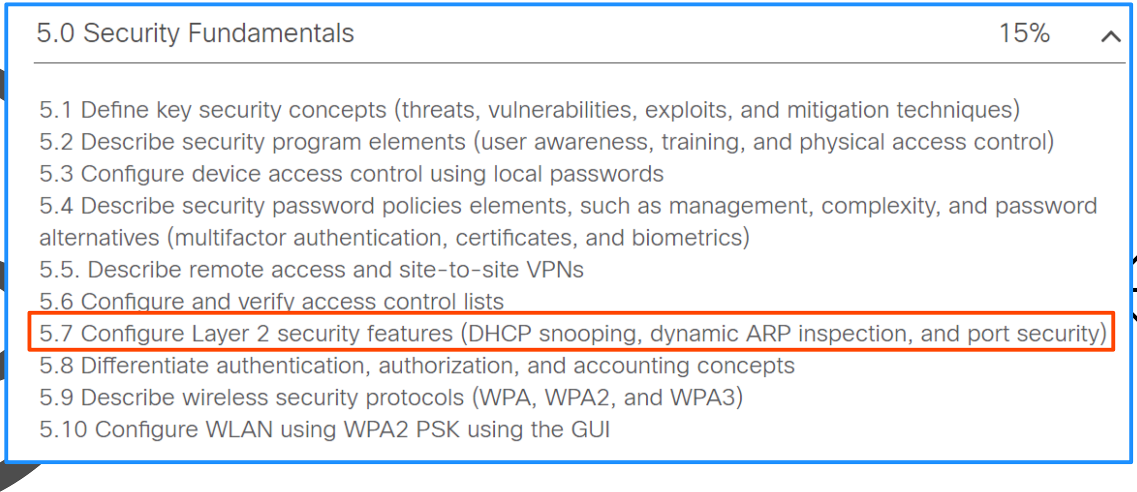
JEREMY'S IT LAB

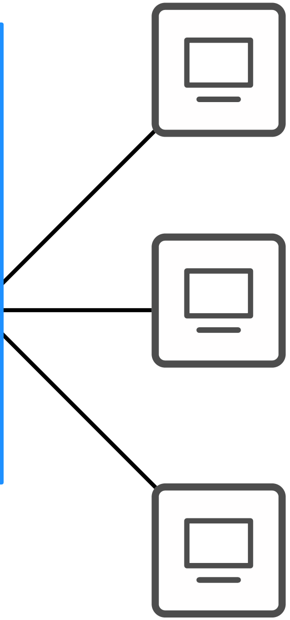
CCNA Day 49

Port Security



5.0 Security Fundamentals 15%

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
5.2 Describe security program elements (user awareness, training, and physical access control)
5.3 Configure device access control using local passwords
5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5.5. Describe remote access and site-to-site VPNs
5.6 Configure and verify access control lists
5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
5.8 Differentiate authentication, authorization, and accounting concepts
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
5.10 Configure WLAN using WPA2 PSK using the GUI

