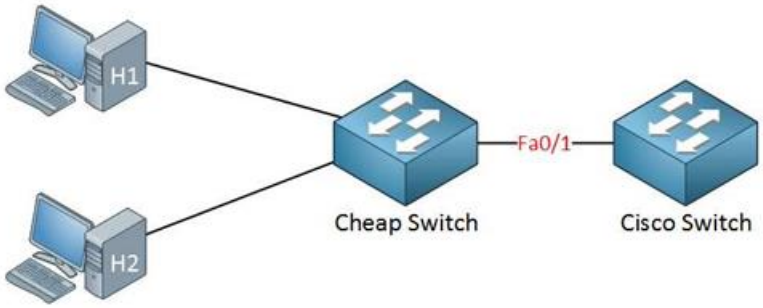
# CÁCH CẤU HÌNH BẢO MẬT CỔNG TRÊN SWITCH CISCO

Mặc định, không có giới hạn về số lượng địa chỉ MAC mà switch có thể học trên một giao diện và tất cả địa chỉ MAC đều được cho phép. Nếu muốn, chúng ta có thể thay đổi hành vi này bằng cách sử dụng port-security. Hãy cùng xem xét mô hình sau :




Trong sơ đồ mạng trên, một switch không được quản lý (unmanaged switch) từ bên ngoài đã được kết nối vào cổng FastEthernet 0/1 của switch Cisco. Điều này thường xảy ra khi người dùng mang thêm switch cá nhân từ bên ngoài vào hệ thống mạng doanh nghiệp. Hệ quả là switch Cisco sẽ học địa chỉ MAC của cả hai thiết bị H1 và H2 thông qua cổng FastEthernet 0/1, có thể dẫn đến rủi ro bảo mật và quản lý mạng.

Tất nhiên, chúng ta không muốn người dùng tự ý mang switch của họ và kết nối vào mạng của chúng ta. Vì vậy, chúng ta cần ngăn chặn điều này xảy ra. Dưới đây là cách thực hiện:

Sử dụng lệnh switchport port-security để kích hoạt tính năng bảo mật cổng (port-security). VnPro đã cấu hình port-security để chỉ cho phép một địa chỉ MAC duy nhất. Khi switch phát hiện một địa chỉ MAC khác trên giao diện này, nó sẽ rơi vào trạng thái violation (vi phạm) và một hành động sẽ xảy ra.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
```

Bên cạnh việc đặt giới hạn tối đa cho số lượng địa chỉ MAC, chúng ta cũng có thể sử dụng bảo mật cổng (port security) để **lọc** các địa chỉ MAC. Bạn có thể sử dụng tính năng này để chỉ cho phép các địa chỉ MAC cụ thể.

Trong ví dụ này ,VnPro đã cấu hình bảo mật cổng sao cho chỉ cho phép địa chỉ MAC aaaa.bbbb.cccc. Đây không phải là địa chỉ MAC của máy tính của máy tính trên mô hình, vì vậy nó là một ví dụ hoàn hảo để minh họa một vi phạm bảo mật.

Sử dụng lệnh switchport port-security mac-address để xác định địa chỉ MAC mà bạn muốn cho phép.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security mac-address aaaa.bbbb.cccc
```

VnPro đang thực hiện lệnh ping đến một địa chỉ IP giả. không có thiết bị nào có địa chỉ IP 1.2.3.4 để tạo một số lưu lượng để gây ra vi phạm bảo mật.

```
C:\Documents and Settings\H1>ping 1.2.3.4
```

VnPro chỉ muốn tạo một ít lưu lượng mạng. Đây là những gì bạn sẽ thấy: (Chúng ta đã gặp một vi phạm bảo mật, và kết quả là cổng chuyển sang trạng thái err-disable. Như bạn có thể thấy, cổng hiện đang bị tắt. Hãy cùng xem xét chi tiết hơn về bảo mật cổng (port security))

```
 SwitchA#
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting
Fa0/1 in err-disable state
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0090.cc0e.5023 on port FastEthernet0/1.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Sử dụng lệnh show port-security interface f0/1 để kiểm tra để xem chi tiết bảo mật cổng trên từng giao diện. Bạn có thể thấy chế độ vi phạm (violation mode) đang ở trạng thái shutdown và lần vi phạm gần nhất do địa chỉ MAC 0090.cc0e.5023 (H1) gây ra.

