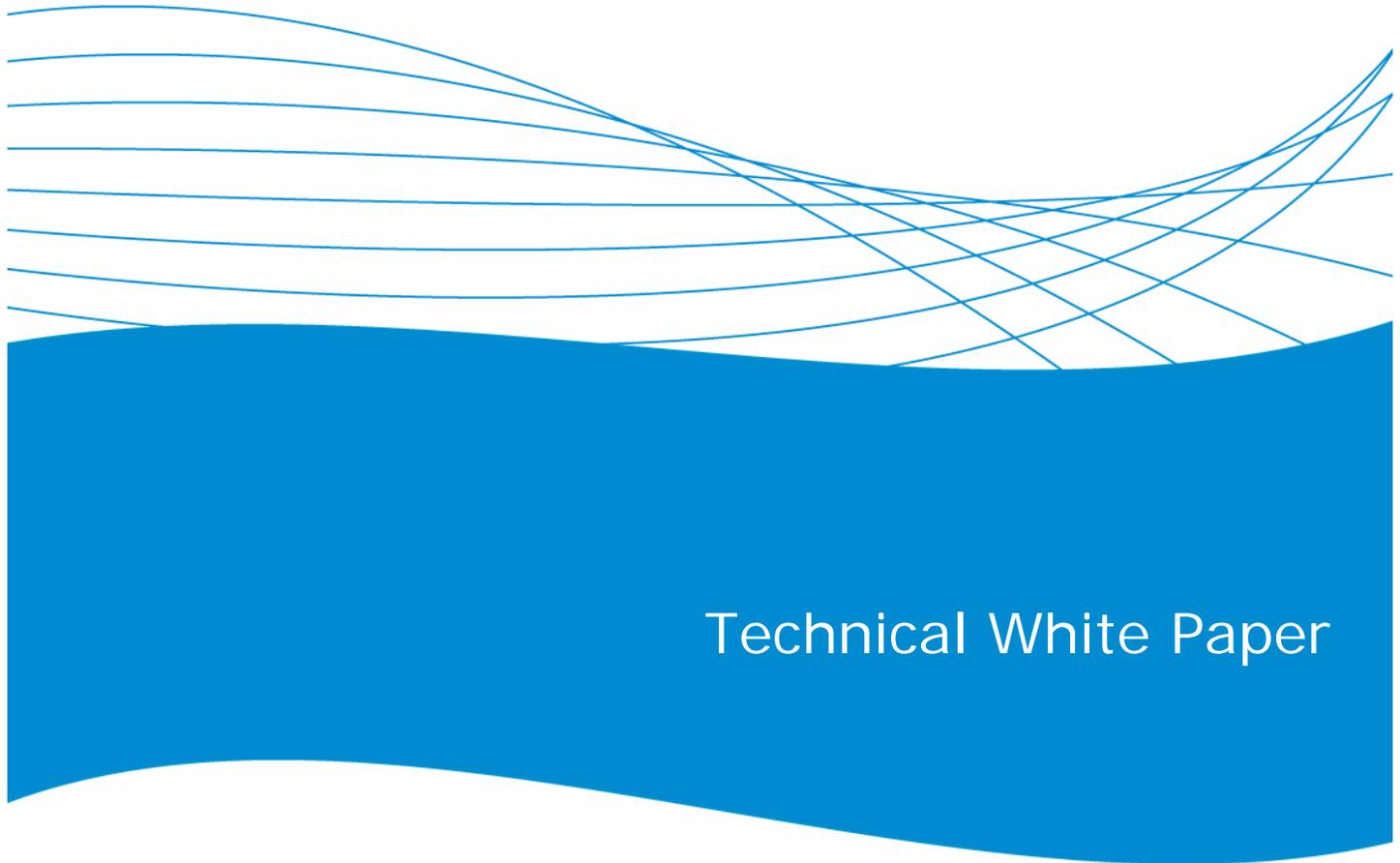


Hardening ProCurve Switches



Technical White Paper

Executive Summary and Purpose	3
Insecure Protocols and Secure Alternatives	3
Telnet vs. Secure Shell	3
HTTP vs. HTTPS	3
TFTP vs. SFTP and SCP	3
SNMPv1/2c vs. SNMPv3	4
IP Stack Management	4
Access Control	5
Secure Management VLAN.....	5
Authorized IP Managers	5
Authentication	6
Local Authentication	7
RADIUS Authentication	7
TACACS Authentication	7
Server-Supplied Privilege Level	7
Attack Prevention	8
Dynamic ARP Protection	8
Physical Security	9
Password Clear Protection – Front-Panel Security.....	9
Conclusion	9