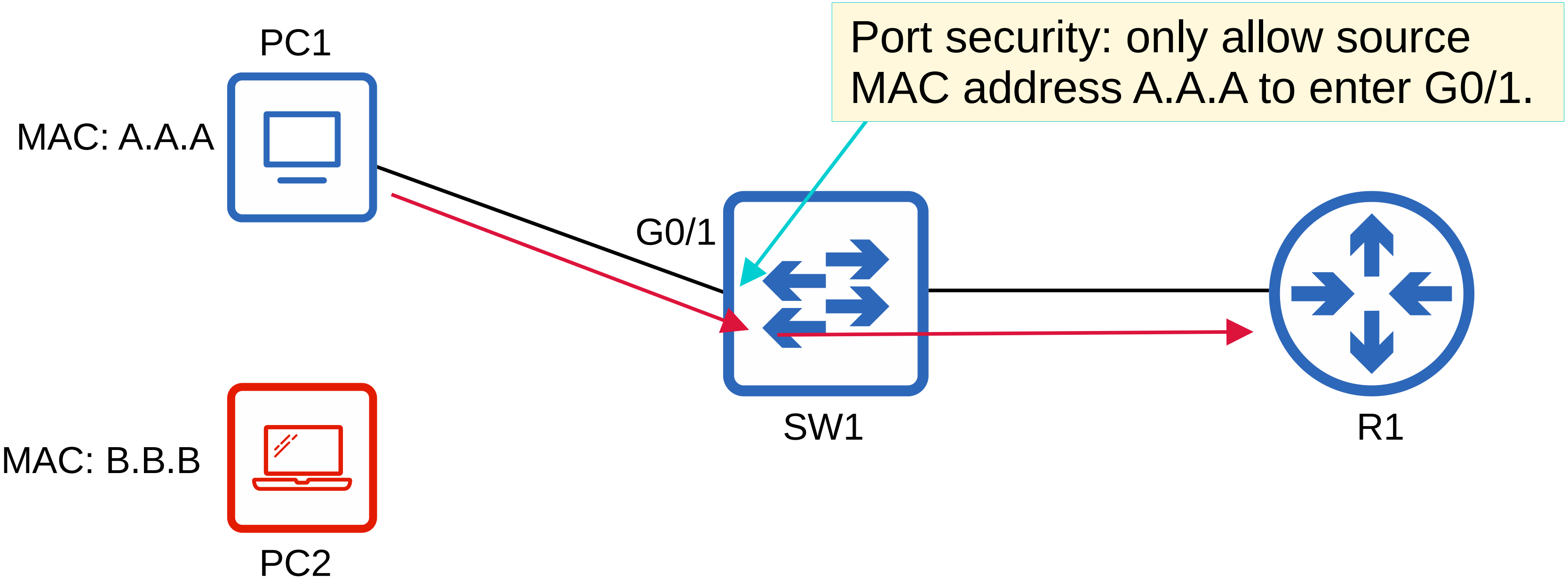


Things we'll cover

- Intro to port security
- Why use port security?
- Port security configuration

Port Security

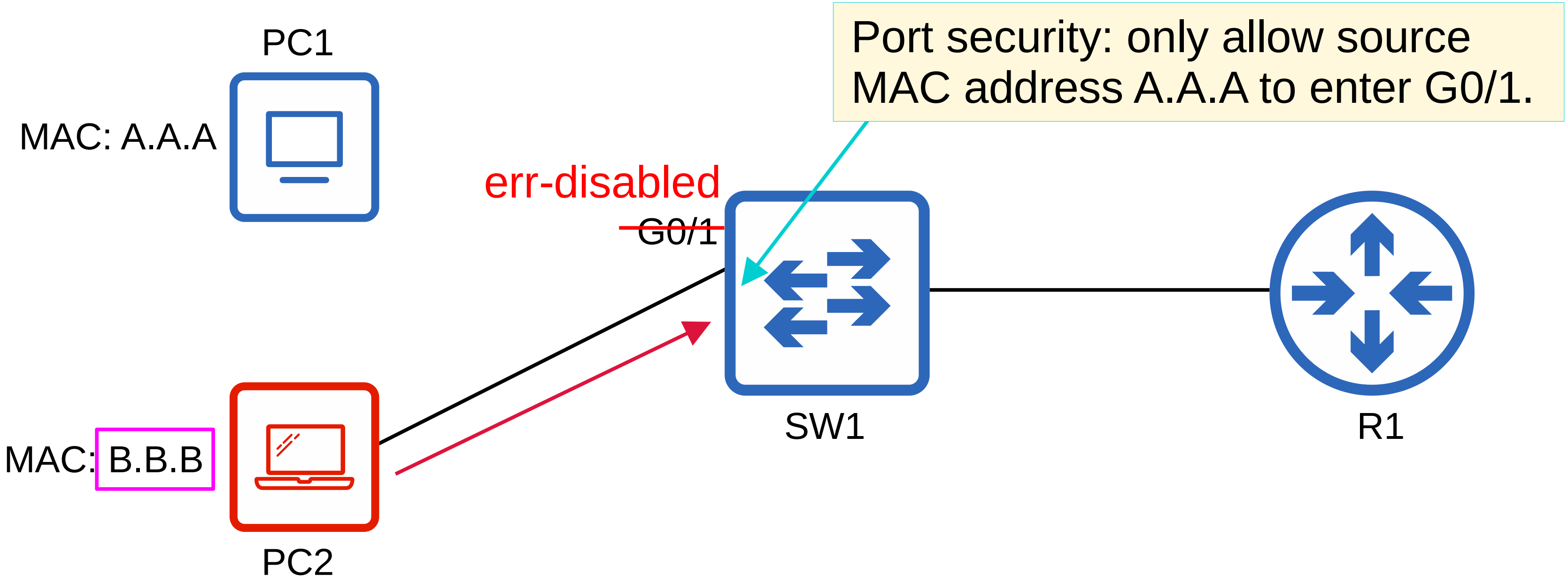
- Port security is a security feature of Cisco switches.
- It allows you to control which source MAC address(es) are allowed to enter the switchport.
- If an unauthorized source MAC address enters the port, an action will be taken.
  → The default action is to place the interface in an 'err-disabled' state.



Port security: only allow source MAC address A.A.A to enter G0/1.

Port Security

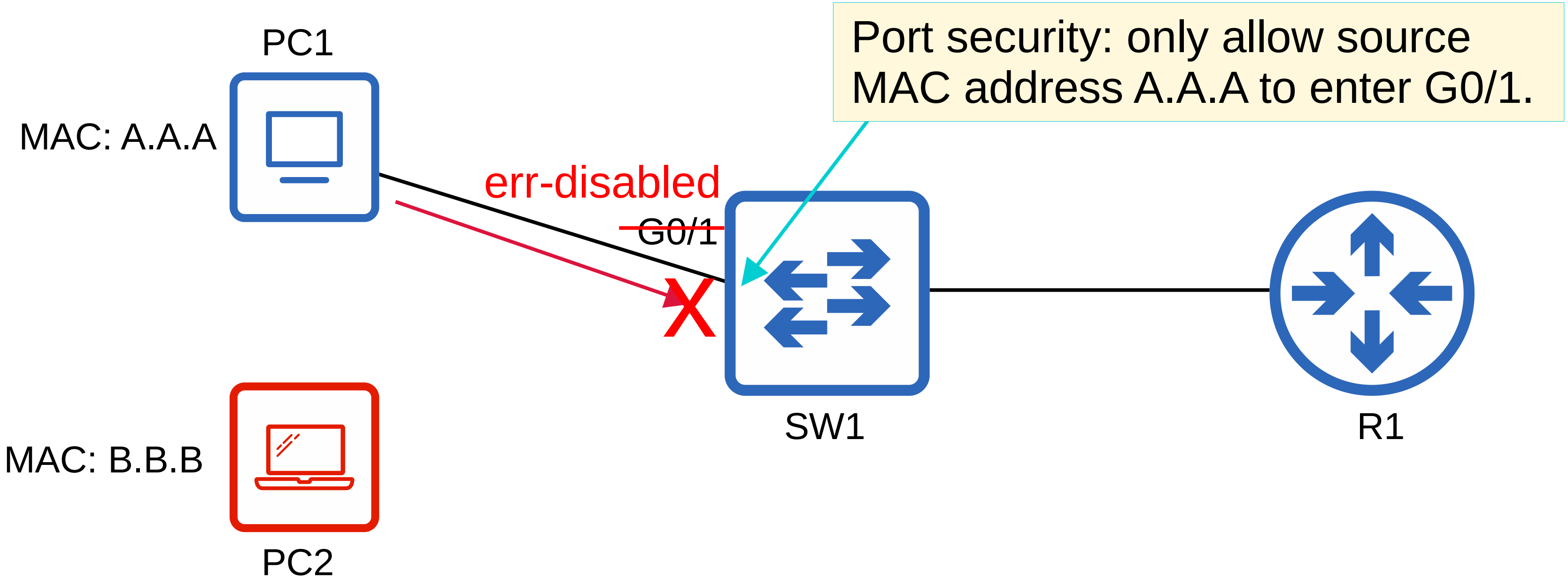
- Port security is a security feature of Cisco switches.
- It allows you to control which source MAC address(es) are allowed to enter the switchport.
- If an unauthorized source MAC address enters the port, an action will be taken.
  → The default action is to place the interface in an 'err-disabled' state.



Port security: only allow source MAC address A.A.A to enter G0/1.

Port Security

- Port security is a security feature of Cisco switches.
- 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.

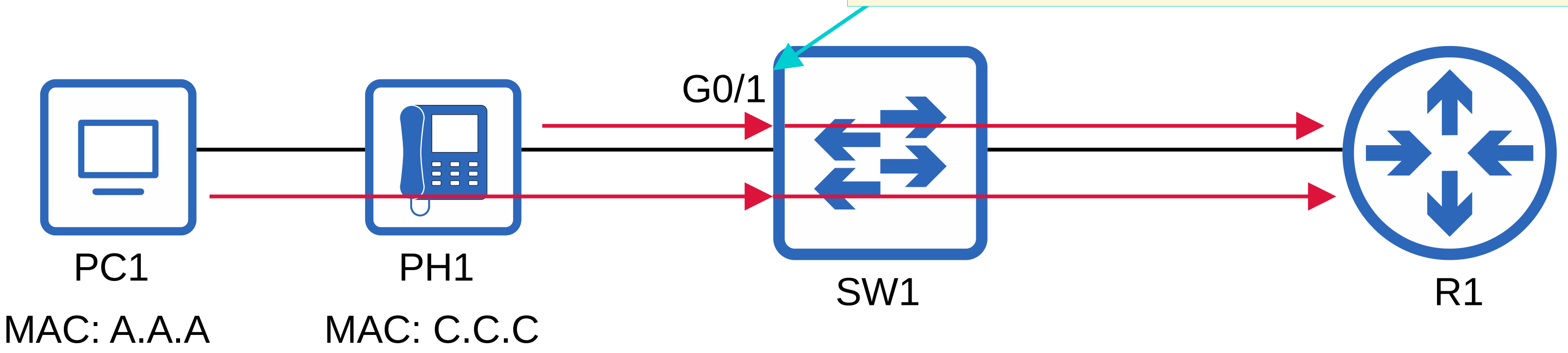


Port security: only allow source MAC address A.A.A to enter G0/1.

