

HƯỚNG DẪN LAB

LAB 17 – Port Security

Designed by : Nguyễn Phú Thịnh

Sơ đồ LAB :



Các bước thực hiện :

- Kết nối thiết bị như sơ đồ
- Cấu hình portfast cho port F0/1
- Cấu hình tính năng port security cho các port F0/1 của switch với yêu cầu sau:
 - port tự học địa chỉ MAC
 - Cho phép tối đa 1 địa chỉ MAC / 1 port
 - Security action : shutdown
- Kiểm tra cấu hình và tính năng port security

Bước 1 : Kết nối thiết bị như sơ đồ

Bước 2 : Cấu hình port fast

Switch
Switch(config)# interface F0/1 Switch(config-if)# spanning-tree portfast

Bước 3 : cấu hình port security

Switch
<pre>Switch(config)#interface F0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport port-security Switch(config-if)#switchport port-security mac-address sticky Switch(config-if)#switchport port-security maximum 1 Switch(config-if)#switchport port-security violation shutdown</pre>

Lưu ý: nếu port không phải đang ở mode access, khi cấu hình sẽ gặp thông báo như sau :

Switch
<pre>Switch(config)#interface F0/1 Switch(config-if)#switchport port-security Command rejected: FastEthernet0/1 is a dynamic port.</pre>

Lúc này , chỉ cần chuyển port sang mode access là có thể cấu hình được :

Switch
<pre>Switch(config)#interface F0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport port-security</pre>

Bước 4: Kiểm tra cấu hình

Switch
<pre>Switch#show port-security interface F0/1 Port Security : Enabled Port Status : Secure-down Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1 Total MAC Addresses : 0 Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Last Source Address:Vlan : 0000.0000.0000:0 Security Violation Count : 0</pre>

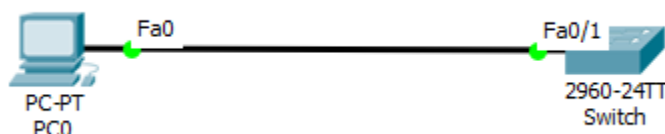
Từ output có thể thấy :

- Tính năng port security đang được bật
- Trạng thái của port là secure-down (vì chưa có PC nào cắm vào port, nên port đang down là bình thường)
- Violation : shutdown
- Số địa chỉ MAC tối đa trên port : 1
- Số địa chỉ MAC hiện tại trên port : 0
- Số địa chỉ MAC sticky hiện tại trên port : 0
- Số địa chỉ MAC static hiện tại trên port : 0
- Số lần vi phạm : 0

Lưu ý cấu hình trên port F0/1 :

Switch
<pre>Switch#show running-config interface FastEthernet0/1 switchport mode access switchport port-security switchport port-security mac-address sticky spanning-tree portfast</pre>

Bước 4: Kết nối PC1 vào port F0/1 trên switch như sơ đồ. Đặt địa chỉ IP cho PC1. Địa chỉ IP tùy ý học viên. Kiểm tra lại cấu hình



Lưu ý : phải đặt IP cho PC1 để có traffic vào port F0/1

PC0

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::250:FFF:FE8C:4C74

IPv6 Gateway:

IPv6 DNS Server:

☐ Top

Kiểm tra bảng MAC trên switch

Switch			
Switch#show mac-address-table			
Mac Address Table			

Vlan	Mac Address	Type	Ports
----	-----	-----	----
1	0050.0f8c.4c74	STATIC	Fa0/1

Xem lại các thông số Port Security

Switch

```
Switch#show port-security interface F0/1
Port Security          : Enabled
Port Status            : Secure-up
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 : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 0050.0F8C.4C74:1
Security Violation Count : 0
```

Từ output có thể thấy :

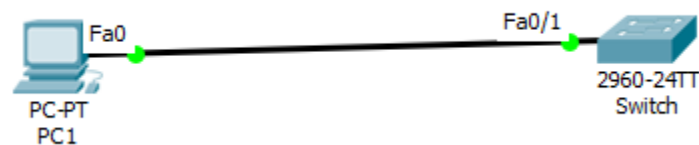
- Tính năng port security đang được bật
- Trạng thái của port là secure-up
- Violation : shutdown
- Số địa chỉ MAC tối đa trên port : 1
- Số địa chỉ MAC hiện tại trên port : 1
- Số địa chỉ MAC sticky hiện tại trên port : 1
- Số địa chỉ MAC static hiện tại trên port : 0
- Số lần vi phạm : 0

