

**Technical brief**  
**Network Hardening: Access Control Switch Features**

---

**Table of Contents**

Introduction.....	2
DHCP Snooping .....	2
Dynamic ARP Protection.....	3
Dynamic IP Lockdown .....	4
Virus Throttle with IP Lockdown.....	5
Network Authentication and Authorization .....	5
User Authentication via 802.1X.....	7
User Authentication via Web Authentication .....	7
User authentication via MAC authentication.....	8

## Introduction

The purpose of this paper is to outline the access control security features available on ProCurve switches. Along with describing the features, some use models are offered to assist in understanding the implementation. For up-to-date product configuration information and advanced features, please view product manuals at <http://www.hp.com/rnd/support/manuals/index.htm>.

## DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) allows clients the ability to obtain IP addresses from a DHCP server. The problem that networks face is the possibility that a user could accidentally or purposely put an unauthorized DHCP server on the network. This can create a denial of service to clients by either assigning them an address outside of the IP address scheme, or by assigning duplicate addresses that have been issued by the primary DHCP server. Finding a rogue DHCP server in a large network can be a difficult task.

Many ProCurve switches are equipped with a feature that provides a solution to this problem called DHCP Snooping. This works by configuring "trusted" and "untrusted" switch ports. Trusted ports will allow DHCP Server traffic where untrusted ports will block these packets. When DHCP clients plug into untrusted ports, the DHCP Snooping database will track client IP address and MAC address mappings. This is a useful tool in troubleshooting DHCP issues.

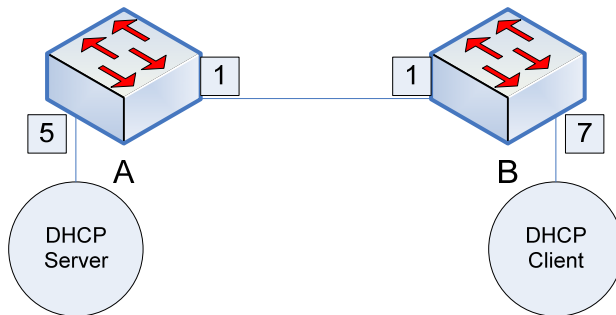
```
ProCurve Switch# show dhcp-snooping binding
```

By default, DHCP option 82 is enabled and allows the switch to track device and port details where a client is connected. The purpose of this option is to give a DHCP server the ability to assign IP addresses based on client location. Your DHCP server must support DHCP option 82 to utilize this.

All switches and vlans that are at risk to rogue dhcp servers should have DHCP Snooping enabled. It is important to note that all interconnect switch ports that have DHCP Snooping enabled should be set to "trust." Otherwise DHCP traffic between these switches will be dropped. ProCurve recommends configuring the DHCP Snooping feature on the edge of your network where rogue DHCP servers have the highest probability of being attached. The lease table size for DHCP Snooping is 8000 entries.

```
(Config)# dhcp-snooping  
(Config)# dhcp-snooping vlan 216  
(Config)# interface 1,5 dhcp-snooping trust
```

```
(Config)# dhcp-snooping  
(Config)# dhcp-snooping vlan 216  
(Config)# interface 1 dhcp-snooping trust
```

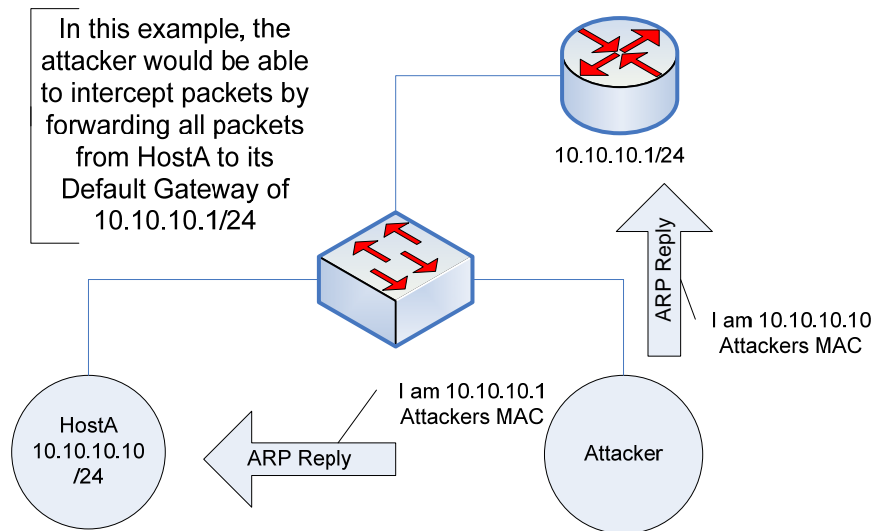


In this example, the rogue DHCP server would not be able to send DHCP Offer packets unless it was plugged into a trusted port

## Dynamic ARP Protection

The following section focuses on some concerns with the Address Resolution Protocol (ARP). It is possible for a malicious user to cause a denial of service on a device by filling up the host ARP cache with spurious MAC to IP address mappings. This is known as ARP cache poisoning and can be carried out on an IP address of a network device or an end node. Another concern is that a malicious user can use ARP to become a man-in-the-middle and intercept packets.