Port Security

- 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 don't 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.

Port security allowed MACs (max 2):
1) C.C.C (manually configured)
2) A.A.A (dynamically learned)



Why 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's 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 carried out in the 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

```
SW1(config)#interface g0/1
SW1(config-if)#switchport port-security
Command rejected: GigabitEthernet0/1 is a dynamic port.

SW1(config-if)#do show int g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
![output omitted]
```

Port security can be enabled on access ports or trunks ports, but they must be statically configured as access or trunk.

`switchport mode access` = OK

`switchport mode trunk` = OK

~~`switchport mode dynamic auto`~~

~~`switchport mode dynamic desirable`~~

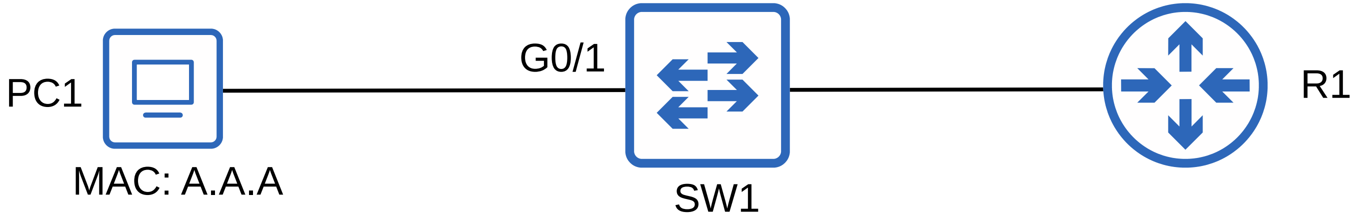
```
SW1(config-if)#switchport mode access
```

```
SW1(config-if)#do show int g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

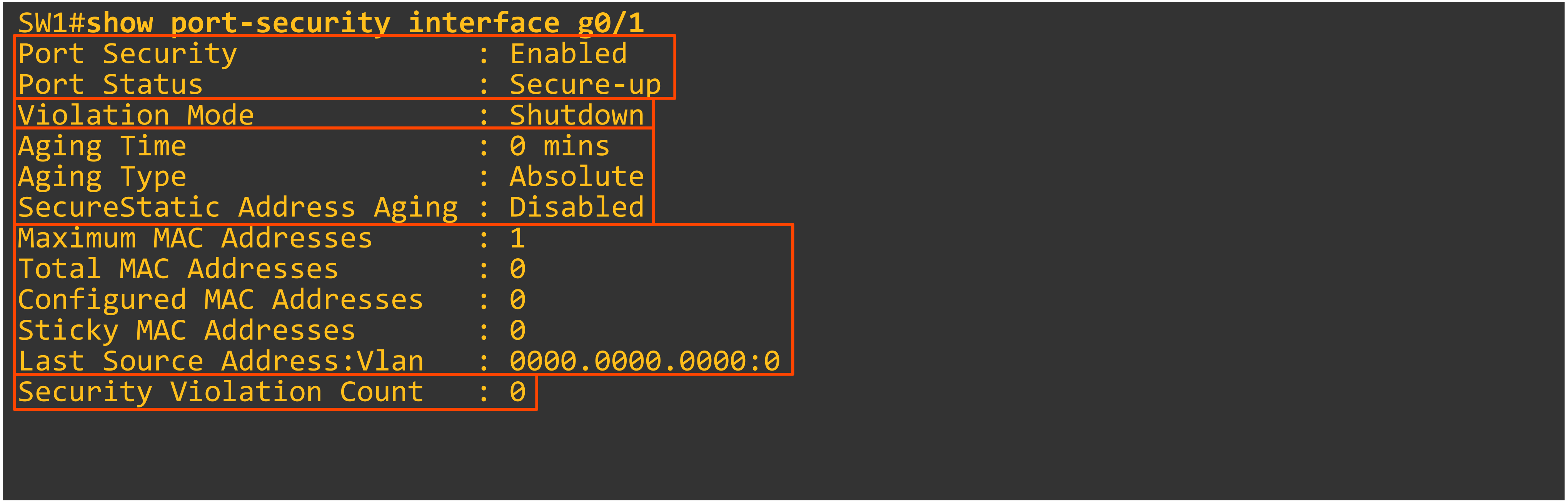
The administrative mode is now static access, so the **`switchport port-security`** command should work.

