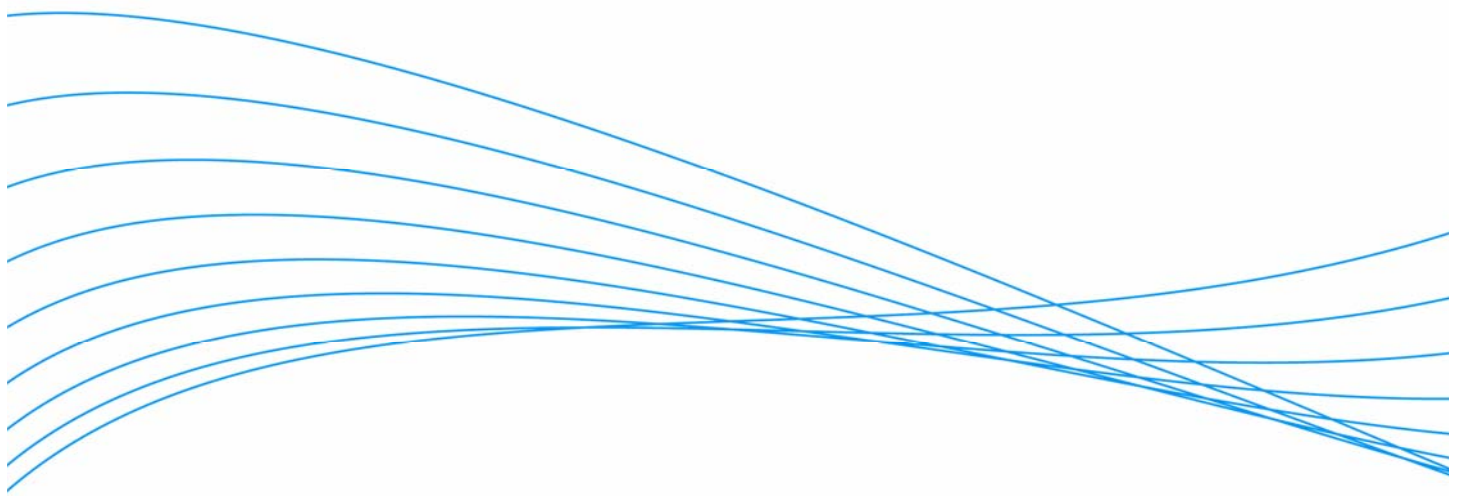


Delivering Intelligent Network Access Through Identity Driven Management



Introduction	2
The Old Model: Technology-Driven Network Access	2
Security	2
Management	2
Performance	3
Operation	3
The New Model: Identity-Driven Network Access	3
ProCurve Networking's Approach to IDM	3
IDM Today and Tomorrow	4
The Value of Deploying ProCurve IDM Solutions	5
Summary	5
For More Information	6

Introduction

In establishing their information technology (IT) networks, companies have traditionally focused on the connection between user devices and the corporate infrastructure, ignoring the unique needs of individuals and groups using the network. Not only does this emphasis hinder workforce productivity, it also creates problems for network security, management and performance.

A new strategy is to implement identity driven management (IDM) functionality that is able to automatically configure the network edge through security and performance policies defined on a centrally administered management server. These IDM solutions facilitate business-driven networks that behave uniquely and appropriately for every user.

This paper describes traditional network access management strategies and defines ProCurve Networking by HP's approach to a new, identity-driven methodology. It also highlights the benefits that can be attained by deploying ProCurve IDM solutions.

The Old Model: Technology-Driven Network Access

Network management and operation have traditionally, and quite obviously, been a technology-focused endeavor. Getting enterprise networks up and running and maintaining performance over time has required a distinct focus on connection facilitation. The emphasis has been to make sure various clients, such as personal computers (PCs), laptops and personal digital assistants (PDAs), can link to the network from various locations, such as a local-area network (LAN) or dial-up connection.

The network's principal responsibilities, therefore, have been discovering 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 users' varying access, application, bandwidth and quality of service (QoS) needs.

With this old model, all network intelligence and decision-making abilities are placed in the core devices, handling device identification and enforcement of access and security policies. Basic, simplistic configuration is employed for basic, simplistic connectivity across multiple domains to ensure the core switches can handle all identification and connection decisions. Conversely, edge devices are essentially unintelligent and unable to assist in the authentication and connection process. They are able only to pass packets to the core routing switch, with no recognition or decision-making capacity.

