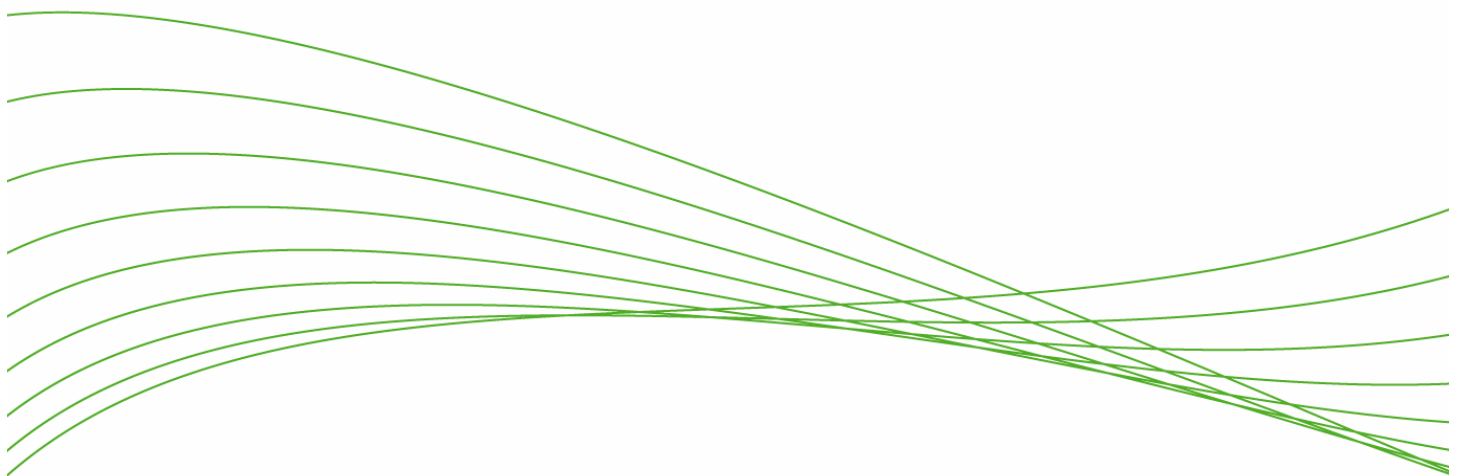


# ProCurve Secure Access 700wl Series User Authentication and Authorization Technical Brief



Authentication and Authorization in the 700wl Series.....	2
How the ProCurve 700wl Series System Identifies Users .....	2
Authenticating Users through Existing Databases .....	3
ProCurve 700wl Series Authentication Methods.....	3
Active Authentication .....	4
Browser-based Logon Authentication .....	4
Authentication using a VPN client .....	5
802.1X / WPA Authentication using the internal RADIUS server.....	5
Passive Authentication .....	5
802.1X authentication.....	5
NT domain authentication.....	6
Determining Access Authorization.....	6
Getting Group Information from a Database.....	6
RADIUS .....	7
LDAP .....	7
Kerberos.....	7
Retrieving Group Information Separately from Authentication.....	7
How Group Information Determines an Identity Profile .....	7
Authentication and Authorization Examples .....	8
For more information .....	10

# Authentication and Authorization in the 700wl Series

Networks commonly employ two complementary and related mechanisms for determining who can access information resources over the network – authentication and authorization.

Authentication is the process of determining the identity of a network user by verifying a set of user credentials, typically a user ID and password. Authorization is the process of determining what resources on the network – services, printers, servers, network devices etc. – a given user is allowed to access. Authorization is often determined by a combination of a group affiliation, restricted destinations (e.g. applications, servers, or intranet sites that require their own login) and physical barriers.

In a wired, switched network, the policy that controls what traffic an authenticated user can send and receive is typically based on the port through which the user is connected (via VLANs and ACLs) rather than on the user's identity. This works when only one user is connected via a given port. Also, where physical barriers (locked doors, cardkeys etc.) are used to control access, it can be assumed that a user who has physical access to a port is authorized to connect on that port.