Both methods are possible by sending ARP Replies directly to a specific host or out to the entire network. Below is an example of a man-in-the-middle-attack with ARP Replies.



ProCurve switches counter these attacks with a feature called Dynamic ARP Protection. It works by dynamically mapping MAC addresses to IP addresses via the DHCP Snooping database. While you do not have to have DHCP Snooping configured to use Dynamic ARP Protection, it does have to be enabled on the VLAN.

This feature works by using trusted ports and untrusted ports. Trusted ports have the protection disabled. This should be used on ports that connect to other switches that have ARP protection configured on them. It is important to "trust" these interconnect switch links because each switch uses its own database for DHCP Snooping and ARP Protection. One switch would not know the learned mappings of another switch and could block their ARP packets.

Edge ports should be untrusted. If clients are not receiving their IP addresses via DHCP, then you must configure static MAC to IP mappings on the switch. When a switch port is untrusted, the host must have a mapping to send an ARP Request or an ARP Reply packet.

It is also important to note that if you choose to use ARP protection on one VLAN and not another, the switch would be vulnerable through the excluded VLAN's.

```
(Config)# arp-protect  
(Config)# arp-protect vlan <vlan>  
(eth-1)# arp-protect trust <port>  
(Config)# ip source-binding <vlan> <ip address> <mac address> <port>
```

## Dynamic IP Lockdown

Dynamic IP Lockdown is a new feature that provides IP address level port based security to protect against IP spoofing attacks. Malicious users often spoof their IP address to circumvent security controls and to avoid being tracked. This can range from applications that authenticate via

source IP address to Access Control List (ACL) that permit traffic based on source IP address.

DHCP Snooping must be enabled on any vlan that you intend to implement IP Lockdown. The IP to MAC address mappings are obtained dynamically through the DHCP Snooping database or they can be set statically as illustrated below.

```
(Config)# ip source-lockdown  
(Config)# ip source-lockdown <port-list>
```

To set the binding statically, use the following command:

```
(config)# ip source-binding <vlan> <ip> <mac> <port>
```

## Virus Throttle with IP Lockdown

Virus Throttle (VT) technology has a powerful ability to detect and respond to real-world virus and worm attacks. Developed in HP labs, VT technology is implemented through the connection-rate filtering feature in the ProCurve Switch 3500yl, 5300xl, 5400zl, 6200yl, and 8212zl series. The VT technology works by monitoring all IP connection requests and putting a rate limit on connections to new computers. A computer infected with a virus – such as the well-known “Sasser” – will attempt to infect more computers on the network, thus triggering the VT technology to respond.

It is possible for a malicious user to trigger the VT engine by using network “worm” like behavior. Enabling the IP Lockdown feature will prevent a malicious user from spoofing a legitimate host IP address, and forcing that IP address to be blocked by the network after triggering Virus Throttle. In addition to deploying IP Lockdown, VT provides an interface for “white listing” specific devices. For more information on VT, please visit the ProCurve website at [http://www.hp.com/rnd/pdfs/virus\\_throttling\\_tech\\_brief.pdf](http://www.hp.com/rnd/pdfs/virus_throttling_tech_brief.pdf)

## Network Authentication and Authorization

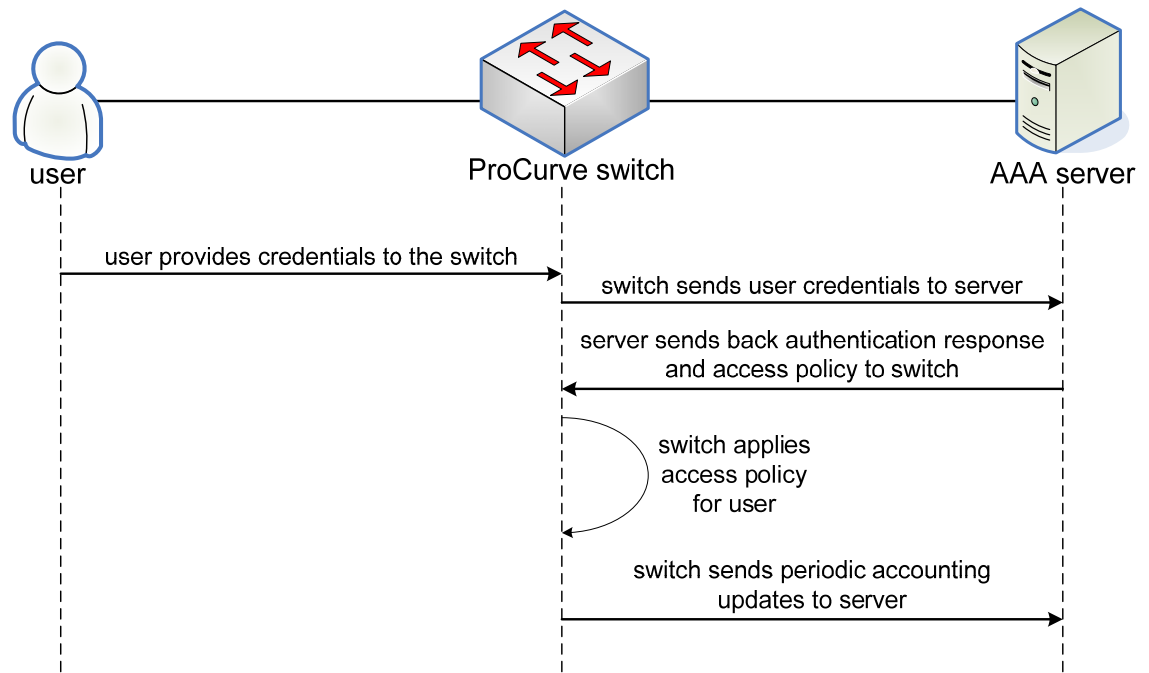
The days of relying on physical access as being a way to restrict users of coming onto the network are long over. The emergence of network connectivity has extended to conference rooms, coffee break stations, and also includes devices such as phones and printers. In the past, a user could plug their computer into one of these locations and access all network resources. Nowadays, there is greater importance and ability to restrict users from gaining access to specific resources.

