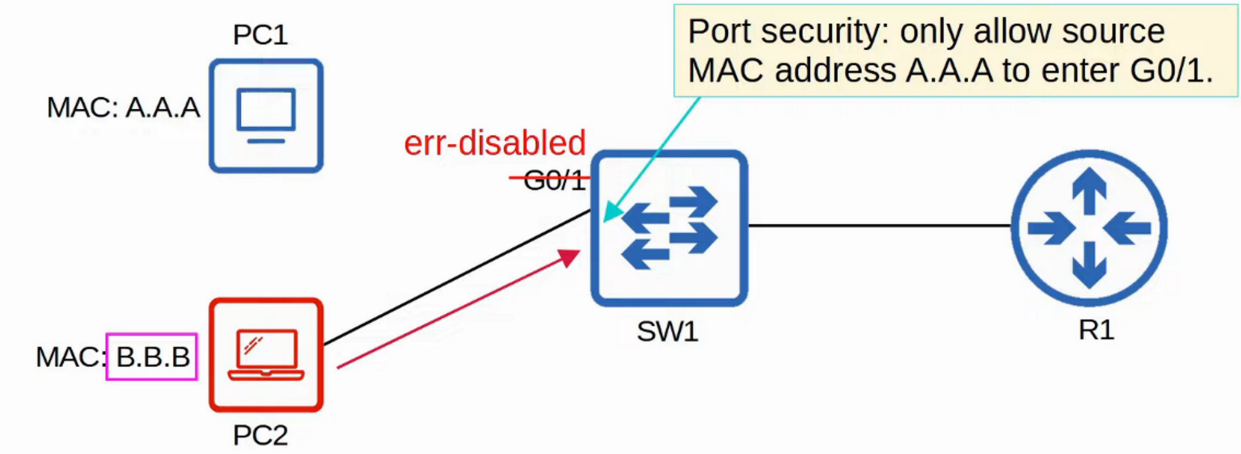
Saturday, August 16, 2025 8:40 PM

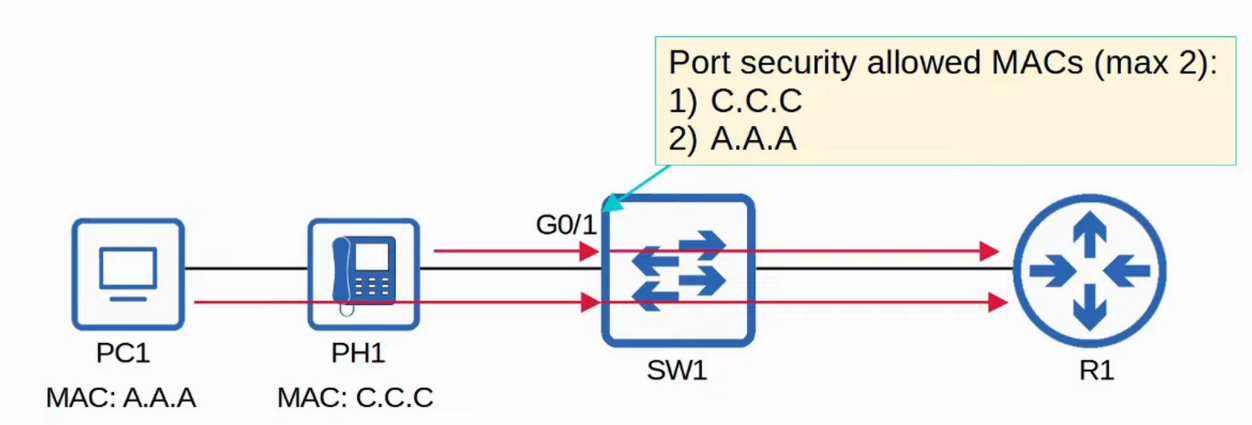
PORT SECURITY

INTRO TO PORT SECURITY

- PORT SECURITY is a security feature of Cisco S WITCHES
- It allows you to control WHICH SOURCE MAC ADDRESS(ES) are allowed to enter the SWITCHPORT
- If an unauthorized SOURCE MAC ADDRESS enters the PORT, an ACTION will be TAKEN
  - The DEFAULT action is to place the INTERFACE in an “err-disabled” state



