

# Configuring and Monitoring Port Security

---

## Contents

<b>Overview</b> .....	10-3
<b>Port Security</b> .....	10-4
Basic Operation .....	10-4
Eavesdrop Protection .....	10-5
Blocking Unauthorized Traffic .....	10-5
Trunk Group Exclusion .....	10-6
Planning Port Security .....	10-7
Port Security Command Options and Operation .....	10-8
Port Security Display Options .....	10-8
Configuring Port Security .....	10-12
Retention of Static Addresses .....	10-16
<b>MAC Lockdown</b> .....	10-22
Differences Between MAC Lockdown and Port Security .....	10-23
MAC Lockdown Operating Notes .....	10-24
Deploying MAC Lockdown .....	10-25
<b>MAC Lockout</b> .....	10-29
Port Security and MAC Lockout .....	10-31
<b>Web: Displaying and Configuring Port Security Features</b> .....	10-32
<b>Reading Intrusion Alerts and Resetting Alert Flags</b> .....	10-32
Notice of Security Violations .....	10-32
How the Intrusion Log Operates .....	10-33
Keeping the Intrusion Log Current by Resetting Alert Flags .....	10-34
Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags .....	10-35
CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags .....	10-36
Using the Event Log To Find Intrusion Alerts .....	10-38

**Configuring and Monitoring Port Security**  
**Contents**

Web: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags . . . . . 10-39

**Operating Notes for Port Security . . . . . 10-40**

## Overview

Feature	Default	Menu	CLI	Web
Displaying Current Port Security	n/a	—	page 10-8	page 10-32
Configuring Port Security	disabled	—	page 10-12	page 10-32
Retention of Static Addresses	n/a	—	page 10-16	n/a
MAC Lockdown	disabled	—	page 10-22	
MAC Lockout	disabled	—	page 10-29	
Intrusion Alerts and Alert Flags	n/a	page 10-38	page 10-36	page 10-39

**Port Security (Page 10-4).** This feature enables you to configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

### Note

This feature does not prevent intruders from receiving broadcast and multi-cast traffic. Also, Port Security and MAC Lockdown are mutually exclusive on a switch. If one is enabled, then the other cannot be used.

**MAC Lockdown (Page 10-22).** This feature, also known as “Static Addressing”, is used to prevent station movement and MAC address “hijacking” by allowing a given MAC address to use only an assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN. (See also the **Note**, above.)

**MAC Lockout (Page 10-29).** This feature enables you to block a specific MAC address so that the switch drops all traffic to or from the specified address.

# Port Security

## Basic Operation

**Default Port Security Operation.** The default port security setting for each port is off, or “continuous”. That is, any device can access a port without causing a security reaction.

**Intruder Protection.** A port that detects an “intruder” blocks the intruding device from transmitting to the network through that port.

**Eavesdrop Protection.** Using either the port-security command or the switch’s web browser interface to enable port security on a given port automatically enables eavesdrop prevention on that port.

**General Operation for Port Security.** On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once port security is configured, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as ProCurve Manager (PCM and PCM+)
- Alert Log entries in the switch’s web browser interface
- Event Log entries in the console interface
- Intrusion Log entries in the menu interface, CLI, or web browser interface

For any port, you can configure the following:

- **Action:** Used when a port detects an intruder. Specifies whether to send an SNMP trap to a network management station and whether to disable the port.
- **Address Limit:** Sets the number of authorized MAC addresses allowed on the port.
- **Learn-Mode:** Specify how the port acquires authorized addresses.
  - **Continuous:** Allows the port to learn addresses from inbound traffic from any connected device. This is the default setting.
  - **Limited-Continuous:** Sets a finite limit (1 - 32) to the number of learned addresses allowed per port.

- **Static:** Enables you to set a fixed limit on the number of MAC addresses authorized for the port and to specify some or all of the authorized addresses. (If you specify only some of the authorized addresses, the port learns the remaining authorized addresses from the traffic it receives from connected devices.)
- **Configured:** Requires that you specify all MAC addresses authorized for the port. The port is not allowed to learn addresses from inbound traffic.
- **Authorized (MAC) Addresses:** Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
  - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
  - Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port. (For more on configuring the switch for SNMP management, see “Trap Receivers and Authentication Traps” in the *Management and Configuration Guide* for your switch.)
- **Port Access:** Allows only the MAC address of a device authenticated through the switch’s 802.1X Port-Based access control. Refer to chapter 9, Configuring Port-Based and User-Based Access Control (802.1X).

For configuration details, refer to “Configuring Port Security” on page 10-12.

## Eavesdrop Protection

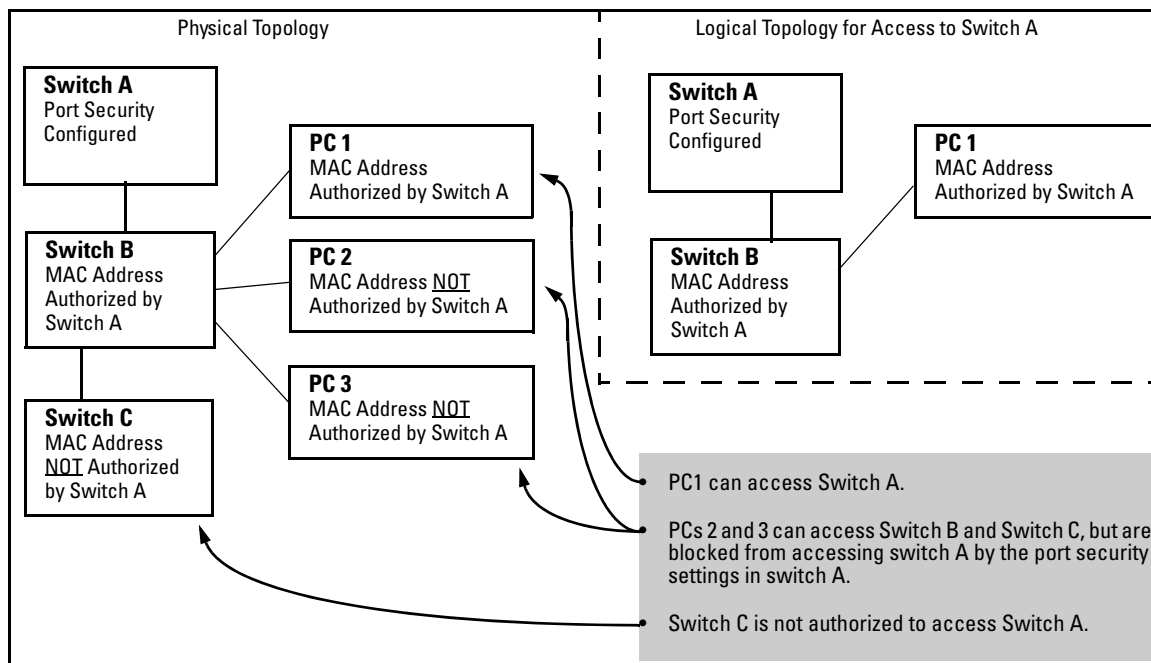
Configuring port security on a given switch port automatically enables eavesdrop protection for that port. This prevents use of the port to flood unicast packets addressed to MAC addresses unknown to the switch. This blocks unauthorized users from eavesdropping on traffic intended for addresses that have aged-out of the switch’s address table. (Eavesdrop prevention does not affect multicast and broadcast traffic, meaning that the switch floods these two traffic types out a given port regardless of whether port security is enabled on that port.)

## Blocking Unauthorized Traffic

Unless you configure the switch to disable a port on which a security violation is detected, the switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security

## Configuring and Monitoring Port Security Port Security

configuration to ports on which hubs, switches, or other devices are connected, and to maintain security while also maintaining network access to authorized users. For example:



**Figure 10-1. Example of How Port Security Controls Access**

### Note

Broadcast and Multicast traffic is always allowed, and can be read by intruders connected to a port on which you have configured port security.