One method of restricting users into a network is through user authentication. User authentication methods require that the user provide some user credentials to the switch that are then verified against a user database. The authentication process also allows the authentication server to act as an authorization authority and provide an access policy for that user. These access policies are then applied on the port that the user is connected to.

ProCurve switches offer the following policies that can be applied to users:

- VLAN – determine the network that the user will be on
- ingress rate limit – limit the rate of traffic that a user can send into the network per second
- QoS – set the priority of the user's traffic
- ACLs – restrict the user's traffic

In addition to authentication and authorization, ProCurve switches can also send accounting updates to the accounting server which contain statistics for the user. This summarizes ProCurve's Authentication, Authorization, and Accounting (AAA) services. A Remote Authentication Dial-In User Server (RADIUS) is typically used as the AAA server. Below is a sequence diagram showing the steps of this AAA process.



The configuration and monitoring of user policies can also be enhanced with ProCurve's Identity Driven Manager (IDM) product. IDM is a security plug-in to the ProCurve Manager (PCM) Plus software product. It provides a graphical interface for a network or security administrator to apply and enforce network access policies on the network. The enforcement can be based on schedule, location, or group that the user is associated with. IDM is a tool that simplifies the deployment of access control for ProCurve adaptive edge networks

ProCurve switches offers three forms of user authentication:

- 802.1X
- Web Authentication
- MAC Authentication

Each of these authentications methods are described below.

## User Authentication via 802.1X

802.1X provides clients with a method of authenticating themselves with the network. Below is the basic set of configuration commands needed to configure 802.1X on ProCurve switches:

```
(config)# aaa port-access authenticator <ports>
(config)# aaa port-access authenticator active
(config)# radius-server host <ip address> key <radius secret>
```

In order for 802.1X to work properly, every client must have an 802.1X client software (supplicant) installed on it. This piece of software passes the user credentials to the switch which is then used to authenticate them with the network. The benefit of 802.1x is that it can be used concurrently with Web authentication and MAC authentication for clients that do not have a supplicant installed.

## User Authentication via Web Authentication

Much like 802.1X, the switch will first block all unauthenticated users from accessing the network. While 802.1X requires special software on the client, web authentication provides the client with a captive portal upon the first web (HTTP or HTTPS) request that they make with a standard browser. This initial web request will be intercepted by the switch and a login page will be presented back to the user. Once the user credentials are provided to the switch, the switch performs the same user authentication request as 802.1X and gets the user attributes if their credentials are valid. Below is the basic set of configuration commands needed to enable web authentication on a ProCurve switch:

```
(config)# aaa port-access web-based <ports>
(config)# radius-server host <ip address> key <radius secret>
```

Web Authentication requires that the user open up a web browser before they can obtain network access.

## User authentication via MAC authentication

As mentioned earlier, 802.1X has a deployment issue of requiring a piece of software on all authenticating clients. Web authentication requires that all clients have a user to interact with the captive portal to provide their user credentials. Unfortunately, there are devices on the network that do not have an interactive user to authenticate nor are they capable of installing special 802.1X software. Examples of these devices are some VoIP phones, printers, and legacy servers.

In order to allow such devices onto the network and yet still provide the provisioning of access policies based on user credentials, ProCurve offers MAC authentication. MAC authentication uses the MAC address of the client as the user credentials of the device which is then sent to the authentication server.

```
(config)# aaa port-access mac-based <ports>
(config)# aaa port-access mac-based <ports> addr-format <fmt>
(config)# radius-server host <ip address> key <radius secret>
```

MAC authentication can be used concurrently with 802.1X. For example, There may be a VoIP phone that uses MAC authentication with a PC plugged into the phone using 802.1X authentication concurrently. There are two main problems with MAC authentication. First, a malicious user can spoof the MAC address of the device connected to the port. The second is maintaining many MAC addresses can be cumbersome.

## For more information

To learn more about HP ProCurve Networking, please visit [ProCurve.com](http://ProCurve.com)