- When you enable PORT SECURITY on an INTERFACE with the DEFAULT settings, one MAC ADDRESS is allowed
  - You can configure the ALLOWED MAC ADDRESS manually
  - If you DO NOT configure it manually, the SWITCH will allow the first SOURCE MAC ADDRESS that enters the INTERFACE
- You can CHANGE the MAXIMUM number of MAC ADDRESSES allowed
- A COMBINATION of manually configured MAC ADDRESSES and DYNAMICALLY LEARNED ADDRESSES is possible

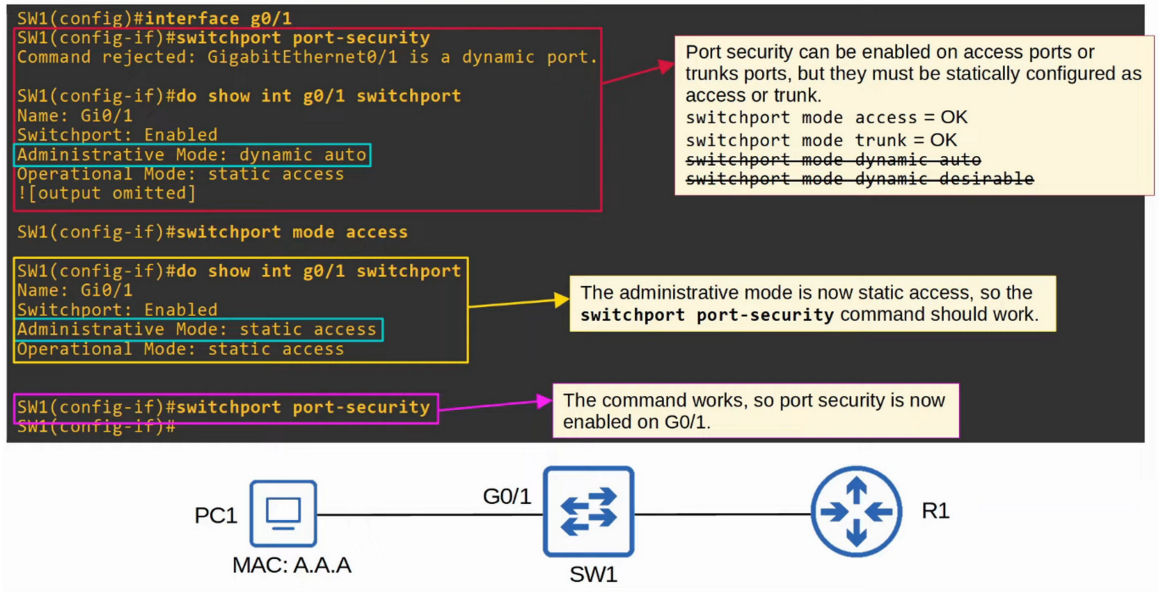


WHY USE PORT SECURITY?

- PORT SECURITY allows NETWORK admins to control which DEVICES are allowed to access the NETWORK

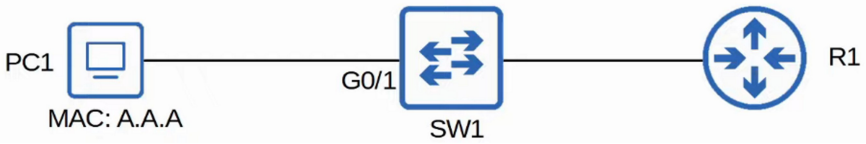
- However, MAC ADDRESS SPOOFING is a simple task
  - It is easy to configure a DEVICE to send FRAMES with a different SOURCE MAC ADDRESS
- Rather than manually specifying the MAC ADDRESSES allowed on each PORT, PORT SECURITY'S ability to limit the number of MAC ADDRESSES allowed on an INTERFACE is more useful
- Think of the DHCP STARVATION ATTACK (DAY 48 LAB video)
  - The ATTACKER spoofed thousands of fake MAC ADDRESSES
  - The DHCP SERVER assigned IP ADDRESSES to these fake MAC ADDRESSES, exhausting the DHCP POOL
  - The SWITCH'S MAC ADDRESS table can also become full due to such an attack
- Limiting the NUMBER of MAC ADDRESSES on an INTERFACE can protect against those attacks