Executive Summary and Purpose

Security is a growing concern in today's Information Technology (IT) infrastructure. Upper level managers and IT managers alike are held to a higher accountability for the integrity and availability of their data. While host clients and servers often are the focus of security discussions, securing network devices such as switches and routers should not be ignored. All data traverses these devices, and properly securing them is paramount to a stable infrastructure.

This document is intended to inform managers and administrators about insecure management protocols that run on ProCurve switches. It will also provide a guide to follow for securing these devices. For up-to-date product CLI configuration syntax and advanced features, please view product manuals at <http://www.hp.com.rnd/support/manuals/index.htm>.

Insecure Protocols and Secure Alternatives

Out of the box, ProCurve switches and routers run Telnet, Simple Network Management Protocol v1/2c (SNMP v1/2c), Trivial File Transfer Protocol (TFTP) and Hypertext Transfer Protocol (HTTP) for device management purposes. These protocols are supported out of the box because they provide an ease of use that customers expect from the ProCurve Networking by HP product line. For the sake of securing these devices, these protocols should be disabled.

Telnet vs. Secure Shell

Telnet is insecure by nature as it sends all traffic across the wire in clear text. This includes user names and passwords. Anyone snooping or sniffing network traffic will be able to see these passwords. It is recommended that you use Secure Shell (SSH) instead of Telnet. SSH uses asymmetric authentication to exchange keys and create a secure encrypted session. Follow these steps to enable SSH and disable Telnet:

```
ProCurve Switch(config)# crypto key generate ssh

ProCurve Switch(config)# ip ssh

ProCurve Switch(config)# no telnet-server
```

HTTP vs. HTTPS

ProCurve switches and routers can be configured through the HTTP interface. The HTTP interface that is started by default has the same limitations as Telnet. It is recommended that the HTTPS interface be configured and the HTTP interface be disabled. HTTPS is HTTP traffic running over a Secure Sockets Layer (SSL).

```
ProCurve Switch(config)# crypto key generate cert <key_size>

ProCurve Switch(config)# web-management ssl

ProCurve Switch(config)# no web-management plaintext
```

TFTP vs. SFTP and SCP

TFTP client and server should be disabled as they do not require any authentication. Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP) are part of the SSH protocol suite. They provide an encrypted session using public/private keys between client and server just like SSH. In this case, the switch would be the server, and your PC would be the client. Please note that you will need a secure terminal client program running on your PC.

```
ProCurve Switch(config)# crypto key generate ssh

ProCurve Switch(config)# ip ssh filetransfer

ProCurve Switch(config)# no tftp server

ProCurve Switch(config)# no tftp client
```

When executing "ip ssh filetransfer", the TFTP client and server will be disabled automatically. To disable the TFTP client and server manually, execute the following commands:

```
ProCurve Switch(config)# no tftp server
```

```
ProCurve Switch(config)# no tftp client
```

SNMPv1/2c vs. SNMPv3

SNMP version 2 is enabled by default. This protocol is used to manage switches and routers from a central management server such as ProCurve Manager (PCM). SNMPv2 uses community names for read and write access, much like passwords are used for authentication. These community names are sent across the wire as clear text. If a malicious user were to capture these community names, they could issue SNMP set commands to reconfigure your network device.

SNMP version 3 was developed to overcome these weaknesses. It uses asymmetric cryptography to encrypt SNMP traffic over the wire.

```
ProCurve Switch(config)# snmpv3 enable
```

```
ProCurve Switch(config)# snmpv3 only
```

For additional configuration examples for SNMPv3, please reference the product manual. It is important to consider user names, groups and privileges when configuring SNMPv3. Further considerations should include encryption settings.