```
SW1(config-if)#switchport port-security
SW1(config-if)#
```

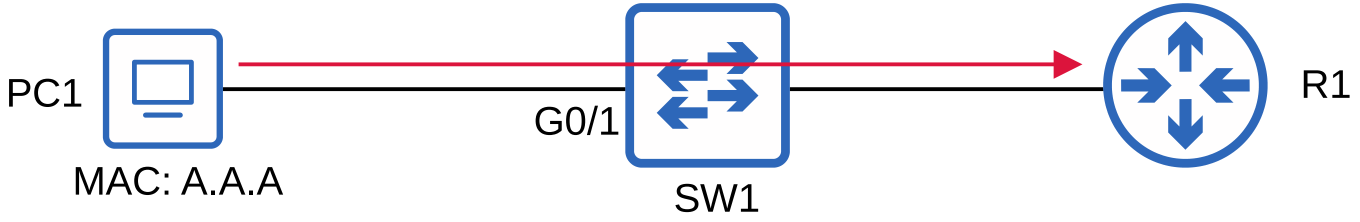
The command works, so port security is now enabled on G0/1.



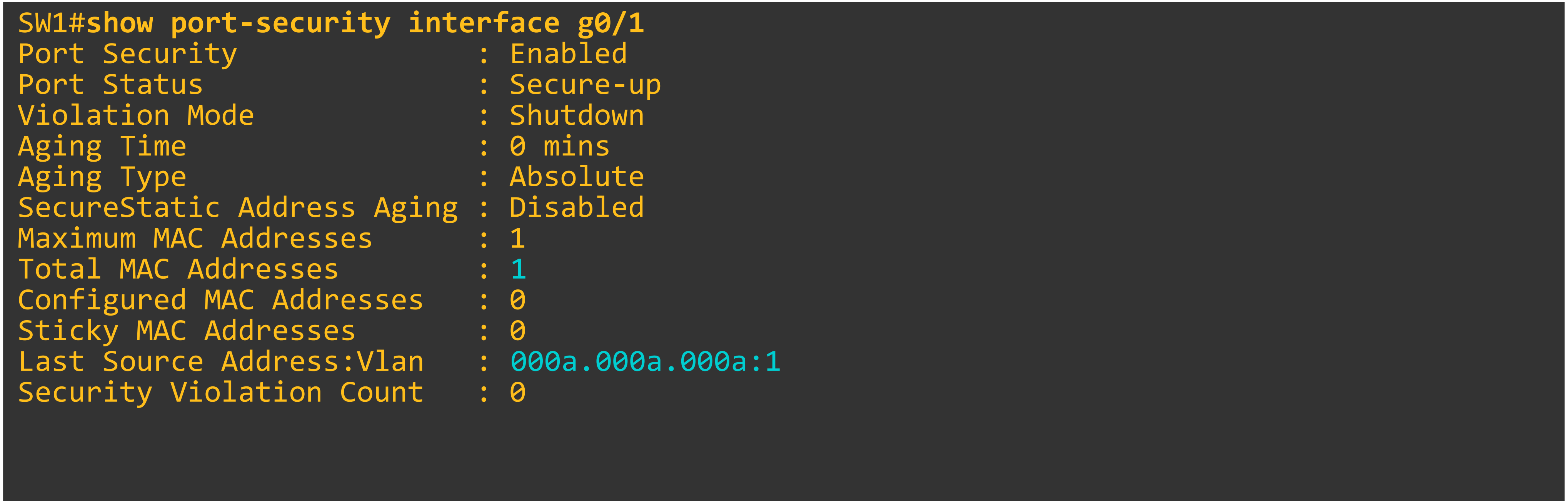
show port-security interface



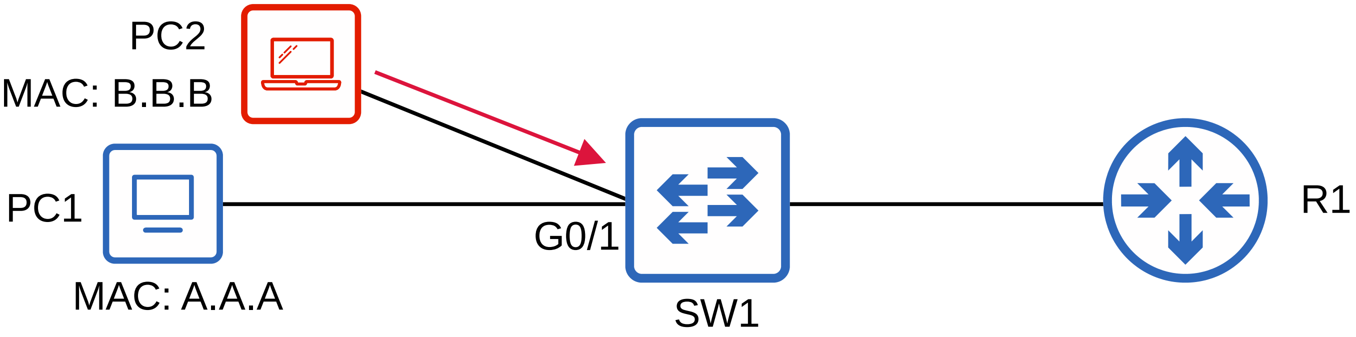
```
SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```



show port-security interface



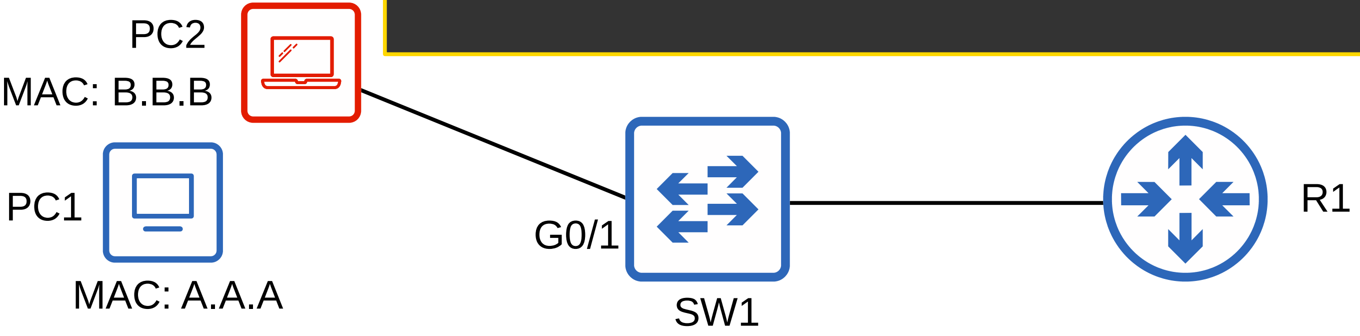
```
SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total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



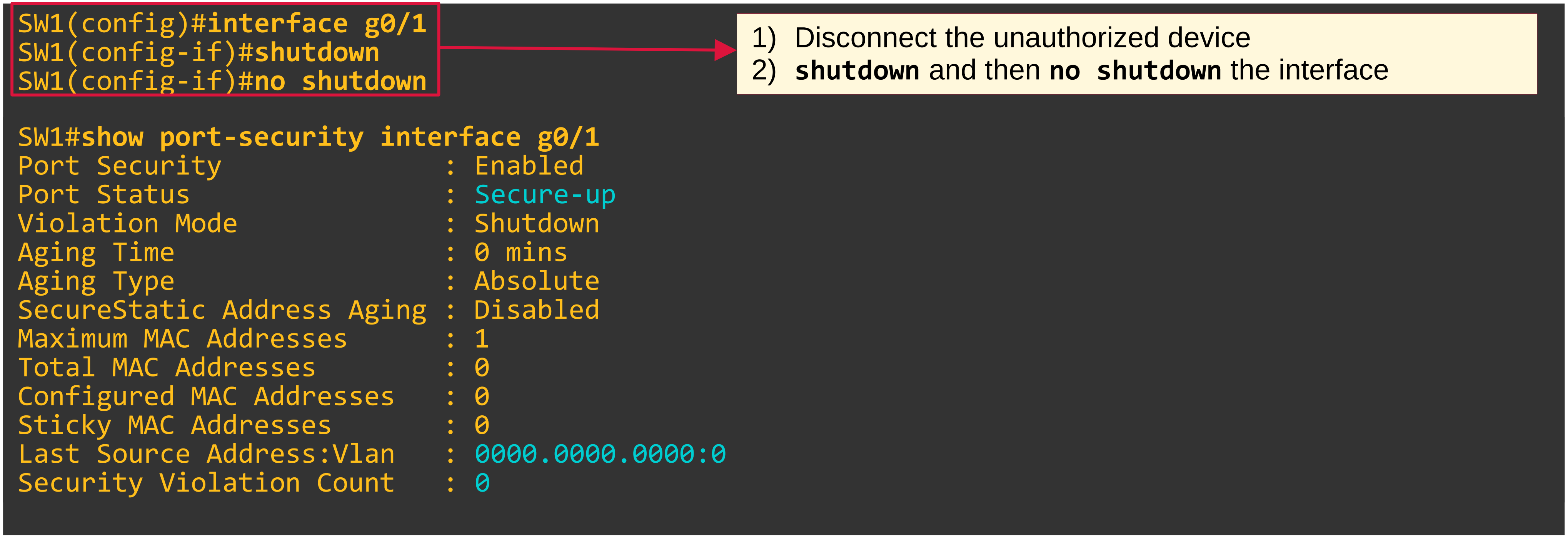
show port-security interface