As a result, the infrastructure behaves uniformly no matter what user is connecting to the network, whether it is a guest or a CIO. In fact, the network is unable to distinguish among different users, and is capable only of recognizing the devices through which these users are trying to connect.

This traditional model of network management and access facilitation not only hinders workforce productivity, but also creates several problems and limitations. Chief among them are challenges associated with network security, management, performance and operation.

Security

Security is frequently compromised and difficult to manage with traditional network access strategies. Because the infrastructure is able only to recognize clients connecting to the network, there are no safeguards to identify the people operating these clients. And since all decision-making and access enforcement responsibilities reside in the core devices, users are oftentimes already on the network before the core routing switches are able to identify and approve their clients' access rights, if at all. Furthermore, networks are frequently left wide open within a building or campus, with security gates being relegated to users logging on remotely; few, if any, safeguards exist at the port level. Consequently, most enterprise networks offer minimal, inconsistent security checks, clearing the way for malicious traffic to infiltrate the infrastructure.

Management

The traditional model of device- and connection-centric infrastructure also renders network management complex and expensive. Network administrators have to manually configure each core routing switch and edge switch to behave a particular way for a particular client or service.

There is no specificity of network behavior based on individuals or groups with varying network requirements. The result is a static, rigid infrastructure that, once configured, does not change or adapt.

Nevertheless, change is an inescapable truism in the business world. With organizational and technological needs continually evolving – new applications and network services, new edge switches, wireless network connections, new clients that connect to the network, new employees, etc. – companies get locked into an ongoing, time-consuming, expensive cycle of network reconfigurations, redesigns and upgrades.

Performance

Network performance can also be compromised through this model because various individuals and groups have diverse networking needs. For example, an engineering organization may need constant, uninterrupted access to high-bandwidth services such as computer-automated design (CAD) applications, whereas guests may need only Internet access. However, with the network behaving uniformly for every user, there is no prioritization for these particular individuals or the groups with which they are associated. This hinders an organization's ability to create efficiencies and maximize network performance based on factors such as traffic, bandwidth and QoS propagation.

Operation

Lastly, traditional access management renders network operation more of a technology function than a business function. The overriding emphasis is on enabling connectivity and maintaining network performance, not meeting business objectives and users' unique needs. This creates roadblocks to continually evolving and improving overall business efficiency and performance.

The New Model: Identity-Driven Network Access

Pioneered by ProCurve, a new model of network management and access 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 implement intelligent network access through IDM.

IDM helps companies maximize network security and improve productivity by enabling automatic and dynamic configuration of the network edge through security and management policies defined on a centrally administered management server. IDM solutions make this possible by allowing network administrators to define network access policies that 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 and converged 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.

ProCurve Networking's Approach to IDM

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 delivers continuous command from the center with control to the edge.

With intelligence pushed to the edge, security is enhanced, traffic prioritization is improved and users can connect anytime, anywhere with a singular 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 traffic types 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 IDM solutions use command from the center to dynamically automate the configuration of the edge to provide unique behavior for every individual or group. Control to the edge allows switch and access point features to make correct decisions at the perimeter of the network. This creates the ability to easily manage and facilitate:

Access Control – Based on users and their business needs, not their device type or physical location.

Access Rights – Based not only on the individuals and their group associations, but also on the device accessing the network, as well as day, time, location, applications and services.

Policy Enforcement – On a per-user, per-session basis.

Some have argued that intelligence at the edge of the network poses unmanageable complexity for an IT organization to handle. They contend it is conceptually easier to implement and manage intelligence at the core in a couple of switches versus the edge, where there are potentially thousands of ports and even more users.

However, if the configuration and desired behavior of that intelligence is automated, and the complexity remains behind the scenes, network management becomes simpler at the same time that the user experience is enhanced.

Just as configuring each switch and port for every potential user is unrealistic, so is manually creating unique profiles for each user. Creating communities based on common user needs is a more reasonable solution. Communities are formed around particular user groups that have common networking requirements. They contain specific resources as well as specific users that need those resources.

Users can be defined by a particular department, such as marketing, or task, such as purchasing. Resources include applications, servers, printers, Internet, intranet, etc. Attributes define when, where and how the users and resources connect.