If for any reason SNMPv3 is not an option for your network, you can enable SNMPv2 in restricted mode. This will allow management devices to "get" information from a networking device, but not "set" or change any settings on the networking device.

```
ProCurve Switch(config)# snmp-server community <community_name> restricted
```

Some security policies may mandate that SNMP be disabled altogether.

```
ProCurve Switch(config)# no snmp-server enable
```

IP Stack Management

IP Stack Management allows ProCurve stackable devices to be managed as a group using only a single IP address. There are a number of advantages, though they are more related to ease of use than security. For those who choose not to deploy IP Stack Management, it is advisable to disable the feature to prevent potential hijacking of the switch.

To determine whether the stacking protocol is enabled, execute the command:

```
ProCurve Switch(config)# show stack
```

Once it's determined that the IP Stack Management is enabled, it only requires one command to disable:

```
ProCurve Switch(config)# no stack
```

Once the IP Stack Management protocol is disabled, the switch cannot become a Commander or a Member.

See the ProCurve Advanced Traffic Management Guide for more information on IP Stack Management and a list of devices on which it is supported.

Access Control

Secure Management VLAN

Secure Management VLANs are designed to restrict management access to the switch to only those nodes connected to the Management VLAN. That is, only clients who are connected to ports who are members of the Secure Management VLAN can be allowed to gain management access to the ProCurve device. This sharply limits the universe of devices that can attempt unauthorized access.

Configuring a Management VLAN takes only one command:

```
ProCurve Switch(config)# management-vlan <vid | vlan-name>
```

Any VLAN can be assigned as the management VLAN. Take care to ensure that the same VLAN is configured as Management VLAN on all ProCurve switches that are to be members of the management VLAN.

There are a few restrictions on Secure Management VLANs worth noting:

- Only one VLAN per switch can be identified as the Secure Management VLAN.
- IP addresses must be assigned manually to the Secure Management VLAN. The switch will not allow the Management VLAN to acquire its address through DHCP/Bootp.
- To maintain the secure nature of the management VLAN, only ProCurve switch ports that are connecting authorized management stations, or those extending the management VLAN to other ProCurve switches, should be members of the Management VLAN.
- Internet Group Management Protocol (IGMP) is not supported on the Management VLAN.
- Routing to or from the Secure Management VLAN is not permitted. Routing can be enabled on the switch and all other VLANs will be routable, but the Secure Management VLAN will remain isolated.

For more information on the Secure Management VLAN see the “Advanced Traffic Management Guide” manual for your product at the ProCurve Networking Web site, (<http://www.hp.com/rnd/support/manuals/index.htm>).

Authorized IP Managers

In cases where configuring a Secure Management VLAN is too restrictive, it's possible to identify up to 10 IP addresses or address groups that are allowed management access to the switch via the network. The command to configure the management stations is as follows:

```
ProCurve Switch(config)# ip authorized-manager <IP address> mask <mask bits> <operator | manager>
```

Once configured, only those addresses identified will be granted access to the switch over the network. The addresses are configured using a mask to allow the 10 entries to be either a single host (using a mask of 255.255.255.255) or groups of hosts. Note that the access level is also configurable. Some addresses can be limited to operator access while others are granted full manager status.

It's important to keep in mind that this is not fool-proof access control. IP spoofing will defeat this protection, as will an authorized workstation whose security has been compromised. It also does not protect against unauthorized access through the serial console. It's recommended that this feature be used in conjunction with a secondary authentication scheme, such as password protection.

Consider the following standard ACL:

```
ip access-list standard "mgmt-traffic"  
10 permit 10.1.1.0 0.0.0.255  
20 permit 10.1.0.50 0.0.0.0  
exit
```

This list, when applied inbound on the VLAN or port on which the management interface resides, will allow only hosts from 10.1.1.0/24 or 10.1.0.50 to access the switch. All traffic from other source IP addresses is dropped.

Note that all ACLs have an implicit “deny any” at the bottom. Traffic must be permitted explicitly in order to pass through an applied ACL.