Xem lại cấu hình trên port F0/1

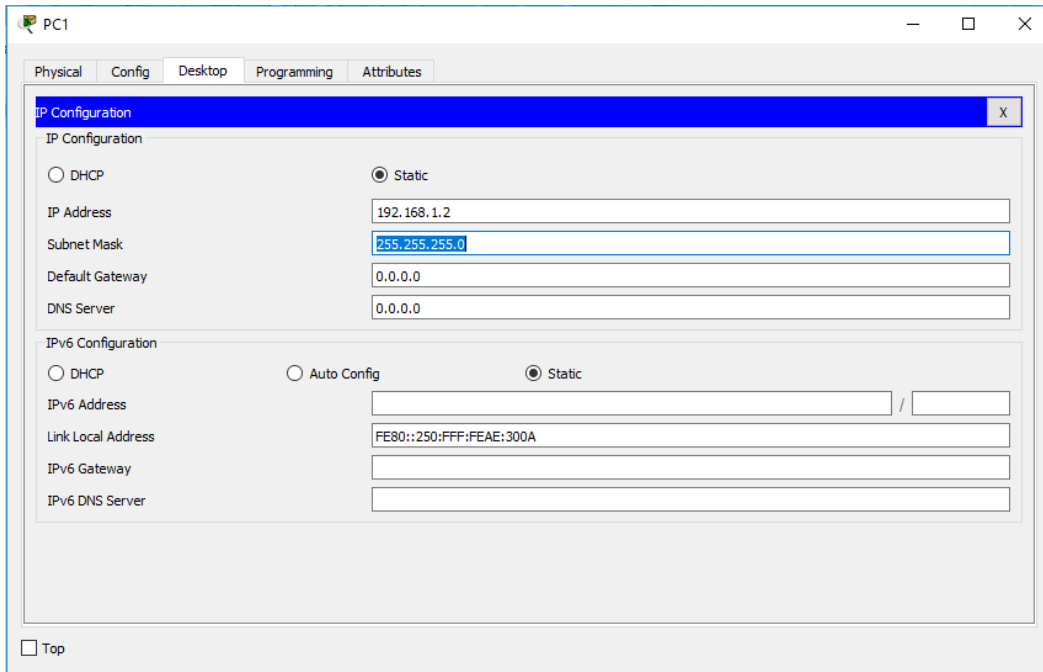
Switch
<pre>Switch#show running-config interface FastEthernet0/1 switchport mode access switchport port-security switchport port-security mac-address sticky switchport port-security mac-address sticky 0050.0F8C.4C74 spanning-tree portfast</pre>

Trong cấu hình, đã xuất hiện địa chỉ MAC của PC0, cho thấy, sticky MAC được lưu vào file configure. Nếu lưu lại cấu hình, MAC này sẽ không bị mất khi reload switch

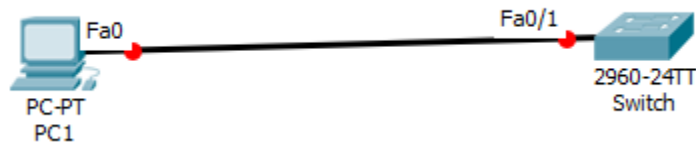
Bước 5: Rút PC0 ra, sau đó cắm một PC1 khác vào port F0/1 của switch.



Đặt IP cho PC1



Đèn trên port F0/1 lúc này là màu đỏ. Nếu làm trên thiết bị thật, port F0/1 lúc này sẽ bị tắt



Kiểm tra thông số Port Security

Switch	
Switch#show port-security interface F0/1	
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	: 0
Sticky MAC Addresses	: 1
Last Source Address:Vlan	: 0050.0FAE.300A:1
Security Violation Count	: 1

Từ output có thể thấy :

- Tính năng port security đang được bật
- Trạng thái của port là secure-shutdown (do port bị shutdown vì vi phạm)
- Violation : shutdown
- Số địa chỉ MAC tối đa trên port : 1
- Số địa chỉ MAC hiện tại trên port : 1

- Số địa chỉ MAC sticky hiện tại trên port :1
- Số địa chỉ MAC static hiện tại trên port : 0
- Số lần vi phạm : 1

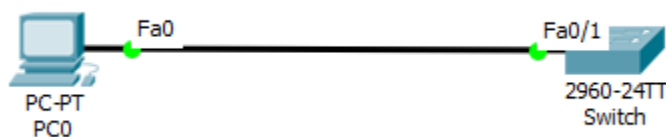
Kiểm tra trạng thái port F0/1

Switch
<pre>Switch#show interface F0/1 FastEthernet0/1 is down, line protocol is down (err-disabled) Hardware is Lance, address is 00e0.a370.b801 (bia 00e0.a370.b801) BW 100000 Kbit, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full-duplex, 100Mb/s input flow-control is off, output flow-control is off ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:08, output 00:00:05, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue :0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 956 packets input, 193351 bytes, 0 no buffer Received 956 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 0 watchdog, 0 multicast, 0 pause input 0 input packets with dribble condition detected 2357 packets output, 263570 bytes, 0 underruns 0 output errors, 0 collisions, 10 interface resets 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier 0 output buffer failures, 0 output buffers swapped out</pre>

Chính xác thì port F0/1 bị đưa vào trạng thái Error Disabled.

Bước 6 : Bring up port F0/1.

Rút PC1 ra khỏi port F0/1 , cắm PC0 lại (trả lại trạng thái không vi phạm)



Bring up port F0/1 bằng cách shutdown/no shutdown port

Switch
<pre>Switch(config)#interface F0/1 Switch(config-if)#shutdown Switch(config-if)#no shutdown</pre>

Port đã up trở lại

Switch
<pre>Switch#show interface F0/1</pre>

```
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 00e0.a370.b801 (bia 00e0.a370.b801)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

-Hết-