## Trunk Group Exclusion

Port security does not operate on either a static or dynamic trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch will reset the port security parameters for those ports to the factory-default configuration. (Ports configured for either Active or Passive LACP, and which are not members of a trunk, can be configured for port security.)

## Planning Port Security

1. Plan your port security configuration and monitoring according to the following:
  - a. On which ports do you want port security?
  - b. Which devices (MAC addresses) are authorized on each port?
  - c. For each port, what security actions do you want? (The switch automatically blocks intruders detected on that port from transmitting to the network.) You can configure the switch to (1) send intrusion alarms to an SNMP management station and to (2) optionally disable the port on which the intrusion was detected.
  - d. How do you want to learn of the security violation attempts the switch detects? You can use one or more of these methods:
    - Through network management (That is, do you want an SNMP trap sent to a net management station when a port detects a security violation attempt?)
    - Through the switch's Intrusion Log, available through the CLI, menu, and web browser interface
    - Through the Event Log (in the menu interface or through the CLI **show log** command)
2. Use the CLI or web browser interface to configure port security operating and address controls. The following table describes the parameters.

## Port Security Command Options and Operation

### Port Security Commands Used in This Section

---

show port-security	10-9
show mac-address	
port-security	10-12
< <i>port-list</i> >	10-12
learn-mode	10-12
address-limit	10-15
mac-address	10-15
action	10-16
clear-intrusion-flag	10-16
no port-security	10-16

---

This section describes the CLI port security command and how the switch acquires and maintains authorized addresses.

---

#### Note

---

Use the global configuration level to execute port-security configuration commands.

### Port Security Display Options

You can use the CLI to display the current port-security settings and to list the currently authorized MAC addresses the switch detects on one or more ports.

### Displaying Port Security Settings.

**Syntax:** show port-security  
 show port-security <port number>  
 show port-security [<port number>-<port number>]. . [<port number>]

*The CLI uses the same command to provide two types of port security listings:*

- *All ports on the switch with their Learn Mode and (alarm) Action*
- *Only the specified ports with their Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses*

*Without port parameters, **show port-security** displays Operating Control settings for all ports on a switch.*

```
ProCurve(config)# show port-security
Port Security
Port Learn Mode | Action
-----+-----
A1 1 Static | Send Alarm, Disable Port
A2 2 Static | Send Alarm, Disable Port
A3 3 Static | Send Alarm
A4 4 Static | Send Alarm
A5 5 Static | Send Alarm
A6 6 Static | Send Alarm
A7 7 Continuous | None
A8 8 Continuous | None
```

**Figure 10-2. Example Port Security Listing (Ports A7 and A8 Show the Default Setting)**

With port numbers included in the command, **show port-security** displays Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses for the specified ports on a switch. The following example lists the full port security configuration for a single port:

```
ProCurve(config)# show port-security A3
Port Security
  Port : A3
  Learn Mode : Static           Address Limit : 1
  Action : Send Alarm

  Authorized Addresses
  -----
  00906d-fdcc00
```

**Figure 10-3. Example of the Port Security Configuration Display for a Single Port**

The next example shows the option for entering a range of ports, including a series of non-contiguous ports. Note that no spaces are allowed in the port number portion of the command string:

```
ProCurve(config)# show port-security A1-A3,A6,A8
```

#### **Listing Authorized and Detected MAC Addresses.**

**Syntax:** show mac-address [ *port-list* | *mac-address* | vlan < vid > ]

*Without an optional parameter, show mac-address lists the authorized MAC addresses that the switch detects on all ports.*

**mac-address:** *Lists the specified MAC address with the port on which it is detected as an authorized address.*

**port list:** *Lists the authorized MAC addresses detected on the specified port(s).*

**vlan < vid >:** *Lists the authorized MAC addresses detected on ports belonging to the specified VLAN.*

```
ProCurve(config)# show mac-address

Status and Counters - Port Address Table

MAC Address   Located on Port
-----
0004ea-84d980 7
0004ea-84d9ee 7
000a57-4d8d40 5
      :
      :
00a0c9-f1786f 5

ProCurve(config)# show mac-address 7

Status and Counters - Port Address Table - 7

MAC Address
-----
0004ea-84d980
0004ea-84d9ee

ProCurve(config)# show mac-address 000a57-4d8d40

Status and Counters - Address Table - 000a57-4d8d40

MAC Address : 000a57-4d8d40
Located on Port : 5

ProCurve(config)# show mac-address vlan 1

Status and Counters - Address Table - VLAN 1

MAC Address   Located on Port
-----
0004ea-84d980 7
0004ea-84d9ee 7
000a57-4d8d40 5
      :
      :
00a0c9-f1786f 5
```

Figure 10-4. Examples of Show Mac-Address Outputs

## Configuring Port Security

Using the CLI, you can:

- Configure port security and edit security settings.
- Add or delete devices from the list of authorized addresses for one or more ports.
- Clear the Intrusion flag on specific ports

**Syntax:** port-security

```
[e] <port-list>< learn-mode | address-limit | mac-address | action |  
clear-intrusion-flag >
```

**< port-list >:** Specifies a list of one or more ports to which the port-security command applies.

```
learn-mode < continuous | static | port-access | configured | limited-  
continuous >
```

*For the specified port:*

- Identifies the method for acquiring authorized addresses.
- On switches covered in this guide, automatically invokes eavesdrop protection. (Refer to “Eavesdrop Protection” on page 10-5.)

**continuous** (Default): Appears in the factory-default setting or when you execute **no port-security**. Allows the port to learn addresses from the device(s) to which it is connected. In this state, the port accepts traffic from any device(s) to which it is connected. Addresses learned in the learn continuous mode will “age out” and be automatically deleted if they are not used regularly. The default age time is five minutes.

Addresses learned this way appear in the switch and port address tables and age out according to the **MAC Age Interval** in the System Information configuration screen of the Menu interface or the **show system-information** listing. You can set the MAC age out time using the CLI, SNMP, Web, or menu interfaces. For more information on the **mac-age-time** command refer to the chapter titled “Interface Access and System Information” in the Management and Configuration Guide for your switch.

— Continued —

**Syntax:** port-security (*Continued*)

learn-mode < continuous | static | port-access | configured | limited-continuous > (*Continued*)

**static:** *Enables you to use the **mac-address** parameter to specify the MAC addresses of the devices authorized for a port, and the **address-limit** parameter (explained below) to specify the number of MAC addresses authorized for the port. You can authorize specific devices for the port, while still allowing the port to accept other, non-specified devices until the device limit has been reached. That is, if you enter fewer MAC addresses than you authorized, the port authorizes the remaining addresses in the order in which it automatically learns them.*

*For example, if you use **address-limit** to specify three authorized devices, but use **mac-address** to specify only one authorized MAC address, the port adds the one specifically authorized MAC address to its authorized-devices list and the first two additional MAC addresses it detects.*

*If, for example:*

*You use **mac-address** to authorize MAC address 0060b0-880a80 for port A4.*

*You use **address-limit** to allow three devices on port A4 and the port detects these MAC addresses:*

- 1. 080090-1362f2*
- 2. 00f031-423fc1*
- 3. 080071-0c45a1*
- 4. 0060b0-880a80 (the address you authorized with the **mac-address** parameter)*

*In this example port A4 would assume the following list of authorized addresses:*

*080090-1362f2 (the first address the port detected)*

*00f031-423fc1 (the second address the port detected)*

*0060b0-880a80 (the address you authorized with the **mac-address** parameter)*

*The remaining MAC address detected by the port, 080071-0c45a1, is not allowed and is handled as an intruder. Learned addresses that become authorized do **not** age-out. See also “Retention of Static Addresses” on page 10-16.*

*— Continued —*

**Syntax:** port-security (*Continued*)

learn-mode < continuous | static | port-access | configured | limited-continuous > (*Continued*)

**Caution:** Using the **static** parameter with a device limit greater than the number of MAC addresses specified with **mac-address** can allow an unwanted device to become “authorized”. This is because the port, to fulfill the number of devices allowed by the **address-limit** parameter (see below), automatically adds devices it detects until it reaches the specified limit.