When wireless access enters the picture, the identity of the user becomes crucial. Since multiple users can connect through a single wireless access point, the assumption of one user per port is no longer valid, and port-based access policies do not work. All sorts of users – visitors, temporary workers, system administrators, the CFO – may all happen to access the network via the same access point, sharing the same port. A single set of access rights for that port would be too permissive for some users and too restrictive for others. Therefore, the system must be able to distinguish between the users on a port, and apply policy based on each user's identity.

Further, given the range of wireless access point signals, physical barriers become meaningless; given the mobility of wireless devices, users are no longer constrained to connect only through specific ports. In a wireless network, therefore, it is important both to determine who the user is when he attempts to connect and to track the user throughout his entire session on the network. The system must be able to track the user if he or she physically moves (from desk to conference room, for example, roaming to a different access point and thus appearing on a different port) in order to enforce the appropriate policy for that user.

In most networks, the user's authenticated identity is not the only factor used to determine a user's access rights – access authorization is often based upon an individual's role within the organization. Employees in Finance may have access to restricted data and applications, for example, while system and network administrators typically have access to network equipment denied to other employees. Authentication and authorization may be tightly integrated, where the same mechanism that provides authentication services also provides information about a user's authorization level – often implemented through group membership, where a user's group affiliations denote what sort of permissions he has relative to the organization's information resources.

In addition to the user's identity, the ProCurve Secure Access 700wl series uses other factors that influence the access policy that is enforced for the user – specifically how the user has connected to the network (i.e. the location of the access point through which the user connects, and the time at which he connects). These factors are discussed in detail in the ProCurve Secure Access 700wl Series: Identity Based Access Control Technical Brief. This paper discusses only the authentication and authorization components of the 700wl series rights model.

Because user identity is so important, the ProCurve 700wl series system provides a broad range of capabilities for authenticating users, and then tracking, managing, and enforcing the appropriate policies for those users. The 700wl series can interface with a number of authentication databases, allowing it to take advantage of existing authentication services already in place within an organization. It can make use of the existing group structure to define what access policies should apply to a user based on his/her role within the organization.

## How the ProCurve 700wl Series System Identifies Users

The ProCurve 700wl series system identifies users through a combination of the MAC address of the client device, and the authenticated ID of the user associated with that device.

When a client connects to the network through an access point, the 700wl series detects the client's MAC address. If this MAC address is unknown to the 700wl series, the system will force the client to authenticate. The authentication process, if successful, will provide the user's ID to the 700wl system for use in tracking the client.

