# **49. PORT SECURITY**

## **INTRODUCTION TO 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 switch port.
* 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 **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 administrators 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**.
* Instead of manually specifying allowed MAC addresses, **limiting the number of MAC addresses** per interface is more practical.
* **Example: 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 per interface** can help **prevent** these attacks.

## 

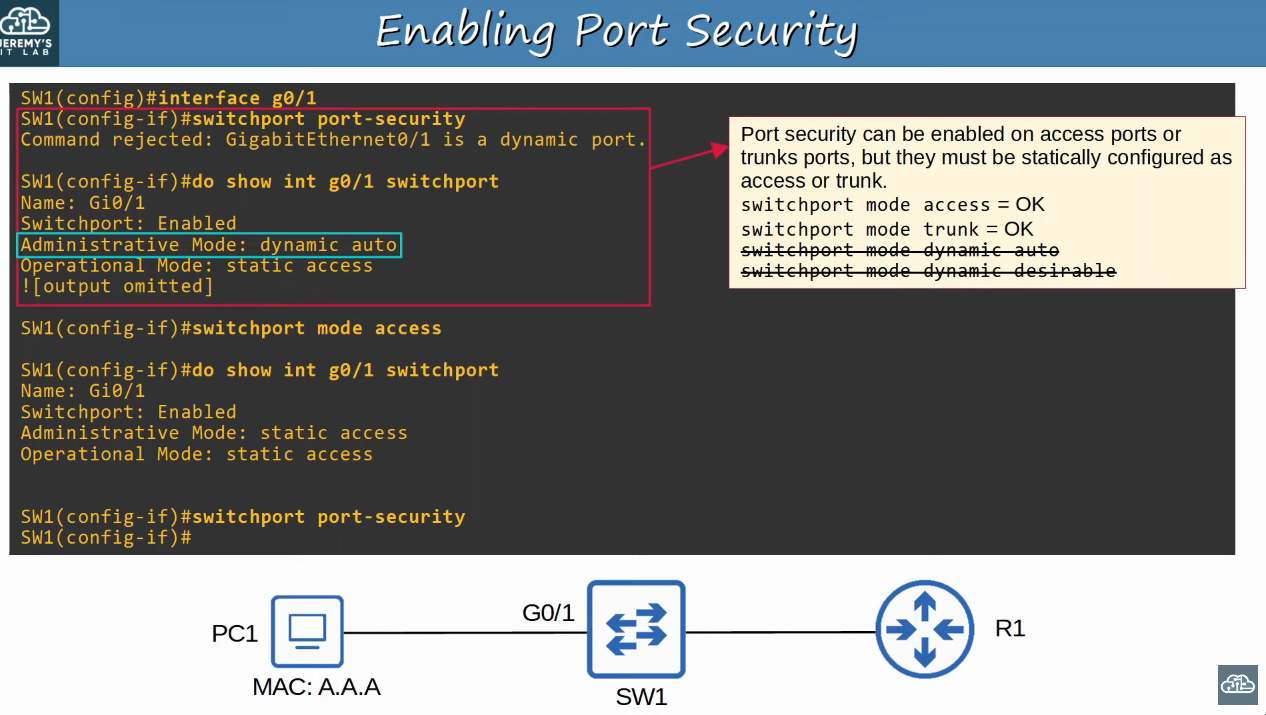
## 

## 

## **ENABLING PORT SECURITY**

### **Show Port Security Information:**

SW1#show port-security interface g0/1



### **Re-Enabling an Interface (Manually)**

SW1#int g0/1

SW1(config-if)#shutdown

SW1(config-if)#no shutdown

### **Re-Enabling an Interface (Err-Disable Recovery)**

## 

## 

## 

## 

## 

## 

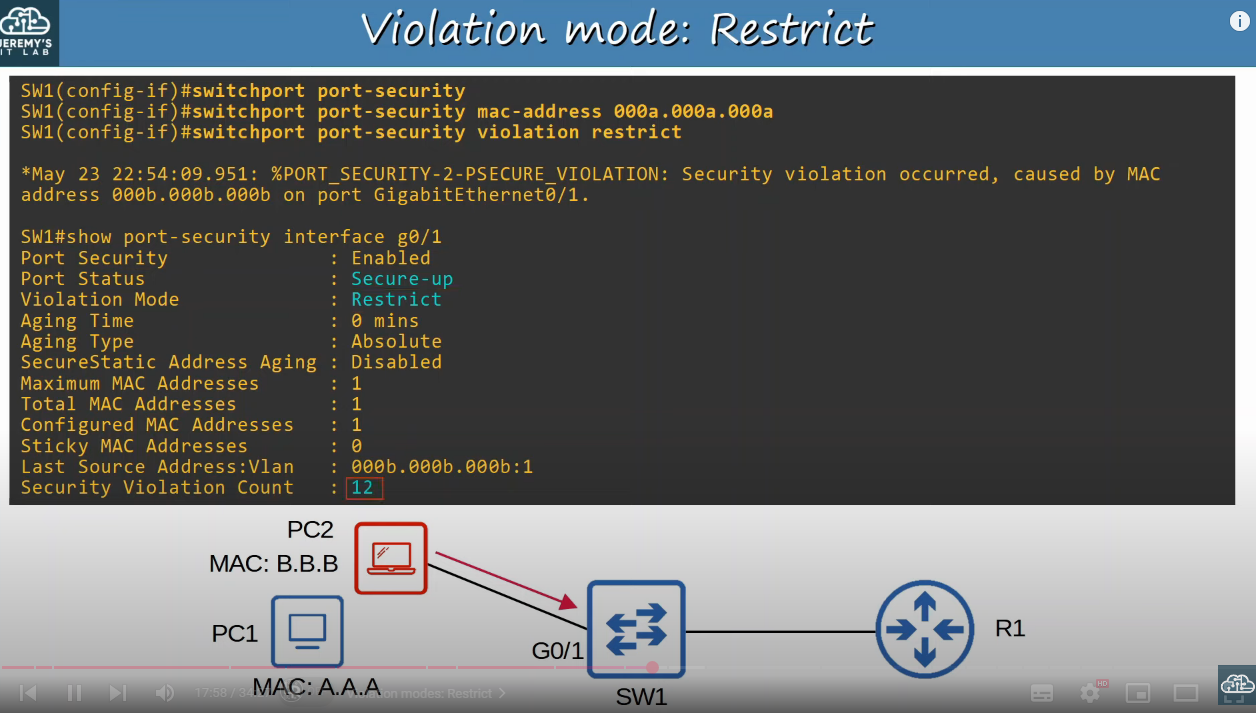
## 

## **VIOLATION MODES**

There are **three different violation modes** that determine what the switch will do if an **unauthorized** frame enters an interface with **Port Security** enabled:

1. **Shutdown**
   * 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.
2. **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** increments by **1** for each unauthorized frame.
3. **Protect**
   * The switch **discards traffic** from unauthorized MAC addresses.
   * The **interface is NOT disabled**.
   * **Does NOT generate** SYSLOG/SNMP messages for unauthorized traffic.
   * **Does NOT increment** the violation counter.

### **Violation Mode - Restrict**



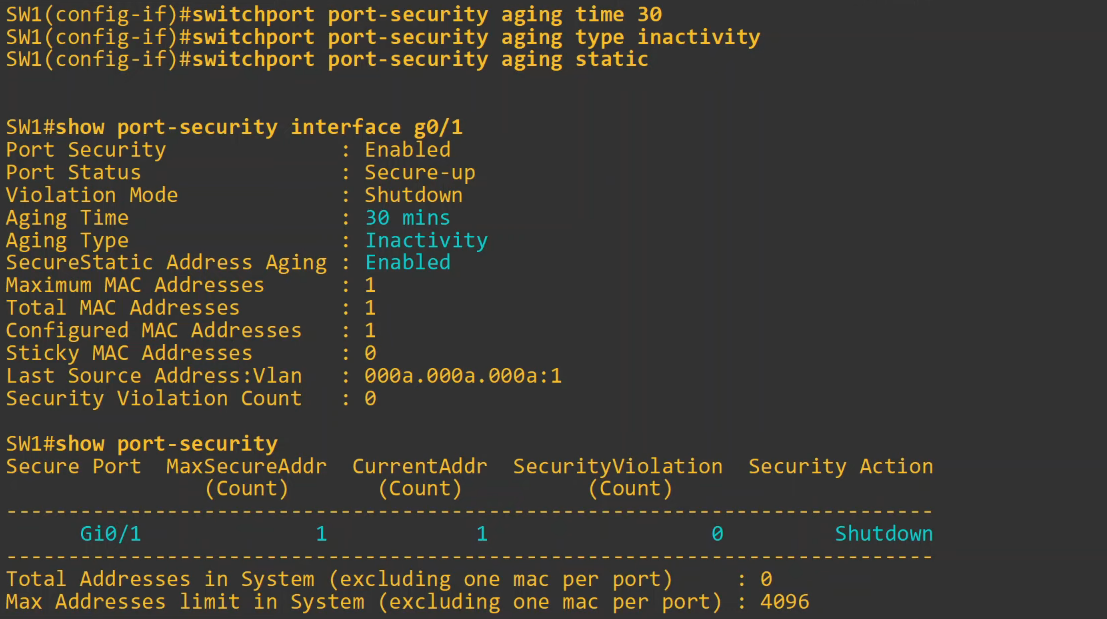