```
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0090.cc0e.5023:1
Security Violation Count   : 1
```

Đây là một lệnh hữu ích để kiểm tra cấu hình bảo mật cổng của bạn. Sử dụng lệnh show port-security interface (Kết quả trong hình cho thấy rằng cổng **FastEthernet0/1** trên switch đang ở trạng thái **err-disabled**. Điều này có nghĩa là cổng đã bị vô hiệu hóa tự động bởi switch do phát hiện một lỗi )

```
Switch#show interfaces fa0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
```

Tắt giao diện sau khi xảy ra vi phạm bảo mật là một ý tưởng tốt (về mặt bảo mật), nhưng vấn đề là giao diện sẽ vẫn ở trạng thái err-disable. Điều này có thể đồng nghĩa với việc bạn phải gọi bộ phận hỗ trợ kỹ thuật (helpdesk) để khôi phục giao diện về trạng thái hoạt động bình thường! Hãy kích hoạt lại nó nào:

Để đưa giao diện ra khỏi trạng thái err-disable, bạn cần nhập lệnh shutdown, sau đó là no shutdown. Chỉ nhập no shutdown là không đủ

```
Switch(config)#interface fa0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

Sẽ tiện lợi hơn nếu giao diện có thể tự phục hồi sau một khoảng thời gian nhất định. Bạn có thể kích hoạt tính năng này bằng lệnh sau:

```
Switch(config)#errdisable recovery cause psecure-violation
```

Sau 5 phút (300 giây), giao diện sẽ tự động phục hồi khỏi trạng thái err-disable. Tuy nhiên, hãy đảm bảo rằng bạn đã khắc phục sự cố, nếu không, vi phạm sẽ tiếp tục xảy ra và giao diện sẽ lại rơi vào trạng thái err-disable.. Bạn có thể đẩy nhanh quá trình này bằng cách thay đổi thời gian hẹn giờ. Hãy đặt nó thành 30 giây

```
SW1(config)#errdisable recovery interval 30
```

Thay vì nhập thủ công địa chỉ MAC, chúng ta có thể cấu hình để switch tự động học địa chỉ MAC phục vụ cho port security:

```
Switch(config-if)#no switchport port-security mac-address aaaa.bbbb.cccc
Switch(config-if)#switchport port-security mac-address sticky
```

Từ khóa sticky đảm bảo rằng switch sẽ sử dụng địa chỉ MAC đầu tiên mà nó học được trên giao diện để phục vụ port security. Hãy kiểm tra lại cấu hình này

(Bạn có thể thấy rằng switch sẽ tự động lưu địa chỉ MAC của H1 vào running-config.)

```
Switch#show run interface fa0/1
Building configuration...
Current configuration : 228 bytes
!
interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 000c.2928.5c6c
```

Việc tắt giao diện khi có vi phạm có thể là quá mức cần thiết. Có những lựa chọn khác, đây là một số tùy chọn bạn có thể sử dụng:

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

Bản tóm tắt về các chế độ xử lý vi phạm trong Port Security:

- Protect: Drop (loại bỏ) các frame từ MAC address không được phép, không có log.
- Restrict: Drop frame từ MAC address không hợp lệ, có log và gửi SNMP trap.
- Shutdown: Đưa cổng vào trạng thái err-disable, có log và gửi SNMP trap.

Cách khôi phục cổng khi bị err-disable:

Thủ công: Dùng lệnh shutdown → no shutdown.
Tự động: Dùng lệnh errdisable recovery.