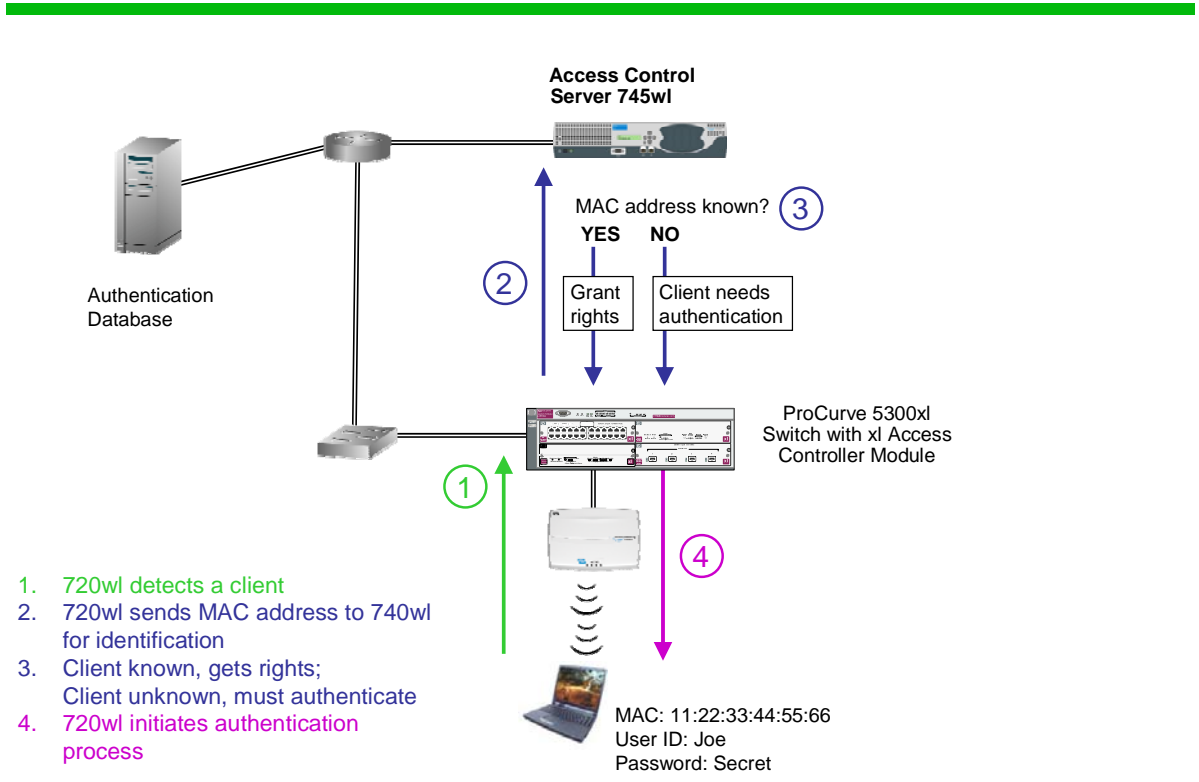


Figure 1. Identifying a Client

If the 700wl series identifies this MAC address as a known client (for example, a user that has moved from his desk to a conference room, and consequently has roamed from one access point to another) then the Access Policy currently in force for that client dictates whether that user will be required to re-authenticate before being granted new access rights, or whether his session can continue without change in user policy.

## Authenticating Users through Existing Databases

The ProCurve 700wl series supports multiple protocols that are used to communicate to different authentication databases, such as RADIUS, LDAP, and Kerberos. In a network where one of these authentication databases is already deployed, the 700wl series, specifically the Access Control Server 745wl, can use these protocols to communicate with the existing database to verify the user's credentials (authentication) and to determine what level of access the user should have (authorization). This means that a 700wl series system can be integrated seamlessly into an organization's existing authentication system without requiring additional databases.

## ProCurve 700wl Series Authentication Methods

The ProCurve 700wl series supports three basic types of authentication methods: Active, Passive, and MAC address authentication.

With *Active* authentication, the 700wl series receives user credentials directly, and in turn sends those credentials to an external authentication database for validation. Active authentication methods are implemented in the 700wl series either through browser-based logon (where the 700wl series presents a logon page to the user through their browser) or through VPN clients.

With *Passive* authentication, the 700wl series waits for an authentication action to occur, then “piggy backs” on that authentication. 802.1X is a passive authentication method in that the 802.1X authentication process happens directly between the authentication server (i.e. RADIUS) and the authenticator (access point). The 700wl series simply monitors the process until it detects an authentication result.

*MAC address* authentication enables an administrator to create a list of known MAC addresses and appropriate set of access rights, without further authentication. This authentication method is primarily intended for “authenticating” devices that cannot support user authentication such as access points and bar code readers.

## **Active Authentication**

The ProCurve 700wl series supports either browser-based logon or authentication through VPN clients as Active Authentication methods.

### **Browser-based Logon Authentication**

The 700wl series provides a browser-based authentication method where the user authenticates to the network through a secured browser logon page. The browser logon page is presented to an unauthenticated user the first time the user launches a browser and attempts to go to any web location.

The logon page prompts the user for credentials, which the 700wl series sends to an external database for validation. The administrator can configure the 700wl series to use an external LDAP, RADIUS, or Kerberos database for authentication. The 700wl series also provides a built-in database that can be used if an external database is not available.

Upon successful verification of the user credentials, the user’s browser is then allowed to access its original destination, assuming the destination address is permitted by the user access policy (i.e. the user’s browser home page).