**Note:** If 802.1X port-access is configured on a given port, then port-security learn-mode must be set to either **continuous** (the default) or **port-access**.

**port-access:** Enables you to use Port Security with (802.1X) Port-Based Access Control. Refer to chapter 9, *Configuring Port-Based and User-Based Access Control (802.1X)*.

**configured:** Must specify which MAC addresses are allowed for this port. Range is 1 (default) to 8 and addresses are not ageable. Addresses are saved across reboots.

**limited-continuous:** Also known as MAC Secure, or “limited” mode. The limited parameter sets a finite limit to the number of learned addresses allowed per port. (You can set the range from 1, the default, to a maximum of 32 MAC addresses which may be learned by each port.)

All addresses are ageable, meaning they are automatically removed from the authorized address list for that port after a certain amount of time. Limited mode and the address limit are saved across reboots, but addresses which had been learned are lost during the reboot process. Addresses learned in the limited mode are normal addresses learned from the network until the limit is reached, but they are not configurable. (You cannot enter or remove these addresses manually if you are using **learn-mode** with the **limited-continuous** option.)

—Continued—

**Syntax:** port-security (*Continued*)

Addresses learned this way appear in the switch and port address tables and age out according to the **MAC Age Interval** in the System Information configuration screen of the Menu interface or the **show system-information** listing. You can set the MAC age out time using the CLI, SNMP, Web, or menu interfaces. For more on the **mac-age-time** command, refer to the chapter titled “Interface Access and System Information” in the Management and Configuration Guide for your switch. To set the learn-mode to **limited** use this command syntax:

```
port-security <port-list> learn-mode limited address-limit < 1..32 >
action < none | send-alarm | send-disable >
```

The default address-limit is **1** but may be set for each port to learn up to 32 addresses. The default action is **none**. To see the list of learned addresses for a port use the command:

```
address-limit < integer >
```

When **learn-mode** is set to **static**, **configured**, or **limited-continuous**, the **address-limit** parameter specifies how many authorized devices (MAC addresses) to allow. Range: 1 (the default) to 8 for static and configured modes. For **learn-mode** with the **limited-continuous** option, the range is 1-32 addresses.

```
mac-address [<mac-addr>] [<mac-addr>] . . . [<mac-addr>]
```

Available for **learn-mode** with the, **static**, **configured**, or **limited-continuous** option. Allows up to eight authorized devices (MAC addresses) per port, depending on the value specified in the **address-limit** parameter. The **mac-address limited-continuous** mode allows up to 32 authorized MAC addresses per port.

If you use **mac-address** with **static**, but enter fewer devices than you specified in the **address-limit** field, the port accepts not only your specified devices, but also as many other devices as it takes to reach the device limit. For example, if you specify four devices, but enter only two MAC addresses, the port will accept the first two non-specified devices it detects, along with the two specifically authorized devices. Learned addresses that become authorized do **not** age-out. See also “Retention of Static Addresses” on page 10-16.

---

action < none | send-alarm | send-disable >

*Specifies whether an SNMP trap is sent to a network management station when Learn Mode is set to **static** and the port detects an unauthorized device, or when Learn Mode is set to continuous and there is an address change on a port.*

**none:** Prevents an SNMP trap from being sent. **none** is the default value.

**send-alarm:** Sends an intrusion alarm. Causes the switch to send an SNMP trap to a network management station.

**send-disable:** Sends alarm and disables the port. Available only in the **static**, **port-access**, **configured**, or **limited learn** modes. Causes the switch to send an SNMP trap to a network management station and disable the port. If you subsequently re-enable the port without clearing the port's intrusion flag, the port blocks further intruders, but the switch will not disable the port again until you reset the intrusion flag. See the Note on 10-34.

*For information on configuring the switch for SNMP management, refer to the Management and Configuration Guide for your switch.*

—Continued—

clear-intrusion-flag

*Clears the intrusion flag for a specific port. (See “Reading Intrusion Alerts and Resetting Alert Flags” on page 10-32.)*

no port-security <port-list> mac-address <mac-addr> [<mac-addr>  
<mac-addr>]

*Removes the specified learned MAC address(es) from the specified port.*

## Retention of Static Addresses

Static MAC addresses do not age-out. MAC addresses learned by using **learn-mode continuous** or **learn-mode limited-continuous** age out according to the currently configured MAC age time. (For information on the **mac-age-time** command, refer to the chapter titled “Interface Access and System Information” in the *Management and Configuration Guide* for your switch.

**Learned Addresses.** In the following two cases, a port in Static learn mode retains a learned MAC address even if you later reboot the switch or disable

port security for that port:

- The port learns a MAC address after you configure the port for Static learn mode in both the startup-config file and the running-config file (by executing the **write memory** command).
- The port learns a MAC address after you configure the port for Static learn mode in only the running-config file and, after the address is learned, you execute **write memory** to configure the startup-config file to match the running-config file.

To remove an address learned using either of the preceding methods, do one of the following:

- Delete the address by using **no port-security <port-number> mac-address <mac-addr>**.
- Download a configuration file that does not include the unwanted MAC address assignment.
- Reset the switch to its factory-default configuration.

**Assigned/Authorized Addresses.** : If you manually assign a MAC address (using **port-security <port-number> address-list <mac-addr>**) and then execute **write memory**, the assigned MAC address remains in memory until you do one of the following:

- Delete it by using **no port-security <port-number> mac-address <mac-addr>**.
- Download a configuration file that does not include the unwanted MAC address assignment.
- Reset the switch to its factory-default configuration.

**Specifying Authorized Devices and Intrusion Responses.** This example configures port A1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) It also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
ProCurve(config)# port-security a1 learn-mode static  
action send-disable
```

The next example does the same as the preceding example, except that it specifies a MAC address of 0c0090-123456 as the authorized device instead of allowing the port to automatically assign the first device it detects as an authorized device.

```
ProCurve(config)# port-security a1 learn-mode static  
mac-address 0c0090-123456 action send-disable
```

## Configuring and Monitoring Port Security Port Security

This example configures port A5 to:

- Allow two MAC addresses, 00c100-7fec00 and 0060b0-889e00, as the authorized devices.
- Send an alarm to a management station if an intruder is detected on the port, but allow the intruder access to the network.

```
ProCurve(config)# port-security a5 learn-mode static
address-limit 2 mac-address 00c100-7fec00 0060b0-889e00
action send-alarm
```

If you manually configure authorized devices (MAC addresses) and/or an alarm action on a port, those settings remain unless you either manually change them or the switch is reset to its factory-default configuration. You can “turn off” authorized devices on a port by configuring the port to continuous Learn Mode, but subsequently reconfiguring the port to static Learn Mode restores those authorized devices.

**Adding an Authorized Device to a Port.** To simply add a device (MAC address) to a port’s existing Authorized Addresses list, enter the port number with the **mac-address** parameter and the device’s MAC address. *This assumes that Learn Mode is set to **static** and the Authorized Addresses list is not full* (as determined by the current Address Limit value). For example, suppose port A1 allows two authorized devices, but has only one device in its Authorized Address list:

```
ProCurve(config)# show port-security a1
Port Security
Port : A1
Learn Mode [Continuous] : Static      Address Limit [1] : 2
Action [None] : None

Authorized Addresses
-----
0c0090-123456
```

Although the Address Limit is set to 2, only one device has been authorized for this port. In this case you can add another without having to also increase the Address Limit.

The Address Limit has not been reached.

**Figure 10-5. Example of Adding an Authorized Device to a Port**

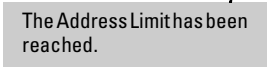
With the above configuration for port A1, the following command adds the 0c0090-456456 MAC address as the second authorized address.