Chúc mừng bạn đã thực hiện thành công

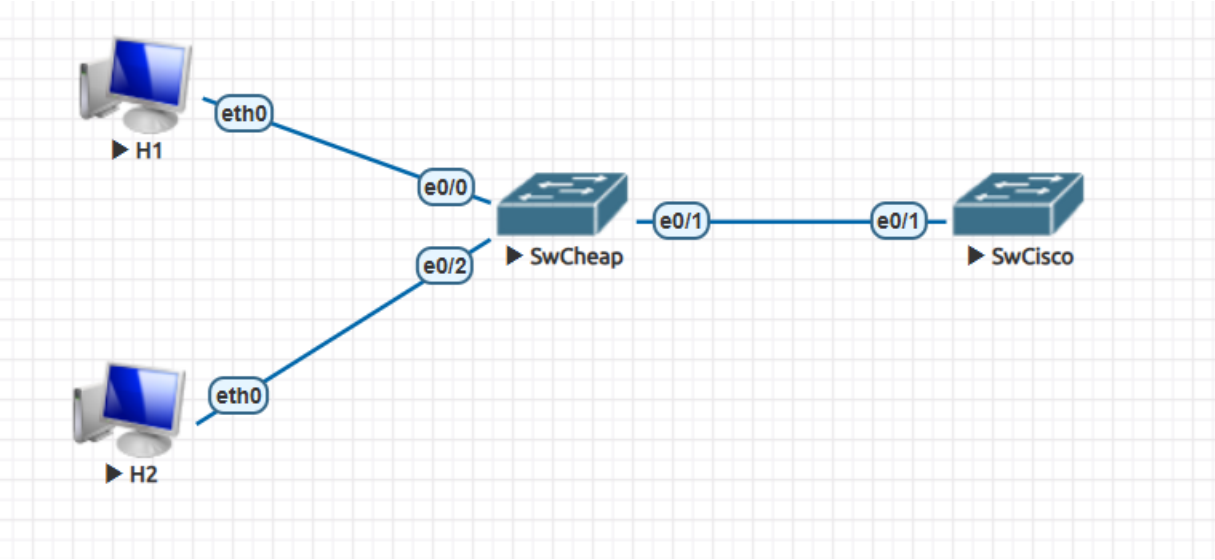
Bạn hãy kiểm tra trên switch

```
hostname Switch
!
interface fastEthernet0/1
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
!
errdisable recovery cause psecure-violation
!
end
```

# THỰC HÀNH LAB TRÊN EVE

**( Vnpro đã thực hiện và chạy thử thành công )**

Mô hình




Cấu hình trên switch

Sử dụng lệnh switchport port-security để kích hoạt tính năng bảo mật cổng (port-security). VnPro đã cấu hình port-security để chỉ cho 2 địa chỉ MAC trên cổng e0/1

Tiếp theo sử dụng lệnh switchport port-security mac-address để xác định địa chỉ MAC mà bạn muốn cho phép Và địa Mac VnPro cho phép là 00:50;79:65:68:01 ( địa chỉ mac này không thuộc 2 pc trên mô hình )

```
Switch(config)#interface e0/1
Switch(config-if)#switchport port-security mac-address 00:50:79:65:68:01
Total secure mac-addresses on interface Ethernet0/1 has reached maximum limit.
Switch(config-if)#switchport port-security mac-address aaaa.bbbb.cccc
Total secure mac-addresses on interface Ethernet0/1 has reached maximum limit.
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address 00:50:79:65:68:01
Switch(config-if)#exit
Switch(config)#exit
Switch#wr
Building configuration...
Compressed configuration from 941 bytes to 643 bytes[OK]
Switch#
*Mar  7 08:45:03.446: %SYS-5-CONFIG_I: Configured from console by console
```