If the verification of the user credentials fails, the user is presented with an incorrect username/password notification error page, and can attempt to authenticate again.

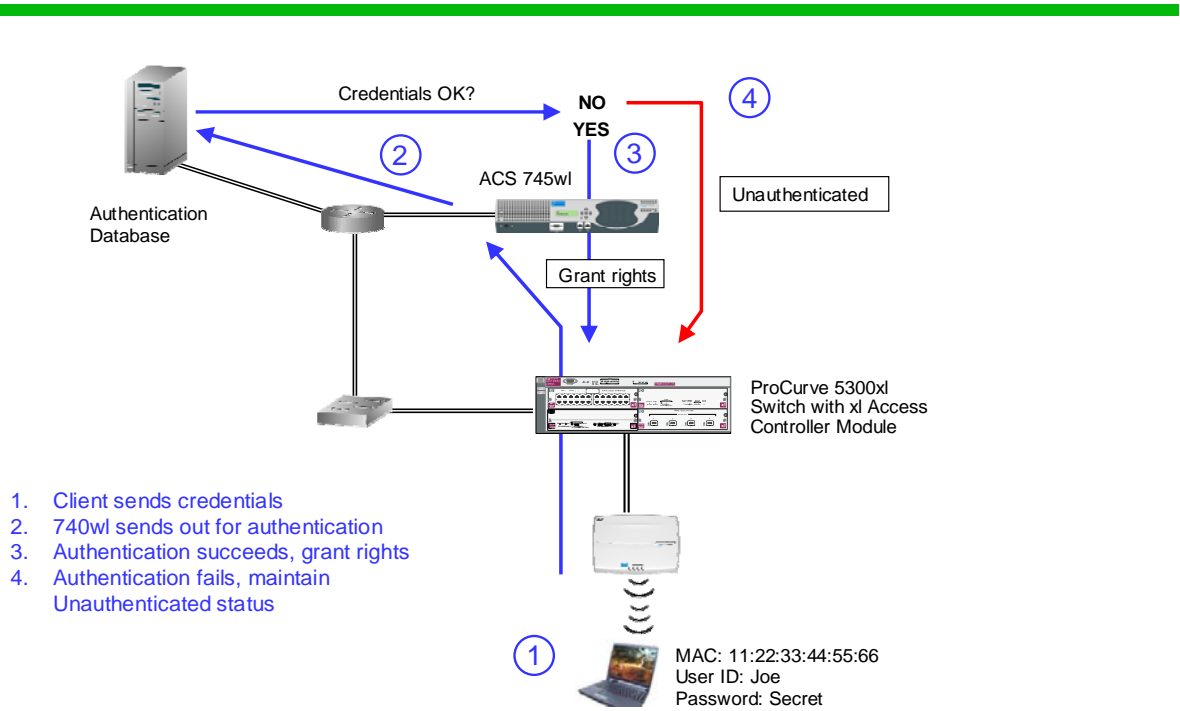


Figure 2. Active Authentication

### Authentication using a VPN client

The ProCurve 700wl series provides VPN termination services for PPTP, L2TP/IPsec, and SSH, and as a result, supports user authentication through VPN clients that are supported by those VPN termination services.

To authenticate through a VPN service, the user launches the VPN client on his wireless client and provides his or her user credentials. The 700 series then sends the user credentials to an external database in the same manner as the browser logon method.

### 802.1X / WPA Authentication using the internal RADIUS server

The ProCurve 700wl series contains an internal RADIUS server that can act as a proxy to an external RADIUS server or authenticate users directly via PEAP. If configured as the RADIUS server, 802.1X authentications using PEAP will be handled by the built-in RADIUS server. If configured as a RADIUS proxy server, all RADIUS messages will be forwarded to the remote RADIUS servers. As a proxy server, authentication requests and responses are passed through the proxy server. If the authentication is successful, whether from the built-in RADIUS server or from a remote RADIUS server, the 700wl series system evaluates the client to determine what rights should be granted. If the authentication fails, the 700wl series system will either try an authentication service specified in the Authentication Policy, or if no other services are defined, will continue to provide only logon rights.