```
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
```

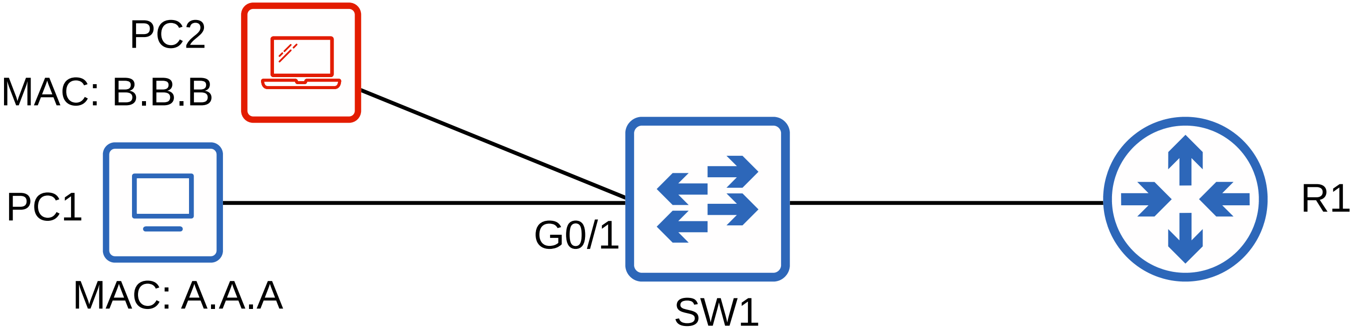


Re-enabling an interface (manually)



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

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
```

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

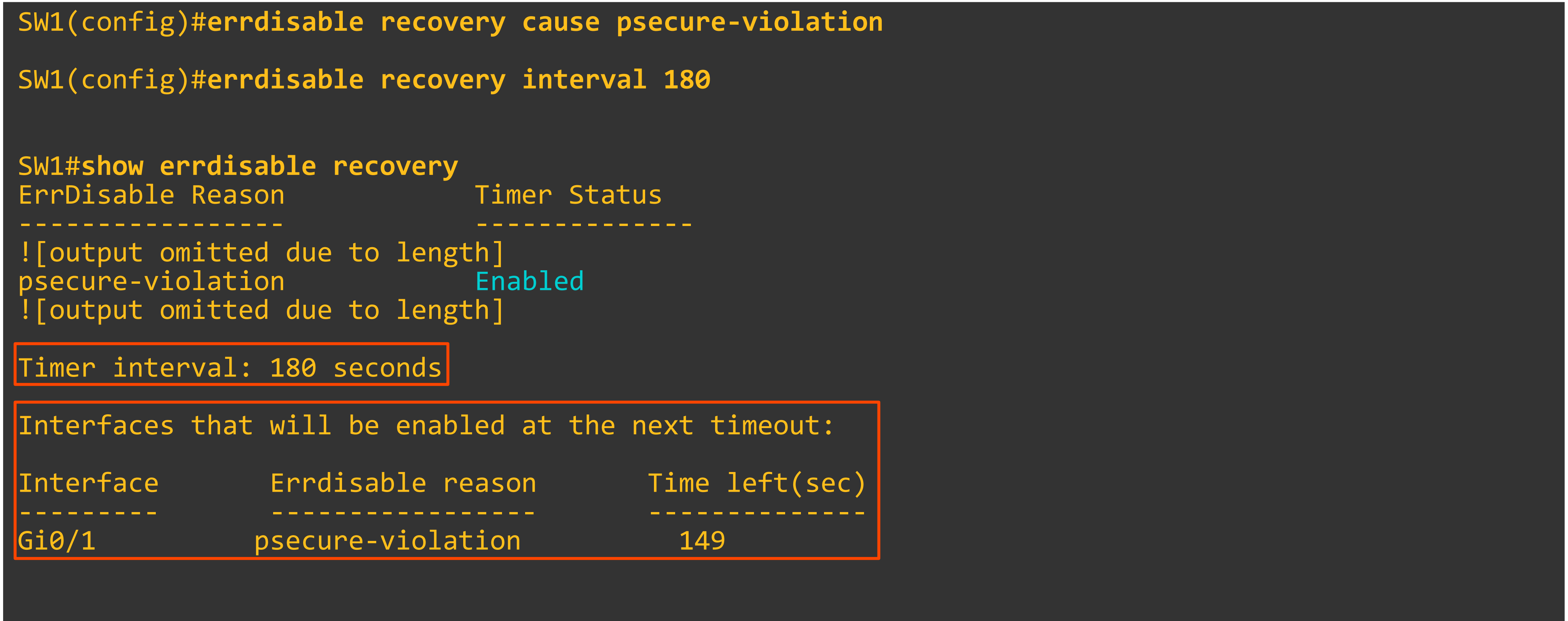


Re-enabling an interface (ErrDisable Recovery)

```
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.**

Re-enabling an interface (ErrDisable Recovery)



```
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.