ACL options and configuration can vary by switch platform. For more information on Access Control Lists, see the “Advanced Traffic Management Guide” manual for your product at the ProCurve Networking website, <http://www.hp.com/rnd/support/manuals/index.htm>.

Authentication

By default, no user authentication is configured, thus leaving the switch open to anyone with physical or remote access. Two types of users can be configured to provide different levels of access to the switch.

- Manager – full access (default)
 - Ability to make configuration changes
 - All “enable” command contexts
 - Read and write access
- Operator – limited access
 - Status and counters, event-log and show commands
 - All “login” command contexts
 - Read-only access

Each access method (console, Telnet, etc.) allows you to configure a primary and secondary way of authenticating users. ProCurve switches default to the following:

```
ProCurve Switch# show authentication

Status and Counters - Authentication Information

Login Attempts: 3

Respect Privilege: Disabled

          | Login      Login      Enable      Enable
Access Task | Primary    Secondary  Primary    Secondary
-----+-----+-----+-----+-----
Console    | Local      None       Local      None
Telnet     | Local      None       Local      None
Port-Access | Local
Webui      | Local      None       Local      None
SSH        | Local      None       Local      None
Web-Auth   | ChapRadius
MAC-Auth   | ChapRadius
```

Note: Port-access (802.1x), Web-Auth and MAC-Auth are means of securing the network from unauthorized users, not the switch itself, and therefore are not covered in the scope of this document.

The default number of login attempts is “3,” meaning the user has three chances to successfully supply access credentials. Once this limit is reached the user must re-initiate a login. The

number of login attempts allowed can be changed by entering the configuration context and using the following command:

```
ProCurve Switch 5406zl(config)# aaa authentication num-attempts <1-10>
```

The “Respect Privilege” option instructs the switch to allow the authenticating server to supply the privilege level of the user. See the “Server-Supplied Privilege Level” section below for more information.

If the primary authentication method fails for any reason, (e.g., the authenticating server(s) are unreachable), the secondary method will be used to authenticate users. In the above configuration, when no “Local” username/passwords are configured everyone has manager permission.

Most access methods allow three methods of authenticating users:

- Local – uses the switch’s locally stored usernames and passwords
- RADIUS – uses a RADIUS server to authenticate users
- TACACS+ – uses a TACACS server to authenticate users

Local Authentication

Local username and passwords are configured on a per-switch basis and provide the most basic form of authentication. The switch allows you to configure manager and operator passwords, as well as an optional username for each. Local authentication is often used as the secondary login method so as to provide a minimum level of security should the primary method fail.

RADIUS Authentication

Authenticating users via RADIUS provides a centralized way to manage access to the switch. This allows the administrator to make modifications to the set of authorized users without having to make changes on every network device.

To enable RADIUS authentication as the primary method, and Local as the secondary method, use the following configuration command:

```
ProCurve Switch (config)# aaa authentication <console|telnet|ssh|web>  
<enable|login> radius local
```

SSH also includes authentication for SCP and SFTP.

Note: If the secondary access method is “None” or “Local” with no passwords configured, the user will be granted manager-level access if the primary method fails for any reason.

TACACS Authentication

Authenticating users via TACACS also provides a centralized way to manage access to the switch. TACACS authentication works along the same lines as a RADIUS authentication, allowing the administrator to manage users from a central server.

To enable TACACS authentication as the primary method, and Local as the secondary method, use the following configuration command:

```
ProCurve Switch (config)# aaa authentication <console|telnet|ssh|web>  
<enable|login> tacacs local
```

Note on RADIUS and TACACS keys: When copying off a switch configuration, certain security parameters, including the RADIUS and TACACS keys, are not included in the copied configuration. If this configuration is then used to restore a device configuration, it will not include this information, possibly resulting in a user being denied access due to a mismatched password that is no longer encrypted.

For more information on configuring Local passwords, RADIUS, or TACACS servers see the “Access Security Guide” manual for your product at the ProCurve Networking website, (<http://www.hp.com/rnd/support/manuals/index.htm>).

Server-Supplied Privilege Level

Login privilege level instructs the switch to accept the authenticating user’s command level (manager or operator) that is supplied by the server. This allows manager-level users to skip

the login context and proceed immediately to enable context, thus eliminating the need for a manager-level user to login twice.