### Passive Authentication

The 700wl series supports both 802.1X and NT Domain logon as passive authentication methods.

#### 802.1X authentication

The 700wl series can "piggy back" on an 802.1X authentication transaction between an authenticator and the authentication server, rather than actively participating in the authentication process. With 802.1X authentication, the client (supplicant) provides user credentials to an access point (authenticator) which in turn sends those credentials to a RADIUS server (authentication server) for verification.

The 700wl series can be configured to monitor the interaction between the access point and the RADIUS server to detect successful and unsuccessful authentication attempts.

With passive 802.1X authentication, the access point sends the user's credentials as well as a client identifier to the RADIUS server as part of the authentication process. For 802.1X passive

authentication with the 700wl series, the MAC address of the client is used as the client identifier. This is usually a configurable setting on an access point, and is supported by HP ProCurve wireless access points.

Upon detecting a successful 802.1X authentication between the authenticator (the access point) and the authentication server, the 700wl series will consider the user to be authenticated to the network, with the username and MAC address it detected through monitoring the authentication process.

### NT domain authentication

The ProCurve 700wl series provides a second passive authentication method which “piggy backs” on NT domain authentication transactions. This method monitors the authentication phase between a client and the NT Domain Controller, and considers the user to be authenticated to the network when it detects a successful NT domain authentication.

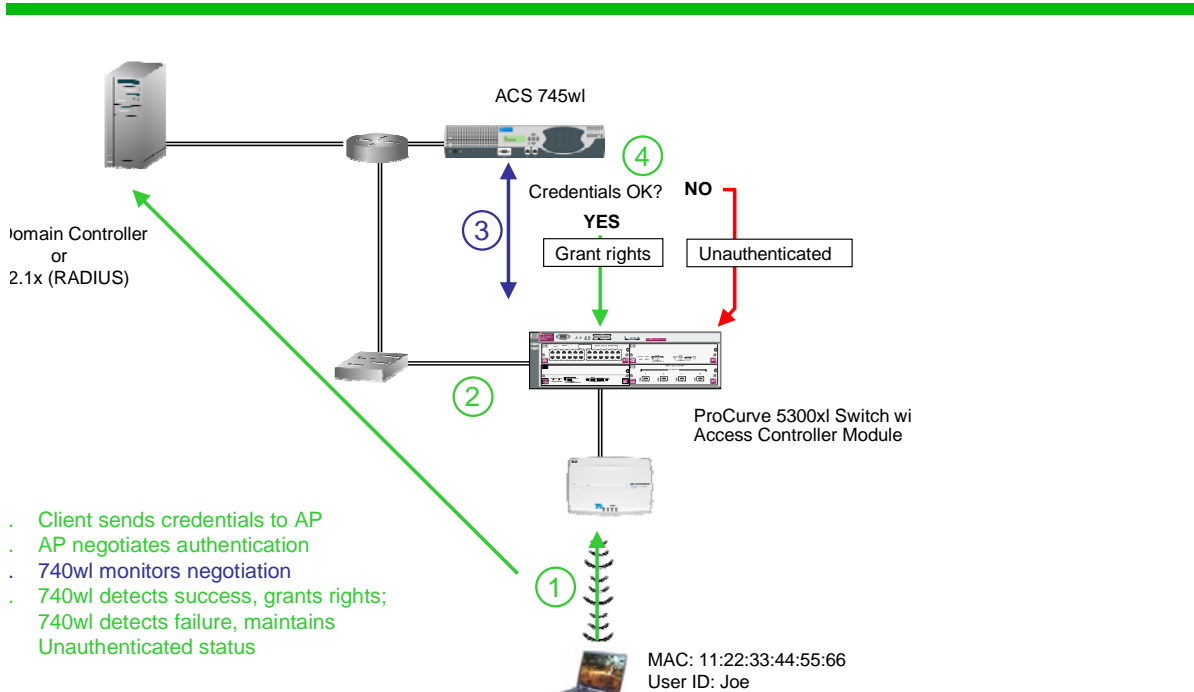


Figure 3. Passive Authentication

## Determining Access Authorization

Authentication is just the process of verifying a user’s credentials. Authorization is the mechanism for determining what access the user should get. In many cases, authorization is tied to group membership, where users’ group affiliations determine the access they are granted. For example, system administrators may belong to an “admin” group, while engineers belong to an “engineering” group.