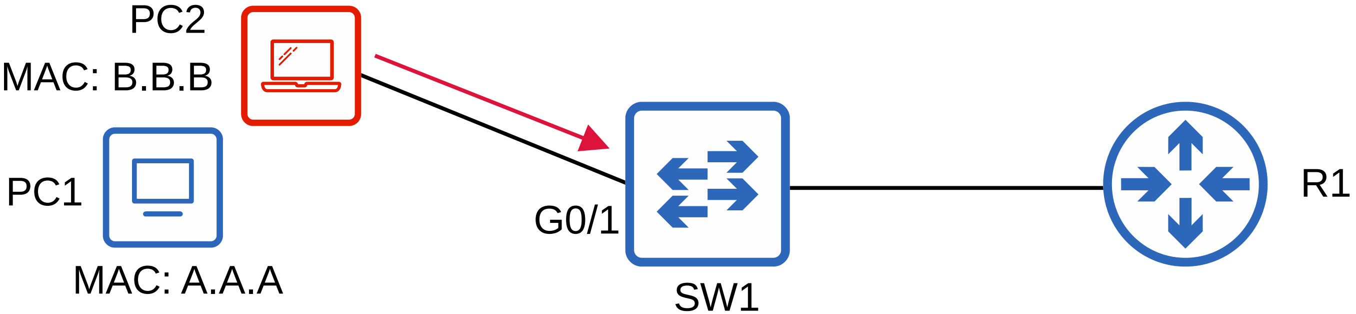
- **Shutdown**
  - → Effectively shuts down the port by placing it in an err-disabled state.
  - → Generates a Syslog and/or SNMP message when the interface is disabled.
  - → The violation counter is set to 1 when the interface is disabled.

- **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.

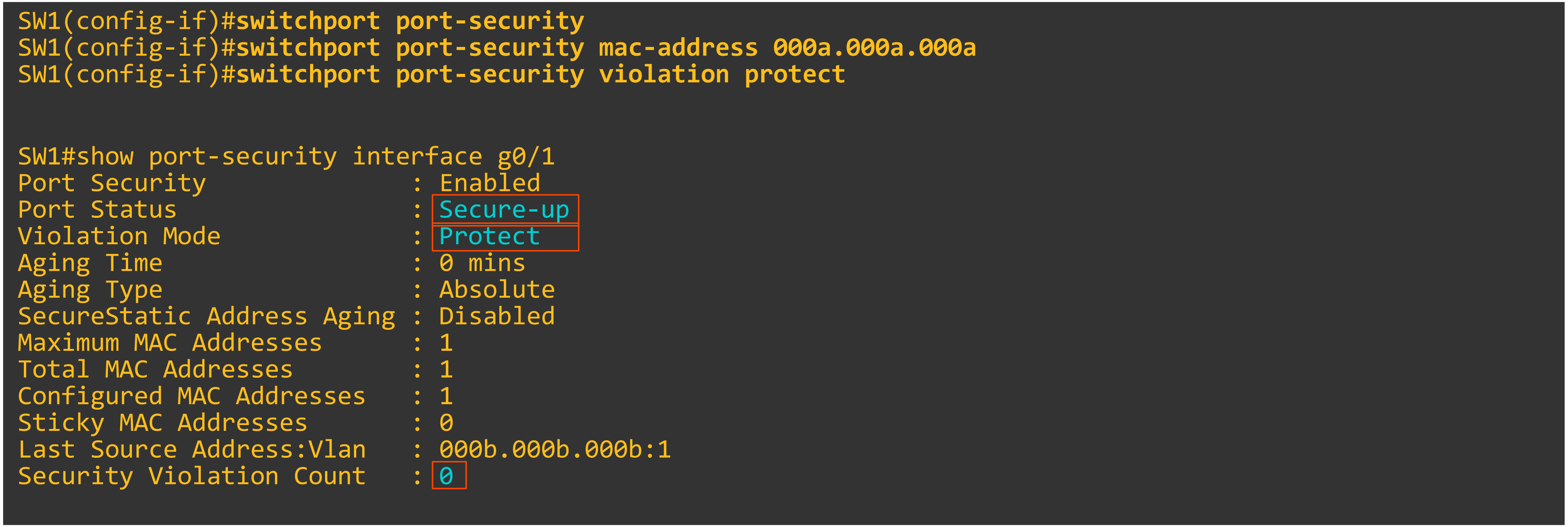
- **Protect**
  - → The switch discards traffic from unauthorized MAC addresses.
  - → The interface is NOT disabled.
  - → It does NOT generate Syslog/SNMP messages for unauthorized traffic.
  - → It does NOT increment the violation counter.

Violation mode: Restrict

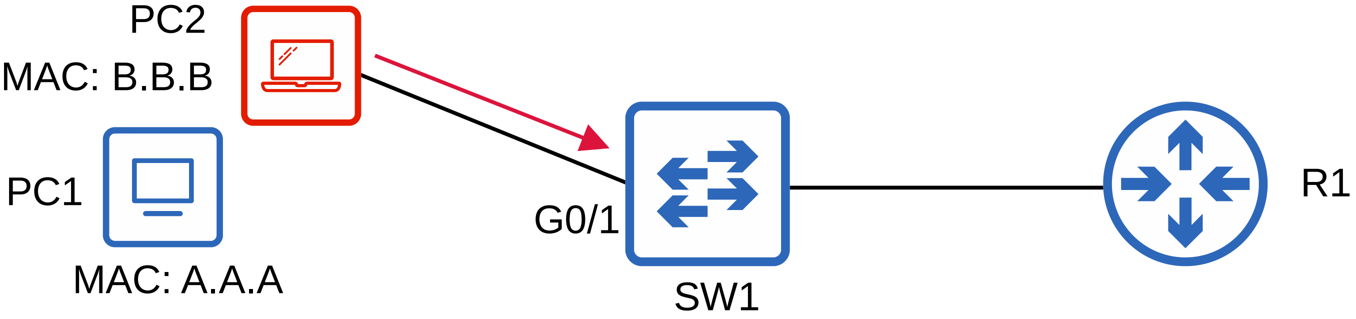
```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000a.000a.000a
SW1(config-if)#switchport port-security violation restrict

*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
```



Violation Modes

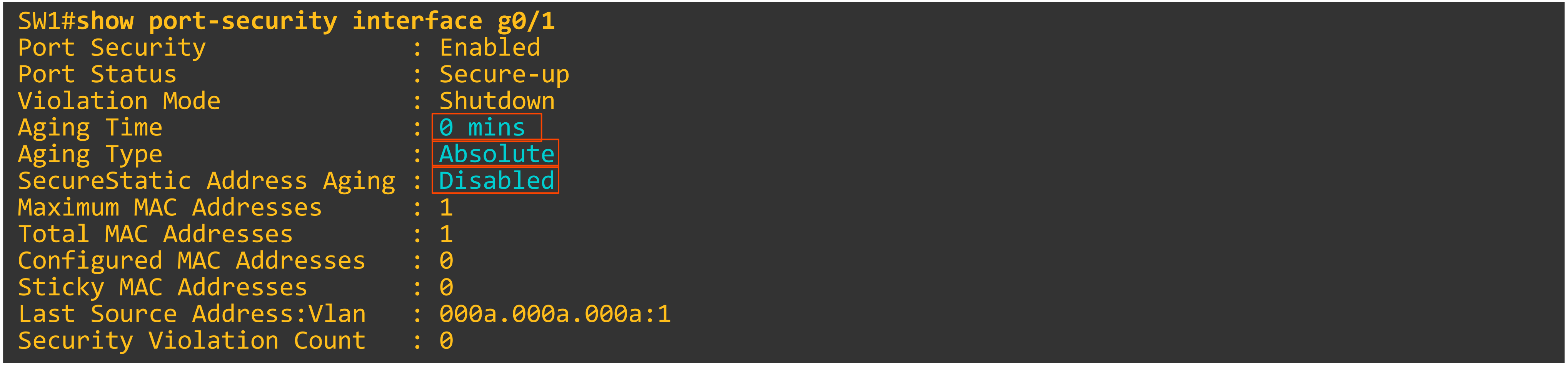
There are three different violation modes that determine what the switch will do if an unauthorized frame enters an interface configured with port security.