ENABLING PORT SECURITY

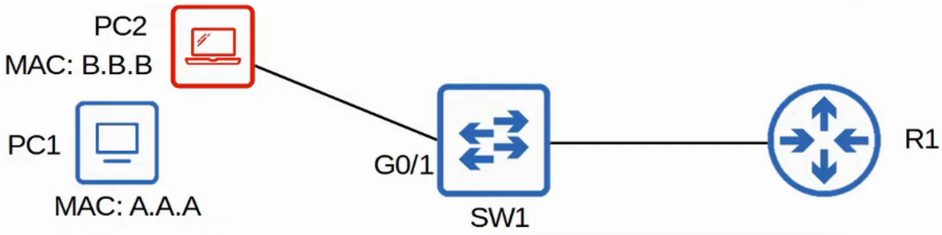


show port-security interface

```
SW1#show port-security interface g0/1
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       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```




```
SW1#show port-security interface g0/1
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000b.000b.000b:1
Security Violation Count   : 1
```



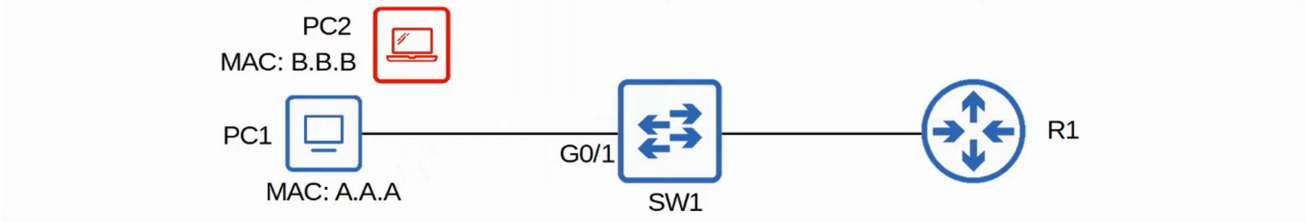

```
SW1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        connected    1            auto   auto unknown
Gi0/1                        err-disabled 1            auto   auto unknown
```

RE-ENABLING AN INTERFACE (MANUALLY)

```
SW1(config)#interface g0/1
SW1(config-if)#shutdown
SW1(config-if)#no shutdown
```

1) Disconnect the unauthorized device
2) **shutdown** and then **no shutdown** the interface

```
SW1#show port-security interface g0/1
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```



RE-ENABLING AN INTERFACE (ERR-DISABLE RECOVERY)

```
SW1#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
![output omitted due to length]
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

Every 5 minutes (by default), all err-disabled interfaces will be re-enabled **if err-disable recovery has been enabled for the cause of the interface's disablement.**

```
SW1(config)#errdisable recovery cause psecure-violation

SW1(config)#errdisable recovery interval 180


SW1#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
![output omitted due to length]
psecure-violation            Enabled
![output omitted due to length]

Timer interval: 180 seconds

Interfaces that will be enabled at the next timeout:

Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Gi0/1          psecure-violation          149
```

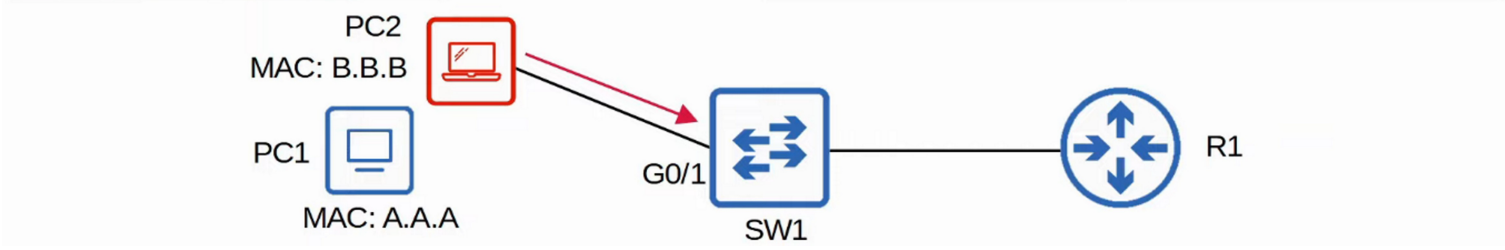
ErrDisable Recovery is useless if you don't remove the device that caused the interface to enter the err-disabled state!

VIOLATION MODES

- There are THREE DIFFERENT VIOLATION MODES that determine what the SWITCH will do if an unauthorized FRAME enters an INTERFACE configured with PORT SECURITY
  - **SHUTDOWN**
    - Effectively **shuts down the PORT** by placing it in an **'err-disabled`** state
    - Generates a **SYSLOG and / or SNMP message** when the INTERFACE is **'disabled'**
    - **The VIOLATION counter is set to 1 when the INTERFACE is 'disabled'**
  - **RESTRICT**
    - The SWITCH discards traffic from unauthorized MAC ADDRESSES
    - The INTERFACE is NOT disabled
    - **Generates a SYSLOG and / or SNMP message each time an unauthorized MAC is detected**
    - **The VIOLATION counter is incremented by 1 for each unauthorized FRAME**
  - **PROTECT**
    - **The SWITCH discards traffic from unauthorized MAC ADDRESSES**
    - **The INTERFACE is NOT disabled**
    - **It does NOT generate a SYSLOG / SNMP message for unauthorized traffic**
    - **It does NOT increment the VIOLATION counter**

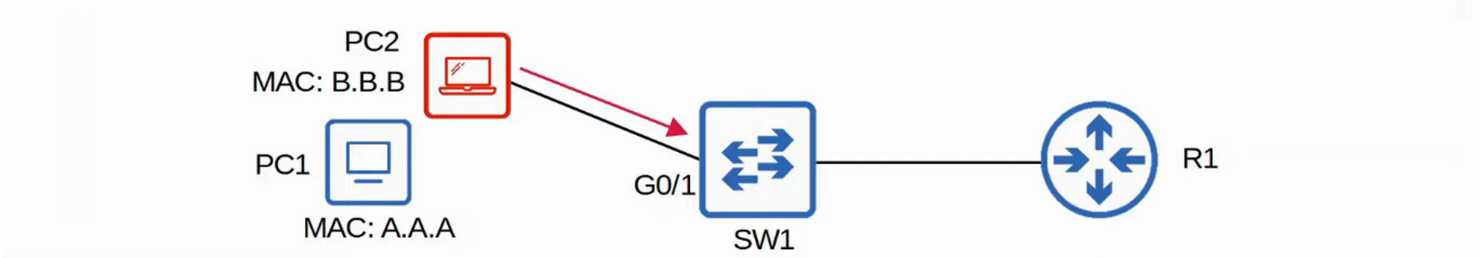
VIOLATION MODE - RESTRICT

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000a.000a.000a
SW1(config-if)#switchport port-security violation restrict

*May 23 22:54:09.951: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000b.000b.000b on port GigabitEthernet0/1.

SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
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   : 000b.000b.000b:1
Security Violation Count   : 12
```



VIOLATION MODE - PROTECT

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000a.000a.000a
SW1(config-if)#switchport port-security violation protect


SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
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   : 000b.000b.000b:1
Security Violation Count   : 0
```



SECURE MAC ADDRESS AGING

```
SW1#show port-security interface g0/1
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       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