### Getting Group Information from a Database

The ProCurve 700wl series can obtain group affiliation information for a user from an external database, if the database supports this type of information. As an example, RADIUS and LDAP databases support this type of mechanism during the authentication process.

The 700wl series can use this group information to determine what Identity Profile to assign to the user. In the 700wl series, Identity Profiles are named constructs used to group users with similar access needs, and are a significant factor in determining the Access Policy that is applied to the user. An Access Policy in turn determines what access rights a user has to network resources.

The 700wl series interacts with various database services to obtain group information as described in the following sections.

### **RADIUS**

A RADIUS database can contain attributes associated with a user. Along with the successful verification of a user's credentials, group membership information for the user can be communicated to the 700wl series by passing a group name in one of these attributes (the attribute that contains the group name is configurable). The 700wl series can then use the group name to determine the Identity Profile to use for each user.

### **LDAP**

An LDAP database can also contain attributes, much like RADIUS database. The attribute can be configured as part of the specification of the LDAP authentication service. The 700wl series uses the group name to determine the Identity Profile for the user, which in turn affects the access rights the user may be granted. With an LDAP service, the group name can be obtained along with the authentication process, or it can be obtained in an entirely separate operation (see *Retrieving Group Information Separately from Authentication* below).

### **Kerberos**

Kerberos does not support the retrieval of a group name. However, the 700wl series can be configured to authenticate the user against a Kerberos database, and then use a separate mechanism to obtain group information.

### **Retrieving Group Information Separately from Authentication**

External identity retrieval is a feature of the 700wl series that enables the retrieval of group membership information from an LDAP database as an entirely separate transaction from user authentication. This means a database such as Kerberos, that does not support group membership information, can be used for authentication, and a separate LDAP service can be used to obtain a group affiliation for authorization.

Additionally, external identity retrieval can be used with the 802.1X and NT Domain passive authentication methods.

## **How Group Information Determines an Identity Profile**

When the 700wl series gets group membership information for a user from an external authentication service, it simply searches for an Identity Profile of the same name. If it finds an exact match, the user is assigned to that Identity Profile. For example, if the group name "admin" is returned along with a user's authentication, the 700wl series will look for an Identity Profile named "admin." If an Identity Profile named "admin" exists, the user is associated with that Identity Profile.

This means that in setting up the 700wl series, Identity Profiles must match the group names that could be returned from the external database.

If no matching Identity Profile is found, the 700wl series associates the user with a predefined Identity Profile, "Authenticated," which provides a default set of access rights for authenticated users.

The following table shows which external authentication services can be used for credential validation with the various authentication methods provided by the 700wl series. For example, when a 700wl series uses a browser-based logon page to request a user's ID and password, it can be configured to use an external RADIUS, LDAP or Kerberos database to validate those credentials.

		Authentication Services					
		RADIUS	RADIUS w/RFC2548	LDAP	Kerberos	802.1X (RADIUS)	NT Domain
Authentication Methods	Browser	√	√	√	√		
	PPTP		√				
	L2TP/IPsec with PAP		√				
	L2TP/IPsec w/ MSCHAP	√	√	√	√		
	IPsec w/Browser*	√	√	√	√		
	SSH	√	√	√	√		
	802.1X					√	
	NT Domain						√

Table 1. Authentication methods and external database

\* Since IPsec alone does box-to-box authentication only to set up an encrypted tunnel, another method must be used to authenticate the user to the network. Thus, in most cases where IPsec is used alone, browser-based authentication is used to authenticate the user for network access.

Note that there are two other authentication services supported in the 700wl series that have not been discussed in this tech note.