- **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 Syslog/SNMP messages for unauthorized traffic.
  - → It does NOT increment the violation counter.

Secure MAC address aging



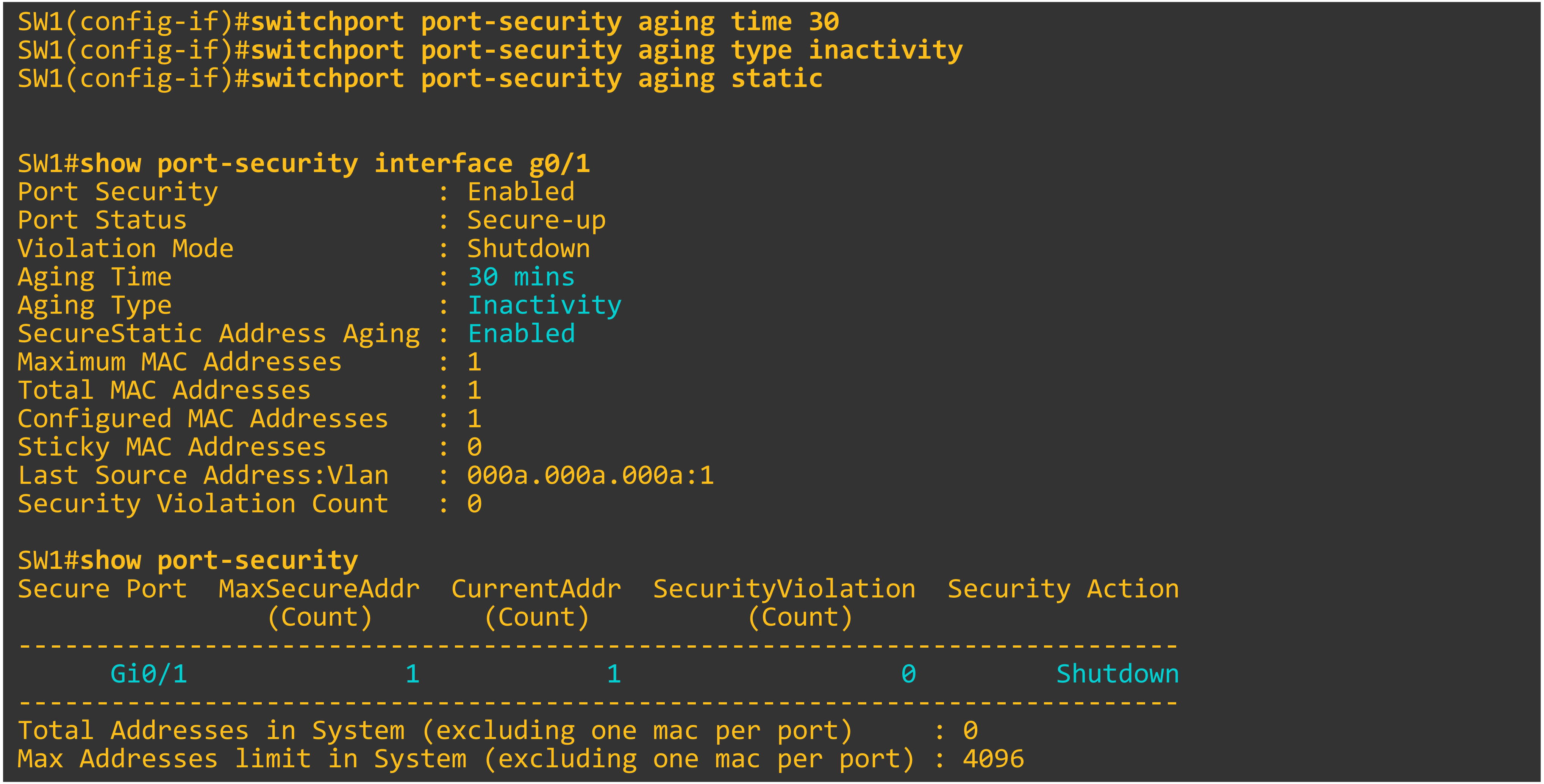
```
SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total 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 (addresses configured with **`switchport port-security mac-address`** *`x.x.x`*) is disabled by default.
  → Can be enabled with **`switchport port-security aging static`**

Secure MAC address aging



```
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:
  `SW1(config-if)#` **`switchport port-security mac-address sticky`**

- When enabled, dynamically-learned secure MAC addresses will be added to the running config like this:
  `switchport port-security mac-address sticky` *`mac-address`*

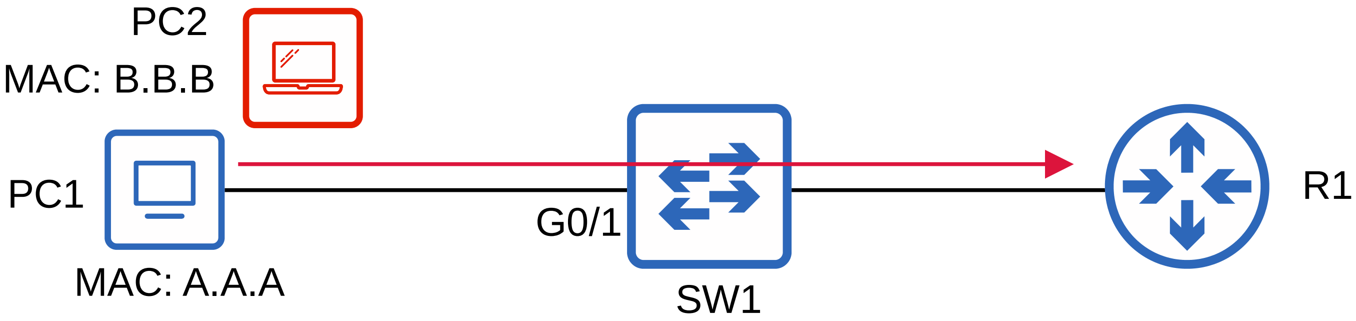
- The 'sticky' secure MAC addresses will <u>never</u> age out.
  → You need to save the running-config to the startup-config to make them truly permanent (or else they will not be kept if the switch restarts)

- 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.