Bây giờ, chúng ta sẽ tạo một số lưu lượng để gây ra vi phạm bảo mật

Trên H1 ping đến địa chỉ 1.2.3.4

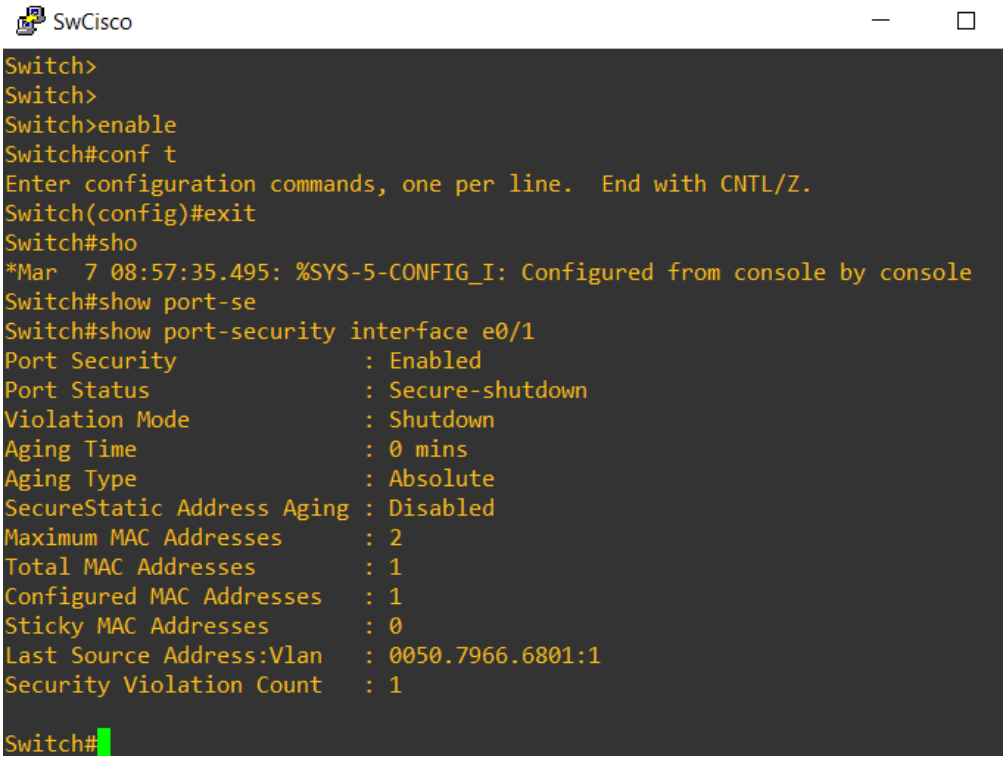
```
H1> ping 1.2.3.4

host (1.2.3.4) not reachable

H1>
```

Kết quả trên Switch Cisco sẽ hiện

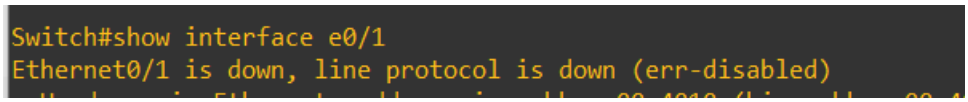
```
Switch#
*Mar  7 08:45:03.446: %SYS-5-CONFIG_I: Configured from console by console
Switch#
*Mar  7 08:45:16.882: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0
/1, putting Et0/1 in err-disable state
Switch#
*Mar  7 08:45:16.883: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occ
urred, caused by MAC address 0050.7966.6801 on port Ethernet0/1.
*Mar  7 08:45:17.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
Switch#
*Mar  7 08:45:18.884: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to do
wn
Switch#
```

Chúng ta đã gặp một vi phạm bảo mật, và kết quả là cổng chuyển sang trạng thái err-disable. Như bạn có thể thấy, cổng hiện đang bị tắt

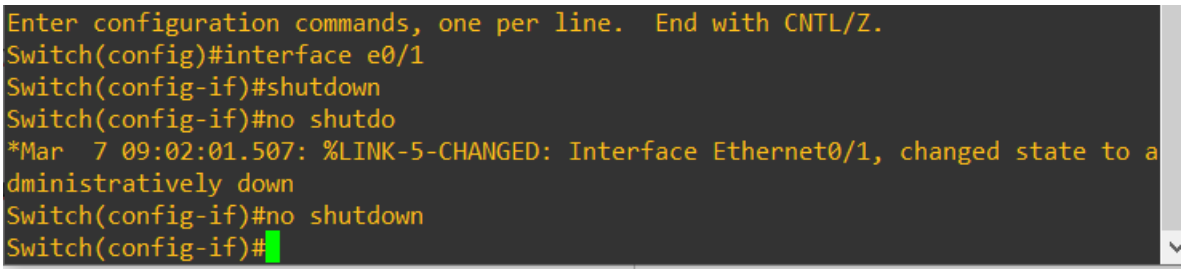
Hãy cùng xem xét chi tiết hơn về bảo mật cổng (port security) bằng lệnh ***show port-security interface e0/1***




. Bạn có thể thấy chế độ vi phạm (violation mode) đang ở trạng thái shutdown và lần vi phạm gần nhất do địa chỉ MAC 0050.7966.6801:1 (H1) gây ra.