### **Violation Mode - Protect**

## 

## 

## **SECURE MAC ADDRESS AGING**

* **By default**, secure MAC addresses will **not age out** (Aging Time: 0 minutes).
  + Can be configured using: switchport port-security aging time \*minutes\*
* **Default Aging Type:** **Absolute**
  + **Absolute:** After a secure MAC address is learned, the aging timer starts and the MAC is **removed after the timer expires**, even if frames are still received from that source.
  + **Inactivity:** After a secure MAC address is learned, the aging timer **resets** every time a frame is received from that source.
    - Configure with: switchport port-security aging type {absolute | inactivity}
* **Secure Static MAC Aging** is **disabled** by default.



## 

## **STICKY SECURE MAC ADDRESSES**

* **Sticky secure MAC address learning** can be enabled with:
  + SW(config-if)# switchport port-security mac-address sticky
* When enabled, dynamically-learned **secure MAC addresses** are added to the **running configuration**:
  + switchport port-security mac-address sticky \*mac-address\*
* **Sticky MAC addresses never age out**.
  + To make them **permanent**, save the **running-config** to **startup-config**.
* Issuing switchport port-security mac-address sticky converts **all current dynamically-learned** MAC addresses to **sticky**.
* Issuing no switchport port-security mac-address sticky converts **all sticky MAC addresses** back to dynamically learned.

## **MAC ADDRESS TABLE**

* **Secure MAC addresses** are added to the **MAC address table**:
  + **Sticky** and **static secure MAC addresses** are labeled **STATIC**.
  + **Dynamically-learned secure MAC addresses** are labeled **DYNAMIC**.
  + View all secure MAC addresses with:
    - show mac address-table secure

## **COMMAND REVIEW**