- By DEFAULT, SECURE MAC ADDRESSES will not 'age out' (Aging Time : 0 mins)
  - Can be configured with switchport port-security aging time *minutes*
- The DEFAULT Aging Type is ABSOLUTE
  - ABSOLUTE
    - After the SECURE MAC ADDRESS is learned, the AGING TIMER starts and the MAC is removed after the TIMER expires, even if the SWITCH continues receiving FRAMES from that SOURCE MAC ADDRESS.
  - INACTIVITY
    - After the SECURE MAC ADDRESS is learned, the AGING TIMER starts but is RESET every time a FRAME from that SOURCE MAC ADDRESS is received on the INTERFACE
      - Aging type is configured with: switchport port-security aging type {absolute | inactivity}

- Secure Static MAC AGING (address configured with switchport port-security mac-address x.x.x) is DISABLED by DEFAULT

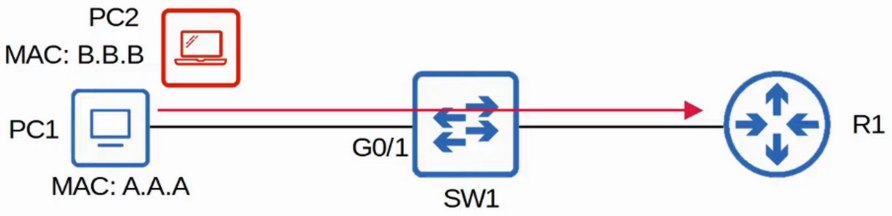
```
SW1(config-if)#switchport port-security aging time 30
SW1(config-if)#switchport port-security aging type inactivity
SW1(config-if)#switchport port-security aging static


SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 30 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0

SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Gi0/1              1           1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

STICKY SECURE MAC ADDRESSES

- 'STICKY' SECURE MAC ADDRESS learning can be enabled with the following command:
  - SW(config-if)# **switchport port-security mac-address sticky**
- When enabled, dynamically-learned SECURE MAC ADDRESSES will be added to the running configuration, like this:
  - switchport port-security mac-address sticky *mac-address*
- The 'STICKY' SECURE MAC ADDRESSES will NEVER age out
  - You need to SAVE the running-config to startup-config to make them TRULY permanent (or else they will not be kept if the SWITCH restarts)
- When you issue the switchport port-security mac-address sticky command, all current dynamically-learned secure MAC addresses will be converted to STICKY SECURE MAC ADDRESSES
- If you issue the no switchport port-security mac-address sticky command, all current STICKY SECURE MAC ADDRESSES will be converted to regular dynamically-learned SECURE MAC ADDRESSES

Sticky Secure MAC Addresses

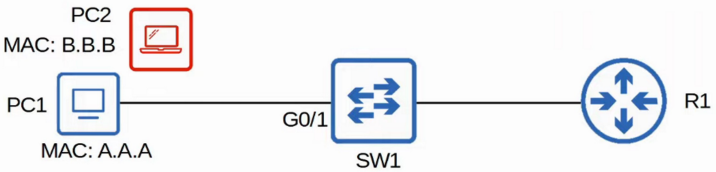
```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#do show running-config interface g0/1
!
interface GigabitEthernet0/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000a.000a.000a
 switchport port-security
 negotiation auto
```



MAC ADDRESS TABLE

- SECURE MAC ADDRESSES will be added to the MAC ADDRESS TABLE like any other MAC ADDRESS
  - STICKY and STATIC SECURE MAC ADDRESSES will have a type of STATIC
  - Dynamically-Learned SECURE MAC ADDRESSES will have a type of DYNAMIC
  - You can view all SECURE MAC ADDRESSES with show mac address-table secure

```
SW1#show mac address-table secure
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000a.000a.000a    STATIC      Gi0/1
Total Mac Addresses for this criterion: 1
```



COMMAND REVIEW

```
SW1# show mac address-table secure
SW1# show port-security
SW1# show port-security interface interface
SW1# show errdisable recovery
SW1(config)# errdisable recovery cause psecure-violation
SW1(config)# errdisable recovery interval seconds
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security mac-address mac-address
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation {shutdown | restrict | protect}
SW1(config-if)# switchport port-security aging time minutes
SW1(config-if)# switchport port-security aging type {absolute | inactivity}
SW1(config-if)# switchport port-security aging static
```