Tắt giao diện khi vi phạm bảo mật giúp tăng cường an ninh, nhưng sẽ khiến cổng bị **err-disable**, cần can thiệp thủ công để khôi phục. Hãy kích hoạt lại nó!




Tiếp theo ta sử dụng lệnh **errdisable recovery cause psecure-violation** dùng để tự động khôi phục cổng switch bị **err-disable** do vi phạm **port security**, giúp giảm yêu cầu can thiệp thủ công.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#errdisable re
Switch(config)#errdisable recovery cause pse
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#
```

Sau 5 phút (300 giây), giao diện sẽ tự động phục hồi khỏi trạng thái err-disable. Tuy nhiên, hãy đảm bảo rằng bạn đã khắc phục sự cố, nếu không, vi phạm sẽ tiếp tục xảy ra và giao diện sẽ lại rơi vào trạng thái err-disable.. Bạn có thể đẩy nhanh quá trình này bằng cách thay đổi thời gian hẹn giờ. Hãy đặt nó thành 30 giây

```
Switch(config)#err
Switch(config)#errdisable re
Switch(config)#errdisable recovery in
Switch(config)#errdisable recovery interval 30
Switch(config)#
```

Thay vì nhập thủ công địa chỉ MAC, chúng ta có thể cấu hình để switch tự động học địa chỉ MAC phục vụ cho port security bằng những lệnh sau :

```
Switch(config)#interface e0/1
Switch(config-if)#no sw
Switch(config-if)#no switchport po
Switch(config-if)#no switchport port-security mac
Switch(config-if)#no switchport port-security mac-address 00:50:79:65:68:01
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Lệnh **switchport port-security mac-address sticky** giúp switch **tự động học và ghi nhớ** địa chỉ MAC đầu tiên kết nối vào cổng, thay vì phải cấu hình thủ công. Địa chỉ MAC này sẽ được lưu trong bảng CAM và duy trì qua các lần khởi động lại (nếu lưu vào cấu hình khởi động).

Sau đó kiểm tra lại cấu hình

```
Switch(config-if)#exit
Switch(config)#exit
Switch#wr
*Mar  7 09:10:51.198: %SYS-5-CONFIG_I: Configured from console by console
Switch#wr
Building configuration...
Compressed configuration from 1122 bytes to 740 bytes[OK]
Switch#show run interface e0/1
Building configuration...

Current configuration : 273 bytes
!
interface Ethernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address 0050.7965.6801
 switchport port-security mac-address sticky aabb.cc00.3010
 switchport port-security
end
```

Việc tắt giao diện khi có vi phạm có thể là quá mức cần thiết. Có những lựa chọn khác, đây là một số tùy chọn bạn có thể sử dụng:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface e0/1
Switch(config-if)#s
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode

Switch(config-if)#switchport port-security violation
```

Giải thích

**Protect (Bảo vệ):**

- Chặn lưu lượng từ địa chỉ MAC không hợp lệ nhưng không gửi thông báo lỗi và không ghi log.
- Cổng vẫn hoạt động bình thường với các địa chỉ MAC hợp lệ.

**Restrict (Hạn chế):**

- Chặn lưu lượng từ địa chỉ MAC không hợp lệ giống chế độ protect.
- Ghi log sự kiện vi phạm và tăng bộ đếm vi phạm bảo mật (security-violation counter).
- Có thể gửi SNMP trap để quản trị viên theo dõi.

**Shutdown (Tắt cổng - chế độ mặc định):**

- Đưa cổng vào trạng thái err-disable khi có vi phạm.
- Cổng sẽ ngừng hoạt động và cần bật lại thủ công bằng lệnh shutdown và no shutdown hoặc thiết lập tự động khôi phục bằng errdisable recovery.
- Ghi log vi phạm và có thể gửi SNMP trap

Tác giả : Phan Văn Phú -PKT VNPRO