One is the built-in database, which is the default authentication service. If no external authentication service is available, user names and passwords can be entered in the built-in database, and manually associated with Identity Profiles.

The other, the XML-RPC “service,” is not really an authentication service, but rather is a way to interface to an arbitrary authentication mechanism, for situations where authentication information is not kept in one of the common types of authentication databases. This is intended for special situations and may require significant effort to implement.

## Authentication and Authorization Examples

The following example illustrates how the ProCurve 700wl series might handle authentication within the fictional ABC Company.

When the 700wl series is installed, several pre-defined Identity Profiles are provided – among them the *Authenticated* Identity Profile, mentioned above, and a *Guest* Identity Profile.

Initially, before ABC Company sets up its own Identity Profiles, authentication works as follows:

- User Mary, an employee, connects to the system and is presented with the logon page. She enters her user ID and password. The 700wl series sends her credentials to an LDAP database, and awaits a response. A successfully authentication response comes back. Because there are no other Identity Profiles defined, and because Mary is not a guest, she matches the *Authenticated* Identity Profile. The 700wl series will now use that Identity Profile in determining Mary’s access rights.
- A visitor arrives, and hopes to access the Internet for email. He is also presented with a logon page, but selects the option “Logon as a Guest”. When the guest selects this option, the

700wl series does not attempt to authenticate this user, but simply assigns him to the *Guest* Identity Profile. Note that for security reasons, the pre-defined default *Guest* Access Policy associated with the *Guest* Identity Profile does not allow any network access. The *Guest* Access Policy must be modified to allow Internet access.

Note that by default (as configured on a new 700wl series), the Access Policy associated with the *Authenticated* Identity Profile allows unrestricted rights to IP destinations. This effectively means there is no real authorization mechanism in place in the default implementation.

To implement a level of authorization, ABC Company decides to take advantage of the group designations it has been using within its wired network. This means the network administrator must create Identity Profiles with names that match each of the groups that can be associated with various employees. When these Identity Profiles are in place, authentication/authorization works as follows:

Now when Mary logs on, and is successfully authenticated, the 700wl series also receives Mary's group affiliation along with her authentication result. The group name identifies Mary as a member of the group *Finance*. The 700wl series searches for an Identity Profile named "*Finance*." It finds one, and as a result, associates Mary with that Identity Profile. The 700wl series now uses the Identity Profile *Finance*, when determining Mary's access rights.

- A network administrator, Adam, now logs on. Along with his authentication results, the 700wl series receives the group name *Admin* as his group affiliation. The 700wl series searches for the Identity Profile *Admin*, finds it, and associates Adam with that Identity Profile. Adam will now receive a set of access rights based on the Access Policy associated with the *Admin* Identity Profile.
- Another visitor arrives, and also wants to access the Internet for email. As before, the visitor is presented with a logon page, and selects "Logon as a Guest." Again the 700wl series does not attempt to authenticate this user, but simply assigns him to the *Guest* Identity Profile. Like the previous guest, this one will get access rights based on the Access Policy associated with the *Guest* Identity Profile – since guest access functions outside the authentication system, guest access is not affected by the addition of other Identity Profiles or the use of group identity for authorization.

As mentioned earlier, the Identity Profile is not the only component the 700wl series uses to determine a user's access rights. While the user's identity and his role within the organization are the primary considerations, the determination of a user's access rights also depends on how the user connected to the network. This is discussed in detail in the 700wl Series Technical Brief "Identity Based Access Control."

In the wireless world, where multiple users appear over a single connection; users can pop up anywhere, unrestricted by building walls and locked doors; and users can roam around within the network, moving from access point-to access point, authentication of users is absolutely critical to network security. And when wireless access is added onto an existing network infrastructure, the 700wl's series' ability to integrate with the existing authentication and authorization mechanisms is a key factor in securing and controlling access to network resources based on business need.

## For more information

For more information on ProCurve Networking products and solutions, visit [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)



© 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.

5982-8267EN Revision 1, 6/2006