These communities are dynamic. Users, resources and attributes can all be added, removed or adjusted (command from the center), creating flexibility and allowing the communities to change in accordance with business needs (control to the edge).

Based on a particular community's parameters – users, resources and attributes – the network is able to authenticate the user and adapt itself to that person uniquely, regardless of location or device type.

Through IDM authentication, the network determines the following and subsequently provides the proper resources and levels of access for each user:

- Who is the user?
- Where is the user (switch/port or access point/SSID)?
- With what community(s) is the user associated?
- What resources are connected to that community(s)?
- What attributes are assigned to that community(s)?

Based on these parameters, the appropriate information and access rights flow from the centrally administered database (where they're created and stored) to the edge (where they're implemented and enforced).

This approach is significantly different from the traditional strategy, where a particular switch and particular port were configured to act in a particular way. This new methodology enables any switch and any port, or wireless connection, to act uniquely for each individual. It provides the user with the same network functionality, resources and view no matter where or how they connect.

This is the essence of an intelligent, adaptive network in general, and IDM in particular. The network no longer behaves uniformly – it behaves differently for each user.

IDM Today and Tomorrow

ProCurve solutions are inherently flexible and enable companies to enhance their networks over time, not continually rip and replace as new technologies become available.

Today's ProCurve IDM solutions authenticate individuals using RADIUS-based technologies already in place. Traditional authentication processes were a yes/no affair. If a user successfully authenticated, he or she was allowed on the network largely without restriction. If not, the user was simply denied access. In contrast, ProCurve IDM solutions authenticate users based on several factors, including their identity, client device, location, time of day and services for which they are given access rights.

To simplify the initial set-up, IDM software synchronizes with the customer's enterprise directory, providing network administrators with the ability to update the list of network users and their group membership from the current enterprise directory, such as Active Directory or any other LDAP directory. In addition, ProCurve IDM integrates with standard RADIUS authentication and the Trusted Network Connect (TNC) architecture.

Once a user is authenticated, IDM software automatically configures the particular edge device so the individual is able to access only the parts of the network, and the resources on the network, appropriate to his or her job. With the addition of dynamic user-based ACLs, the user can be allowed or denied access to specific network resources such as servers, printers and even network services such as Web surfing and instant messaging. Because of this intelligent auto-configuration of the network edge, connectivity is location- and media-independent. Network access is determined and granted based purely on the user and the services to which he or she has privileges.

Tomorrow's ProCurve IDM solutions will advance this process further. In addition to its current capabilities, IDM will be able to authenticate new network devices and apply device-level policies automatically. This secures the network infrastructure from unauthorized network additions, providing secure, consistent, policy-based security and performance configuration as the network expands or changes.

The Value of Deploying ProCurve IDM Solutions

The benefits of moving toward an identity-driven network access management model are significant. Network security is dramatically increased, with identification of particular users rather than of the clients through which they are attempting to gain network access. Furthermore, users are authenticated before they join the network, not after they have been placed on the network and directed to the core routing switch.

Network management and usage also improve through IDM. Since the core is able to automatically and dynamically configure the intelligent edge, network management is vastly simplified. In addition, with the network behaving uniquely for each individual and the complexity behind such behavior remaining transparent, network usage becomes easier.

Network performance can also be enhanced through IDM with traffic, bandwidth and QoS prioritization. This gives different groups varying levels of service to create efficiencies and maximize network operation.

Last but certainly not least, ProCurve IDM solutions ensure appropriate network usage and improve workforce productivity. With an adaptive infrastructure that configures itself based on each individual's particular access rights and service needs, the network better serves business and user objectives rather than simply facilitating technology connectivity.

Summary

Moving toward a user-centric model of network access management helps companies begin serving business and user needs instead of technology and connectivity needs. ProCurve IDM solutions push intelligence to the edge for automatic configuration of the network based on individuals and the unique requirements of their jobs. Network administrators can dynamically apply security and performance settings to network infrastructure devices based on user, location, time and other variables.

By enabling business-driven networks that behave uniquely and appropriately for every user, ProCurve IDM solutions improve not only workforce productivity, but also network security, management and performance.

For More Information

To learn more about ProCurve Networking solutions, contact your local ProCurve sales representative or visit our Web site at: www.procurve.com. To learn more about ProCurve wireless site assessment and installation services, go to: www.hp.com/go/procurveservices.

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

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.

4AA0-2000ENW Rev. 1, 3/2007