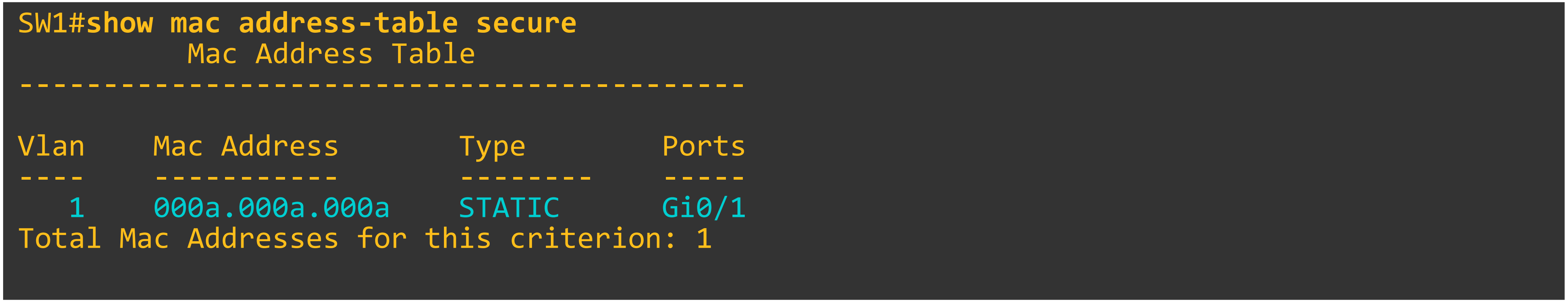
Sticky Secure MAC Addresses

```
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
```

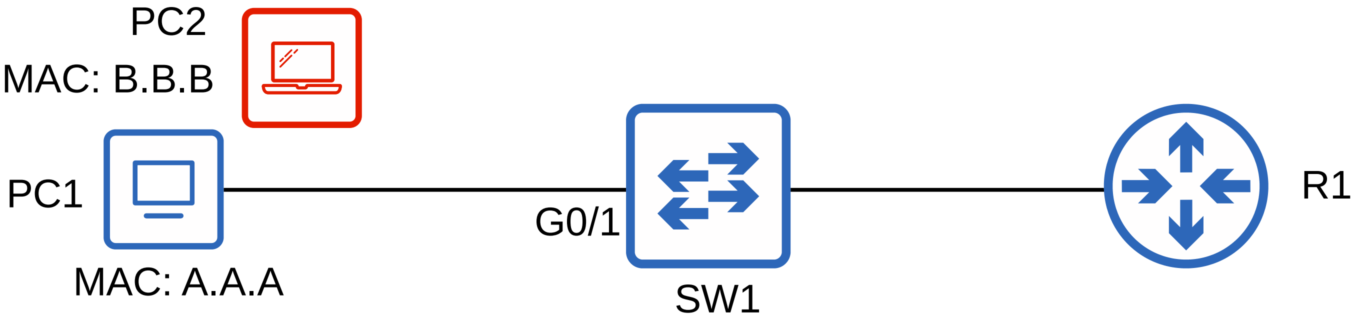


MAC Address Table

- 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 addresess 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

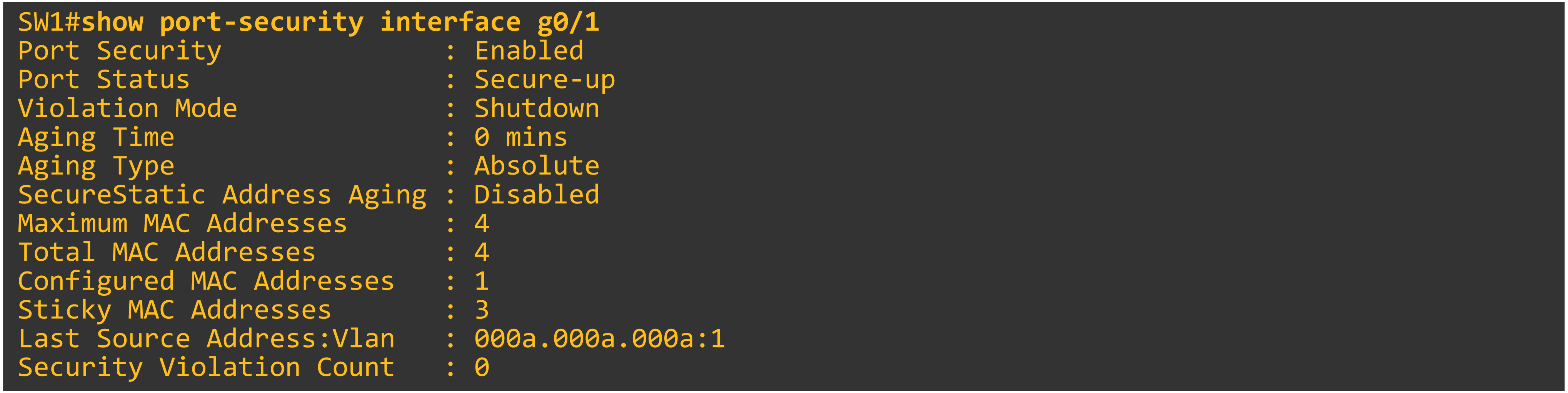
```
SW1# show mac address-table secure

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
```

Things we covered

- Intro to port security
- Why use port security?
- Port security configuration

Quiz 1

Examine the **show** command output below. How many secure MAC addresses were dynamically learned on 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      : 4
Total MAC Addresses        : 4
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 3
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

a) 0

b) 1

c) 3

d) 4

Quiz 2

Which of the following occur when a port-security violation occurs in **restrict** mode?
(select the two best answers)

a) The interface is put in a err-disabled state

b) Unauthorized traffic is discarded

c) All traffic is discarded

d) An SNMP Get message is sent

e) The violation counter is incremented

f) The violation counter is not incremented

Quiz 3

Examine the following output. What will SW1 do when an unauthorized frame arrives on G0/1?

```
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   : 000a.000a.000a:1
Security Violation Count   : 0
```

a) Unauthorized traffic will be dropped.

b) All traffic will be dropped.

c) G0/1 will be err-disabled.

d) The source MAC address will be learned as normal.

Quiz 4

Which of the following will re-enable an interface that was disabled by port security?
(select the two best answers)

a) **`shutdown`** and then **`no shutdown`** on the interface

b) **`errdisable recovery cause psecure-violation`** in global config mode

c) Unplugging the unauthorized device

d) **`switchport port-security aging static`** on the interface

Quiz 5

Examine the following output. What will happen when the **`switchport port-security`** command is issued on G0/1?

```
SW1#show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
[output omitted]
```

a) The command will be accepted.

b) The command will be rejected.