```
ProCurve(config)# port-security a1 mac-address 0c0090-
456456
```

After executing the above command, the security configuration for port A1 would be:

```
ProCurve(config)# show port-security a1
Port Security
Port : A1
Learn Mode [Continuous] : Static      Address Limit [1] : 2
Action [None] : None

Authorized Addresses
-----
0c0090-123456
0c0090-456456
```



**Figure 10-6. Example of Adding a Second Authorized Device to a Port**

(The message **Inconsistent value** appears if the new MAC address exceeds the current Address Limit or specifies a device that is already on the list. Note that if you change a port from static to continuous learn mode, the port retains in memory any authorized addresses it had while in static mode. If you subsequently attempt to convert the port back to static mode with the same authorized address(es), the **Inconsistent value** message appears because the port already has the address(es) in its “Authorized” list.)

If you are adding a device (MAC address) to a port on which the Authorized Addresses list is already full (as controlled by the port’s current Address Limit setting), then you must increase the Address Limit in order to add the device, even if you want to replace one device with another. Using the CLI, you can simultaneously increase the limit and add the MAC address with a single command. For example, suppose port A1 allows one authorized device and already has a device listed:

```
ProCurve(config) show port-security a1
Port Security
Port : A1
Learn Mode [Continuous] : Static  Address Limit [1]:1
Action [None] : None

Authorized Addresses
-----
0c0090-20456
```

**Figure 10-7. Example of Port Security on Port A1 with an Address Limit of “1”**

To add a second authorized device to port A1, execute a **port-security** command for port A1 that raises the address limit to 2 and specifies the additional device's MAC address. For example:

```
ProCurve(config)# port-security a1 mac-address 0c0090-456456 address-limit 2
```

**Removing a Device From the “Authorized” List for a Port.** This command option removes unwanted devices (MAC addresses) from the Authorized Addresses list. (An Authorized Address list is available for each port for which Learn Mode is currently set to “Static”. Refer to the command syntax listing under “Configuring Port Security” on page 10-12.)

---

**Caution**

When learn mode is set to static, the Address Limit (address-limit) parameter controls how many devices are allowed in the Authorized Addresses (**mac-address**) for a given port. If you remove a MAC address from the Authorized Addresses list without also reducing the Address Limit by 1, the port may subsequently detect and accept as authorized a MAC address that you do not intend to include in your Authorized Address list. Thus, if you use the CLI to remove a device that is no longer authorized, it is recommended that you first reduce the Address Limit (**address-limit**) integer by 1, as shown below. This prevents the possibility of the same device or another unauthorized device on the network from automatically being accepted as “authorized” for that port.

---

To remove a device (MAC address) from the “Authorized” list and when the current number of devices equals the Address Limit value, you should first reduce the Address Limit value by 1, then remove the unwanted device.

---

**Note**

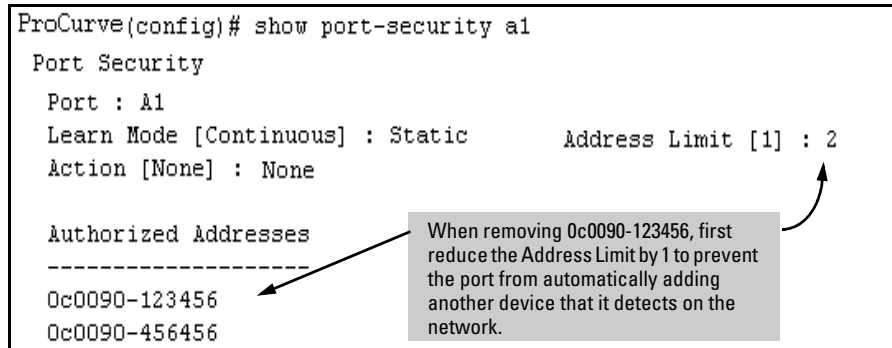
You can reduce the address limit below the number of currently authorized addresses on a port. This enables you to subsequently remove a device from the “Authorized” list without opening the possibility for an unwanted device to automatically become authorized.

---

For example, suppose port A1 is configured as shown below and you want to remove 0c0090-123456 from the Authorized Address list:

```
ProCurve(config)# show port-security a1
Port Security
  Port : A1
  Learn Mode [Continuous] : Static      Address Limit [1] : 2
  Action [None] : None

  Authorized Addresses
  -----
  0c0090-123456
  0c0090-456456
```



**Figure 10-8. Example of Two Authorized Addresses on Port A1**

The following command serves this purpose by removing 0c0090-123456 and reducing the Address Limit to 1:

```
ProCurve(config)# port-security a1 address-limit 1
ProCurve(config)# no port-security a1 mac-address 0c0090-123456
```

The above command sequence results in the following configuration for port A1:

```
ProCurve(config)# show port-sec a1
Port Security
  Port : A1
  Learn Mode : Static      Address Limit : 1
  Action : None
  Authorized Addresses
  -----
  0c0090-456456
```

**Figure 10-9. Example of Port A1 After Removing One MAC Address**

## MAC Lockdown

MAC Lockdown, also known as “static addressing,” is the permanent assignment of a given MAC address (and VLAN, or Virtual Local Area Network) to a specific port on the switch. MAC Lockdown is used to prevent station movement and MAC address hijacking. It also controls address learning on the switch. When configured, the MAC Address can only be used on the assigned port and the client device will only be allowed on the assigned VLAN.

---

### Note

Port security and MAC Lockdown are mutually exclusive on a given port. You can either use port security *or* MAC Lockdown, but never both at the same time on the same port.

**Syntax:** [no] static-mac < mac-addr > vlan < vid > interface < port-number >

You will need to enter a separate command for each MAC/VLAN pair you wish to lock down. If you do not specify a VLAN ID (VID) the switch inserts a VID of “1”.

**How It Works.** When a device’s MAC address is locked down to a port (typically in a pair with a VLAN) all information sent to that MAC address must go through the locked-down port. If the device is moved to another port it cannot receive data. Traffic to the designated MAC address goes only to the allowed port, whether the device is connected to it or not.

MAC Lockdown is useful for preventing an intruder from “hijacking” a MAC address from a known user in order to steal data. Without MAC Lockdown, this will cause the switch to learn the address on the malicious user’s port, allowing the intruder to steal the traffic meant for the legitimate user.

MAC Lockdown ensures that traffic intended for a specific MAC address can only go through the one port which is supposed to be connected to that MAC address. It does not prevent intruders from transmitting packets with the locked MAC address, but it does prevent responses to those packets from going anywhere other than the locked-down port. Thus TCP connections cannot be established. Traffic sent to the locked address cannot be hijacked and directed out the port of the intruder.

If the device (computer, PDA, wireless device) is moved to a different port on the switch (by reconnecting the Ethernet cable or by moving the device to an area using a wireless access point connected to a different port on that same switch), the port will detect that the MAC Address is not on the appropriate port and will continue to send traffic out the port to which the address was locked.

Once a MAC address is configured for one port, you cannot perform port security using the same MAC address on any other port on that same switch.

You cannot lock down a single MAC Address/VLAN pair to more than one port; however you can lock down multiple different MAC Addresses to a single port on the same switch.

Stations can move from the port to which their MAC address is locked to other parts of the network. They can send, but will not receive data if that data must go through the locked down switch. Please note that if the device moves to a distant part of the network where data sent to its MAC address never goes through the locked down switch, it may be possible for the device to have full two-way communication. For full and complete lockdown network-wide all switches must be configured appropriately.

**Other Useful Information.** Once you lock down a MAC address/VLAN pair on one port that pair cannot be locked down on a different port.

You cannot perform MAC Lockdown and 802.1X authentication on the same port or on the same MAC address. MAC Lockdown and 802.1X authentication are mutually exclusive.

Lockdown is permitted on static trunks (manually configured link aggregations).

## Differences Between MAC Lockdown and Port Security

Because port-security relies upon MAC addresses, it is often confused with the MAC Lockdown feature. However, MAC Lockdown is a completely different feature and is implemented on a different architecture level.

Port security maintains a list of allowed MAC addresses on a per-port basis. An address can exist on multiple ports of a switch. Port security deals with MAC addresses only while MAC Lockdown specifies both a MAC address and a VLAN for lockdown.

MAC Lockdown, on the other hand, is not a “list.” It is a global parameter on the switch that takes precedence over any other security mechanism. The MAC Address will only be allowed to communicate using one specific port on the switch.

MAC Lockdown is a good replacement for port security to create tighter control over MAC addresses and which ports they are allowed to use (only one port per MAC Address on the same switch in the case of MAC Lockdown). (You can still use the port for other MAC addresses, but you cannot use the locked down MAC address on other ports.)

Using only port security the MAC Address could still be used on another port on the same switch. MAC Lockdown, on the other hand, is a clear one-to-one relationship between the MAC Address and the port. Once a MAC address has been locked down to a port it cannot be used on another port on the same switch.

The switch does not allow MAC Lockdown and port security on the same port.

## MAC Lockdown Operating Notes

**Limits.** There is a limit of 500 MAC Lockdowns that you can safely code per switch. To truly lock down a MAC address it would be necessary to use the MAC Lockdown command for every MAC Address and VLAN ID on every switch. In reality few network administrators will go to this length, but it is important to note that just because you have locked down the MAC address and VID for a single switch, the device (or a hacker “spoofing” the MAC address for the device) may still be able to use another switch which hasn’t been locked down.

**Event Log Messages.** If someone using a locked down MAC address is attempting to communicate using the wrong port the “move attempt” generates messages in the log file like this:

Move attempt (lockdown) logging:

```
W 10/30/03 21:33:43 maclock: module A: Move 0001e6-1f96c0  
to A15 denied
```

```
W 10/30/03 21:33:48 maclock: module A: Move 0001e6-1f96c0  
to A15 denied
```

```
W 10/30/03 21:33:48 maclock: module A: Ceasing move-denied  
logs for 5m
```

These messages in the log file can be useful for troubleshooting problems. If you are trying to connect a device which has been locked down to the wrong port, it will not work but it will generate error messages like this to help you determine the problem.

**Limiting the Frequency of Log Messages.** The first move attempt (or intrusion) is logged as you see in the example above. Subsequent move attempts send a message to the log file also, but message throttling is imposed on the logging on a per-module basis. What this means is that the logging system checks again after the first 5 minutes to see if another attempt has been made to move to the wrong port. If this is the case the log file registers the most recent attempt and then checks again after one hour. If there are no further attempts in that period then it will continue to check every 5 minutes. If another attempt was made during the one hour period then the log resets itself to check once a day. The purpose of rate-limiting the log messaging is to prevent the log file from becoming too full. You can also configure the switch to send the same messages to a Syslog server. Refer to “Debug and Syslog Messaging Operation” in appendix C of the *Management and Configuration Guide* for your switch.

## Deploying MAC Lockdown

When you deploy MAC Lockdown you need to consider how you use it within your network topology to ensure security. In some cases where you are using techniques such as “meshing” or Spanning Tree Protocol (STP) to speed up network performance by providing multiple paths for devices, using MAC Lockdown either will not work or else it defeats the purpose of having multiple data paths.

The purpose of using MAC Lockdown is to prevent a malicious user from “hijacking” an approved MAC address so they can steal data traffic being sent to that address.

As we have seen, MAC Lockdown can help prevent this type of hijacking by making sure that all traffic to a specific MAC address goes only to the proper port on a switch which is supposed to be connected to the real device bearing that MAC address.

However, you can run into trouble if you incorrectly try to deploy MAC Lockdown in a network that uses multiple path technology, like Spanning Tree or “mesh networks.”

Let’s examine a good use of MAC Lockdown within a network to ensure security first.

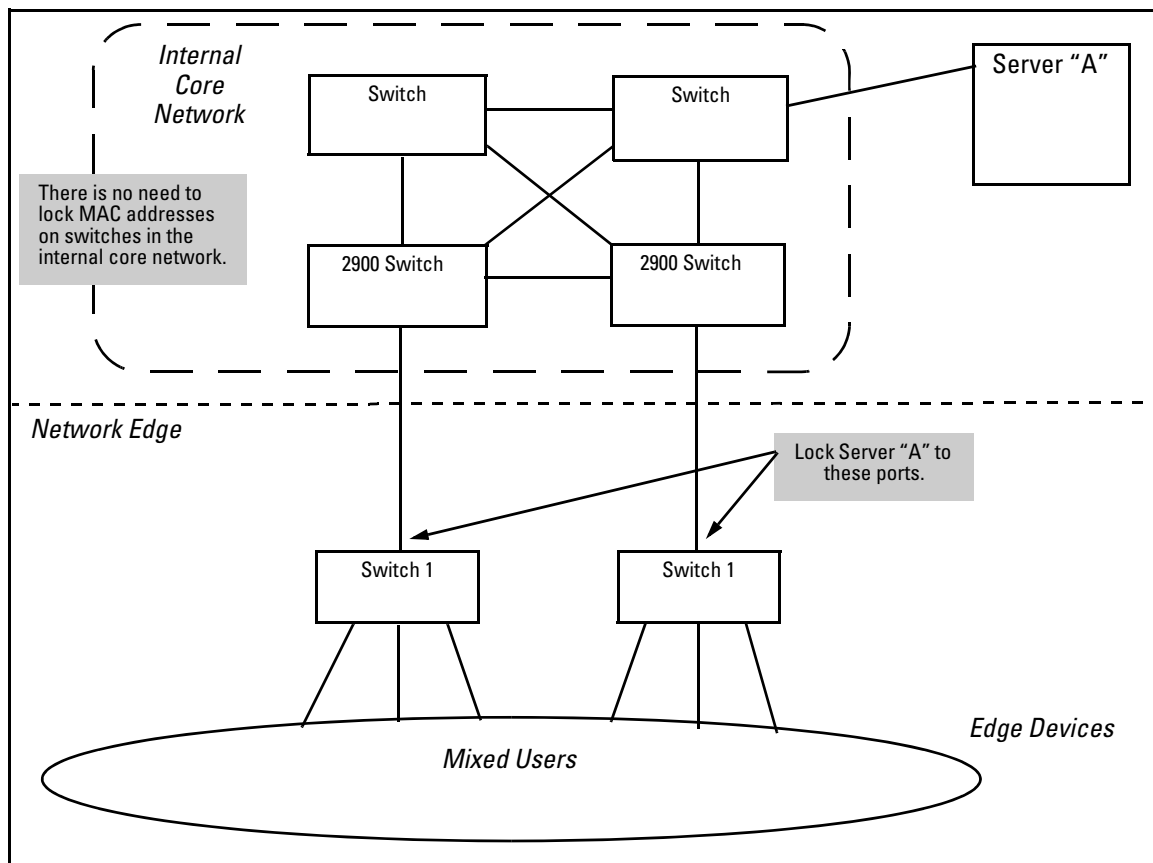


Figure 10-10. MAC Lockdown Deployed At the Network Edge Provides Security

**Basic MAC Lockdown Deployment.** In the Model Network Topology shown above, the switches that are connected to the edge of the network each have one and only one connection to the core network. This means each switch has only one path by which data can travel to Server A. You can use MAC Lockdown to specify that all traffic intended for Server A's MAC Address must go through the one port on the edge switches. That way, users on the edge can still use other network resources, but they cannot "spoof" Server A and hijack data traffic which is intended for that server alone.

The key points for this Model Topology are:

- The Core Network is separated from the edge by the use of switches which have been “locked down” for security.
- All switches connected to the edge (outside users) each have only one port they can use to connect to the Core Network and then to Server A.
- Each switch has been configured with MAC Lockdown so that the MAC Address for Server A has been locked down to one port per switch that can connect to the Core and Server A.

Using this setup Server A can be moved around within the core network, and yet MAC Lockdown will still prevent a user at the edge from hijacking its address and stealing data.

