the appropriate level of access to resources and services on the network.

When new users or employees need access to the network, IT personnel can simply add them to an existing Access Policy Group. And when access rights need to change, modifications can

be made to particular Access Policy Groups, which are automatically propagated to and enforced for each of the group's users.

Figure 2 illustrates how the network automatically configures itself for each user, considering factors such as location, time and system to implement varying VLAN, ACLs, QoS and bandwidth rate-limit policies.

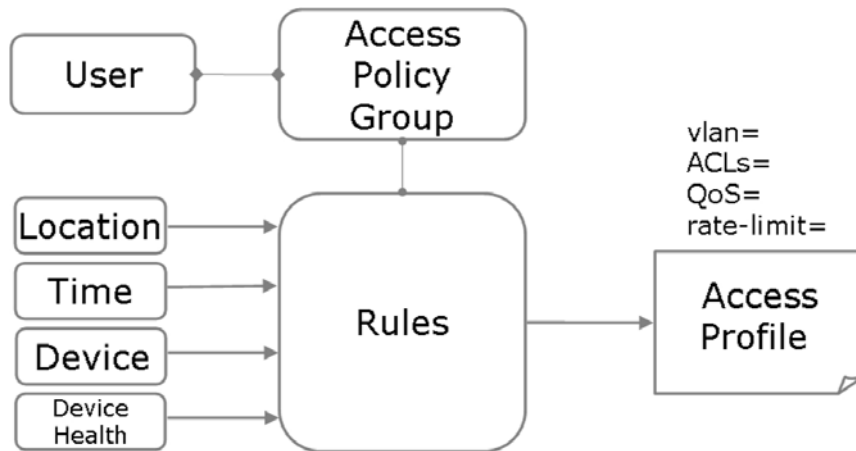


Figure 2. IDM Configuration Model

IDM Architecture and Implementation

Implementing IDM 2.0 requires an existing RADIUS authentication solution or ProCurve Access Control Solution. There are many options for establishing such a solution, but all include three major components: supplicant/client (supporting 802.1X, Web Authentication or MAC Authentication), ProCurve switch or wireless access point and RADIUS Servers: Microsoft Internet Authentication Service, Funk Steel-Belted Radius and FreeRADIUS. These three components form the primary framework on which IDM 2.0 operates.

Without IDM functionality, client traffic is routed by the edge switch or access point to the RADIUS server through a standard RADIUS protocol. The RADIUS server then accesses the user database to find valid users and create a match. When the user has been validated, the RADIUS server allows access by passing authentication information back to the edge device, at which point the user is placed on the network.

When IDM functionality is added to the equation, these processes are not interfered with or altered. IDM 2.0 simply adds to them. Even user authentication tasks (user names, passwords, etc.) remain unchanged through the use of IDM 2.0.

An IDM Agent runs co-resident with the RADIUS server and takes action when a user authenticates to the network through the server. The IDM Agent is able to restrict network access and/or add authorization parameters to the RADIUS reply, which is routed to the device to specify the access rights of the user. These parameters are sent as RADIUS attributes and the switch then applies them to the client access port for the duration of the connection.

The ProCurve Manager Plus Server with IDM 2.0 module, IDM Agent installed on the RADIUS Server and ProCurve edge devices work together to perform the following roles:

- ProCurve Manager Plus Server with IDM 2.0 – Stores and accesses defined policies
- IDM 2.0 Agent – Implements policy decisions for each user
- ProCurve edge devices – Enforces policies on a per-session basis

IDM 2.0 merely augments the security system already in place by adding advanced network access rights and parameters as defined by IT management.

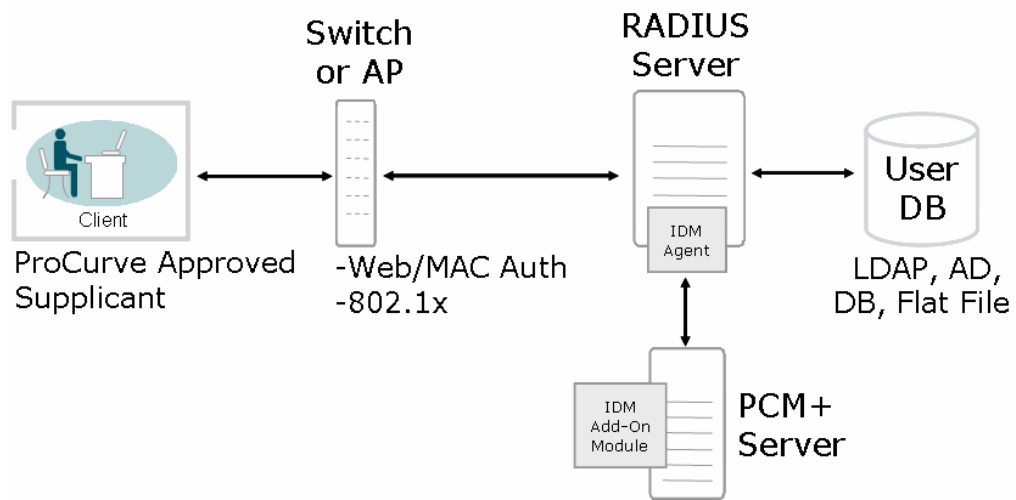


Figure 3. IDM Architecture

Summary

By utilizing ProCurve's IDM solution, companies are able to reap the benefits of a dynamic network that behaves uniquely and appropriately for every user. Not only does this enhance workforce productivity, it also improves network security, management and performance.

Most importantly, with an adaptive infrastructure that configures itself based on individuals and their particular access rights and service needs, the network better serves business and user objectives rather than simply facilitating technology connectivity.

For more information

To learn more about ProCurve Networking solutions, contact your local HP sales representative or visit our Web site at: www.procurve.com.

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

www.procurve.com



© 2006 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.

4AA0-0106ENW Rev. 1, 3/2006