To allow the switch to accept the privilege level provided by the server, use the following configuration command:

```
ProCurve Switch(config)# aaa authentication login privilege-mode
```

To supply a privilege level via RADIUS, specify the "Service-Type" attribute in the user's credentials.

- Service-Type = 6 allows manager-level access
- Service-Type = 7 allows operator-level access
- A user with Service-Type not equal to 6 or 7 is denied access
- A user with no Service-Type attribute supplied is denied access when privilege mode is enabled

To supply a privilege level via TACACS specify the "Max Privilege" level in the user's credentials.

- Max-privilege = 15 allows manager-level access
- Max-privilege = 14 allows operator-level access
- A user with Max-Privilege of 14 or lower is granted operator-level access

Attack Prevention

Dynamic ARP Protection

Address Resolution Protocol (ARP) allows hosts to communicate over the network by creating an IP to MAC address mapping used in the transmission of packets. Attackers can use ARP to generate bogus mappings, thereby allowing them to spoof other clients' MAC addresses and intercept traffic destined to them. Additionally, an attacker could generate an unlimited number of artificial ARP entries, filling up the caches of other clients on the network and creating a Denial of Service.

Dynamic ARP Protection works by intercepting ARP packets and verifying their authenticity before forwarding them. Packets with invalid IP to MAC address bindings advertised in the source protocol address and source physical address fields are discarded, ensuring that only valid ARP requests and replies are forwarded or used to update the local ARP table.

ARP Protection authenticates IP to MAC bindings stored from a lease maintained by DHCP Snooping, or by using static bindings configured for non-DHCP clients. It is configured per VLAN and categorizes ports in two ways, trusted and untrusted (default). ARP packets received on trusted ports are forwarded normally without validating their authenticity, provided no authorized servers are configured.

Note: Enabling ARP protection without first configuring DHCP Snooping and/or static bindings will cause all ARP packets to be dropped.

ARP Protection also can be configured to drop:

- ARP request or response packets, where the source MAC address in the Ethernet header does not match the sender MAC address in the body of the ARP packet.
- Unicast ARP response packets, where the destination MAC address in the Ethernet header does not match the target MAC address in the body of the ARP packet.
- ARP packets, where the sender or target IP address is invalid. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all Class E IP addresses.

For more information on configuring Dynamic ARP Protection or DHCP Snooping, see the "Access Security Guide" manual for your product at the ProCurve Networking website, <http://www.hp.com/rnd/support/manuals/index.htm>.

Physical Security

Password Clear Protection – Front-Panel Security

ProCurve devices utilize the Reset and Clear buttons on the front panel to help users reset the switch configuration to factory default or to reset the console password. This capability creates a security risk anywhere it's impossible to prevent physical access to the switch. ProCurve makes it possible to disable this functionality to protect from malicious use of these features.

There are two components to front-panel security: "password clear" and "factory reset." Both must be disabled to fully secure the device.

In the switch's default mode, a malicious user can utilize the front-panel clear button to reset a console password stored locally on the switch. To disable this feature, issue the command:

```
ProCurve Switch(config)# no front-panel-security password-clear
```

The other capability built into ProCurve switches is the ability to reset the switch configuration to the factory default mode:

```
ProCurve Switch(config)# [no] front-panel-security factory-reset
```

Executing this command prevents reset of the switch configuration by use of the front-panel Reset and Clear buttons.

It's critical to understand that disabling these features severely restricts administrator options if the password is lost or forgotten. Before making these changes, users are strongly encouraged to review all considerations outlined in the Access and Security Guide for your model.

Conclusion

The security features described by this white paper are an excellent starting point for hardening ProCurve networks, and should be used in the context of an organization's greater security policy. Good security practice dictates that an organization have a well-thought security policy that relies on a thorough threat assessment and defense-in-depth strategy. Only after creating a security policy can an organization best capitalize on the many security features present in ProCurve devices, such as MAC lockdown, DHCP protection, BPDU Port Protection and Dynamic IP Lockdown.

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.

4AA1-0313ENW, 02/2007