Please note that in this scenario a user with bad intentions at the edge can still “spoof” the address for Server A and send out data packets that look as though they came from Server A. The good news is that because MAC Lockdown has been used on the switches on the edge, any traffic that is sent *back* to Server A will be sent to the proper MAC Address because MAC Lockdown has been used. The switches at the edge will not send Server A’s data packets anywhere but the port connected to Server A. (Data would not be allowed to go beyond the edge switches.)

---

**Caution**

---

Using MAC Lockdown still does not protect against a hijacker *within the core!* In order to protect against someone spoofing the MAC Address for Server A inside the Core Network, you would have to lock down each and every switch inside the Core Network as well, not just on the edge.

**Problems Using MAC Lockdown in Networks With Multiple Paths.** Now let’s take a look at a network topology in which the use of MAC Lockdown presents a problem. In the next figure, Switch 1 (on the bottom-left) is located at the edge of the network where there is a mixed audience that might contain hackers or other malicious users. Switch 1 has two paths it could use to connect to Server A. If you try to use MAC Lockdown here to make sure that all data to Server A is “locked down” to one path, connectivity problems would be the result since both paths need to be usable in case one of them fails.

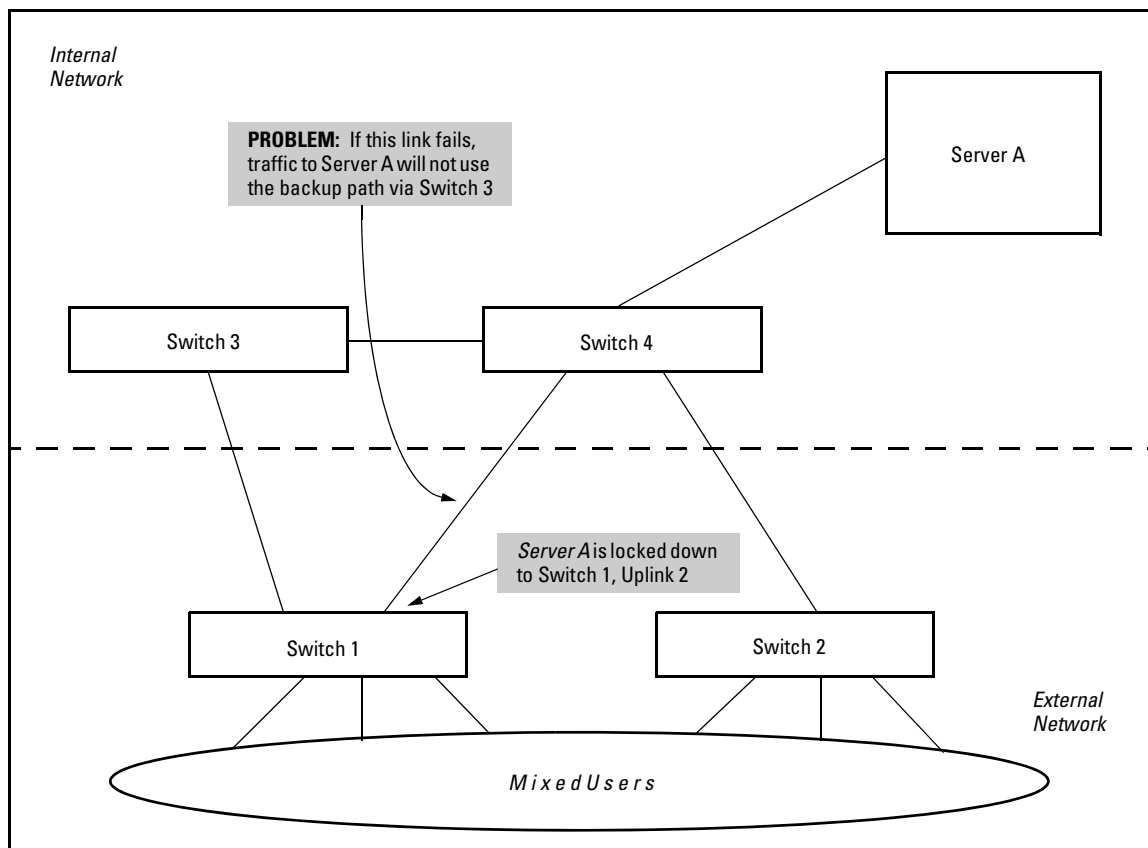


Figure 10-11. Connectivity Problems Using MAC Lockdown with Multiple Paths

The resultant connectivity issues would prevent you from locking down Server A to Switch 1. And when you remove the MAC Lockdown from Switch 1 (to prevent broadcast storms or other connectivity issues), you then open the network to security problems. The use of MAC Lockdown as shown in the above figure would defeat the purpose of using MSTP or having an alternate path.

Technologies such as MSTP or “meshing” are primarily intended for an internal campus network environment in which all users are trusted. MSTP and “meshing” do not work well with MAC Lockdown.

If you deploy MAC Lockdown as shown in the Model Topology in figure 10-10 (page 10-26), you should have no problems with either security or connectivity.

## MAC Lockout

MAC Lockout involves configuring a MAC address on all ports and VLANs for a switch so that any traffic to or from the “locked-out” MAC address will be dropped. This means that all data packets addressed to or from the given address are stopped by the switch. MAC Lockout is implemented on a per switch assignment.

You can think of MAC Lockout as a simple blacklist. The MAC address is locked out on the switch and on all VLANs. No data goes out or in from the blacklisted MAC address to a switch using MAC Lockout.

To fully lock out a MAC address from the network it would be necessary to use the MAC Lockout command on all switches.

To use MAC Lockout you must first know the MAC Address you wish to block.

**Syntax:** [no] lockout-mac < mac-address >

**How It Works.** Let’s say a customer knows there are unauthorized wireless clients who should not have access to the network. The network administrator “locks out” the MAC addresses for the wireless clients by using the MAC Lockout command (**lockout-mac <mac-address>**). When the wireless clients then attempt to use the network, the switch recognizes the intruding MAC addresses and prevents them from sending or receiving data on that network.

If a particular MAC address can be identified as unwanted on the switch then that MAC Address can be disallowed on all ports on that switch with a single command. You don’t have to configure every single port—just perform the command on the switch and it is effective for all ports.

MAC Lockout overrides MAC Lockdown, port security, and 802.1X authentication.

You cannot use MAC Lockout to lock:

- Broadcast or Multicast Addresses (Switches do not learn these)
- Switch Agents (The switch's own MAC Address)

There are limits for the number of VLANs, Multicast Filters, and Lockout MACs that can be configured concurrently as all use MAC table entries. The limits are shown below.

**Table 10-1. Limits on Lockout MACs**

# VLANs	# Multicast Filters	# Lockout MACs
<= 1024	16	16
1025-2048	8	8

If someone using a locked out MAC address tries to send data through the switch a message is generated in the log file:

Lockout logging format:

```
W 10/30/03 21:35:15 maclock: module A: 0001e6-1f96c0
detected on port A15
W 10/30/03 21:35:18 maclock: module A: 0001e6-1f96c0
detected on port A15
W 10/30/03 21:35:18 maclock: module A: Ceasing lock-out
logs for 5m
```

As with MAC Lockdown a rate limiting algorithm is used on the log file so that it does not become overlogged with error messages. (Refer to “Limiting the Frequency of Log Messages” on page 10-25.)

## Port Security and MAC Lockout

MAC Lockout is independent of port-security and in fact will override it. MAC Lockout is preferable to port-security to stop access from known devices because it can be configured for all ports on the switch with one command.

It is possible to use MAC Lockout in conjunction with port-security. You can use MAC Lockout to lock out a single address—deny access to a specific device—but still allow the switch some flexibility in learning other MAC Addresses. Be careful if you use both together, however:

- If a MAC Address is locked out and appears in a static learn table in port-security, the apparently “authorized” address will still be locked out anyway.
- MAC entry configurations set by port security will be kept even if MAC Lockout is configured and the original port security settings will be honored once the Lockout is removed.
- A port security static address is permitted to be a lockout address. In that case (MAC Lockout), the address will be locked out (SA/DA drop) even though it’s an “authorized” address from the perspective of port security.
- When MAC Lockout entries are deleted, port security will then re-learn the address as needed later on.

## Web: Displaying and Configuring Port Security Features

1. Click on the **Security** tab.
2. Click on **[Port Security]**.
3. Select the settings you want and, if you are using the Static Learn Mode, add or edit the Authorized Addresses field.
4. Implement your new data by clicking on **[Apply Changes]**.

To access the web-based Help provided for the switch, click on **[?]** in the web browser screen.

---

## Reading Intrusion Alerts and Resetting Alert Flags

### Notice of Security Violations

When the switch detects an intrusion on a port, it sets an “alert flag” for that port and makes the intrusion information available as described below. *While the switch can detect additional intrusions for the same port, it does not list the next chronological intrusion for that port in the Intrusion Log until the alert flag for that port has been reset.*

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an alert flag for that port. This flag remains set until:
  - You use either the CLI, menu interface, or web browser interface to reset the flag.
  - The switch is reset to its factory default configuration.

- The switch enables notification of the intrusion through the following means:
  - In the CLI:
    - The **show port-security intrusion-log** command displays the Intrusion Log
    - The **log** command displays the Event Log
  - In the menu interface:
    - The Port Status screen includes a per-port intrusion alert
    - The Event Log includes per-port entries for security violations
  - In the web browser interface:
    - The Alert Log's Status | Overview window includes entries for per-port security violations
    - The Intrusion Log in the Security | Intrusion Log window lists per-port security violation entries
  - In network management applications such as ProCurve Manager via an SNMP trap sent to a network management station

## How the Intrusion Log Operates

When the switch detects an intrusion attempt on a port, it enters a record of this event in the Intrusion Log. No further intrusion attempts on that port will appear in the Log until you acknowledge the earlier intrusion event by resetting the alert flag.

The Intrusion Log lists the 20 most recently detected security violation attempts, regardless of whether the alert flags for these attempts have been reset. This gives you a history of past intrusion attempts. Thus, for example, if there is an intrusion alert for port A1 and the Intrusion Log shows two or more entries for port 1, only the most recent entry has not been acknowledged (by resetting the alert flag). The other entries give you a history of past intrusions detected on port A1.

```
Status and Counters - Intrusion Log
Port  MAC Address          Date / Time
-----
A1    080009-e93d4f            03/07/06 21:09:34
A1    080009-e93d4f            03/07/06 10:18:43
```

**Figure 10-12. Example of Multiple Intrusion Log Entries for the Same Port**

The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries (unless you reset the switch to its factory-default configuration). Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

## Keeping the Intrusion Log Current by Resetting Alert Flags

When a violation occurs on a port, an alert flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you reset the alert flag for either all ports or for the individual port.

---

### **Note on Send-Disable Operation**

On a given port, if the intrusion action is to send an SNMP trap and then disable the port (**send-disable**), and an intruder is detected on the port, then the switch sends an SNMP trap, sets the port's alert flag, and disables the port. If you re-enable the port without resetting the port's alert flag, then the port operates as follows:

- The port comes up and will block traffic from unauthorized devices it detects.
- If the port detects another intruder, it will send another SNMP trap, but will not become disabled again unless you first reset the port's intrusion flag.

This operation enables the port to continue passing traffic for authorized devices while you take the time to locate and eliminate the intruder. Otherwise, the presence of an intruder could cause the switch to repeatedly disable the port.

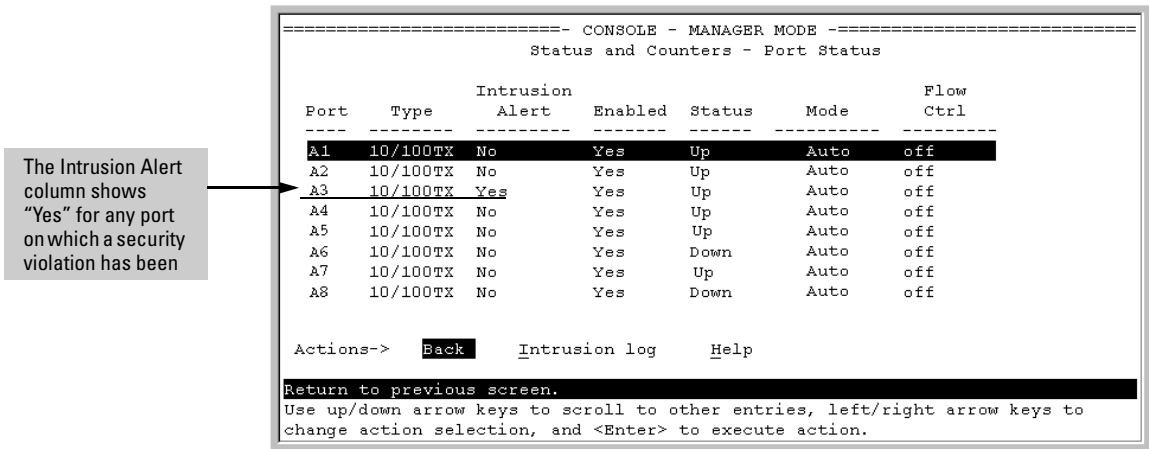
---

## Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The menu interface indicates per-port intrusions in the Port Status screen, and provides details and the reset function in the Intrusion Log screen.

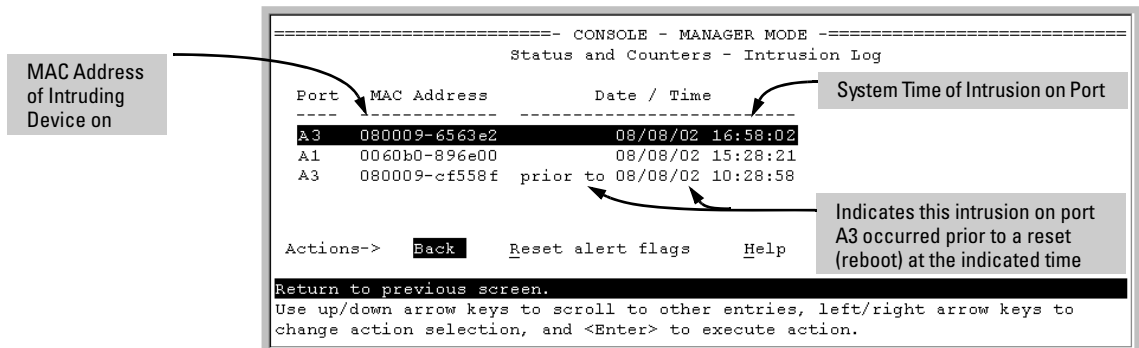
- From the Main Menu select:

- 1. Status and Counters**
  - 4. Port Status**



**Figure 10-13. Example of Port Status Screen with Intrusion Alert on Port A3**

- Type [I] (**Intrusion log**) to display the Intrusion Log.



**Figure 10-14. Example of the Intrusion Log Display**

The example in Figure 7-11 shows two intrusions for port A3 and one intrusion for port A1. In this case, only the most recent intrusion at port A3 has not been acknowledged (reset). This is indicated by the following:

- Because the Port Status screen (figure 10-13 on page 10-35) does not indicate an intrusion for port A1, the alert flag for the intrusion on port A1 has already been reset.
- Since the switch can show only one uncleared intrusion per port, the alert flag for the older intrusion for port A3 in this example has also been previously reset.

(The intrusion log holds up to 20 intrusion records and deletes an intrusion record only when the log becomes full and a new intrusion is subsequently detected.)

Note also that the “**prior to**” text in the record for the earliest intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

3. To acknowledge the most recent intrusion entry on port A3 and enable the switch to enter a subsequently detected intrusion on this port, type **[R]** (for **Reset alert flags**). (Note that if there are unacknowledged intrusions on two or more ports, this step resets the alert flags for all such ports.)

If you then re-display the port status screen, you will see that the Intrusion Alert entry for port A3 has changed to “**No**”. That is, your evidence that the Intrusion Alert flag has been acknowledged (reset) is that the Intrusion Alert column in the port status display no longer shows “**Yes**” for the port on which the intrusion occurred (port A3 in this example). (Because the Intrusion Log provides a history of the last 20 intrusions detected by the switch, resetting the alert flags does not change its content. Thus, displaying the Intrusion Log again will result in the same display as in figure 10-14, above.)

### CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The following commands display port status, including whether there are intrusion alerts for any port(s), list the last 20 intrusions, and either reset the alert flag on all ports or for a specific port for which an intrusion was detected. (The record of the intrusion remains in the log. For more information, refer to “Operating Notes for Port Security” on page 10-40.)

**Syntax:** show interfaces brief

*List intrusion alert status (and other port status information)'.*

show port-security intrusion-log

*List intrusion log content.*

clear intrusion-flags

*Clear intrusion flags on all ports.*

port-security [e] < port-number > clear-intrusion-flag

*Clear the intrusion flag on one or more specific ports.*

In the following example, executing **show interfaces brief** lists the switch's port status, which indicates an intrusion alert on port A1.

```

ProCurve# show interfaces brief
Status and Counters - Port Status

```

Port	Type	Intrusion Alert	Enabled	Status	Mode	Flow Ctrl
A1	10/100TX	Yes	Yes	Up	10HDx	off
A2	10/100TX	No	Yes	Up	10HDx	off
A3	10/100TX	No	Yes	Up	10HDx	off
A4	10/100TX	No	Yes	Up	10HDx	off

Intrusion Alert on port

**Figure 10-15.** Example of an Unacknowledged Intrusion Alert in a Port Status Display

If you wanted to see the details of the intrusion, you would then enter the **show port-security intrusion-log** command. For example:

```

ProCurve# show port-security intrusion-log
Status and Counters - Intrusion Log

```

Port	MAC Address	Date / Time
A1	080009-e93d4f	07/03/06 21:09:34
A1	080009-21ae84	07/03/06 17:26:27
A1	080009-e93d4f	prior to 07/03/06 17:18:43
	0 secs	
	0 secs	

MAC Address of latest Intruder on Port A1

Dates and Times of Intrusions

Earlier intrusions on port A1 that have already been cleared (that is, the Alert Flag has been reset at least twice before the most recent intrusion)

**Figure 10-16.** Example of the Intrusion Log with Multiple Entries for the Same Port

The above example shows three intrusions for port A1. Since the switch can show only one uncleared intrusion per port, the older two intrusions in this example have already been cleared by earlier use of the **clear intrusion-log** or the **port-security < port-list > clear-intrusion-flag** command. (The intrusion log holds up to 20 intrusion records, and deletes intrusion records only when the log becomes full and new intrusions are subsequently added.) The “**prior to**” text in the record for the third intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

To clear the intrusion from port A1 and enable the switch to enter any subsequent intrusion for port A1 in the Intrusion Log, execute the port-security **clear-intrusion-flag** command. If you then re-display the port status screen, you will see that the Intrusion Alert entry for port A1 has changed to **“No”**. (Executing **show port-security intrusion-log** again will result in the same display as above, and does not include the Intrusion Alert status.)

```
ProCurve(config)# port-security a1 clear-intrusion-flag
ProCurve(config)# show interfaces brief
```

Status and Counters - Port Status							
Port	Type	Intrusion			Flow	Bcast	
		Alert	Enabled	Status			
A1	10/100TX	No	Yes	Up	10HDx	off	0
A2	10/100TX	No	Yes	Up	10HDx	off	0
A3	10/100TX	No	Yes	Up	10HDx	off	0

Intrusion Alert on port A1 is now

**Figure 10-17. Example of Port Status Screen After Alert Flags Reset**

For more on clearing intrusions, see “Note on Send-Disable Operation” on page 10-34

## Using the Event Log To Find Intrusion Alerts

The Event Log lists port security intrusions as:

```
W MM/DD/YY HH:MM:SS FFI: port A3 - Security Violation
```

where **“W”** is the severity level of the log entry and **FFI** is the system module that generated the entry. For further information, display the Intrusion Log, as shown below.

**From the CLI.** Type the **log** command from the Manager or Configuration level.

**Syntax:** log < search-text >

For < **search-text** >, you can use **ffi**, **security**, or **violation**. For example:

```
ProCurve(config)# log security
Keys:   W=Warning   I=Information
        M=Major    D=Debug
----  Event Log listing: Events Since Boot  ----
W 08/01/02 01:18:15 FFI: port A2 - Security Violation
W 08/01/02 04:28:08 FFI: port A1 - Security Violation
----  Bottom of Log : Events Listed = 2  ----

ProCurve(config)# log security
Keys:   W=Warning   I=Information
        M=Major    D=Debug
----  Event Log listing: Events Since Boot  ----
----  Bottom of Log : Events Listed = 0  ----
```

Figure 10-18. Example of Log Listing With and Without Detected Security Violations

**From the Menu Interface:** In the Main Menu, click on **4. Event Log** and use **Next page** and **Prev page** to review the Event Log contents.

**For More Event Log Information.** See “Using the Event Log To Identify Problem Sources” in the “Troubleshooting” chapter of the *Management and Configuration Guide* for your switch.

## Web: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

1. Check the Alert Log by clicking on the **Status** tab and the **[Overview]** button. If there is a “Security Violation” entry, do the following:
  - a. Click on the **Security** tab.
  - b. Click on **[Intrusion Log]**. “Ports with Intrusion Flag” indicates any ports for which the alert flag has not been cleared.
  - c. To clear the current alert flags, click on **[Reset Alert Flags]**.

To access the web-based Help provided for the switch, click on **[?]** in the web browser screen.

## Operating Notes for Port Security

**Identifying the IP Address of an Intruder.** The Intrusion Log lists detected intruders by MAC address. If you are using ProCurve Manager to manage your network, you can use the device properties page to link MAC addresses to their corresponding IP addresses.

**Proxy Web Servers.** If you are using the switch's web browser interface through a switch port configured for Static port security, and your browser access is through a proxy web server, then it is necessary to do the following:

- Enter your PC or workstation MAC address in the port's Authorized Addresses list.
- Enter your PC or workstation's IP address in the switch's IP Authorized Managers list. See "Using Authorized IP Managers" in the *Management and Configuration Guide* for your switch.)

Without both of the above configured, the switch detects only the proxy server's MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized.

**"Prior To" Entries in the Intrusion Log.** If you reset the switch (using the Reset button, Device Reset, or Reboot Switch), the Intrusion Log will list the time of all currently logged intrusions as "prior to" the time of the reset.

**Alert Flag Status for Entries Forced Off of the Intrusion Log.** If the Intrusion Log is full of entries for which the alert flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the alert flag status for the port referenced in the dropped entry. This means that, even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the alert flags.

**LACP Not Available on Ports Configured for Port Security.** To maintain security, LACP is not allowed on ports configured for port security. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables port security on that port. For example:

```
ProCurve(config)# port-security e a17 learn-mode static  
address-limit 2  
LACP has been disabled on secured port(s).  
ProCurve(config)#
```

The switch will not allow you to configure LACP on a port on which port security is enabled. For example:

```
ProCurve(config)# int e a17 lacp passive  
Error configuring port A17: LACP and port security cannot  
be run together.  
ProCurve(config)#
```

To restore LACP to the port, you must remove port security and re-enable LACP active or passive.

**Configuring and Monitoring Port Security**  
**Operating Notes for Port Security**