**Lab 12: Configuring MAC-Based Port Security with Violation Modes**

**✅ Scenario (Real-Time):**

You are a network engineer at a corporate office where **unauthorized users frequently plug their personal laptops** into network ports. To prevent this, your company implements **MAC-based port security** on access switches.

You need to configure port security such that:

* Only **one authorized device** can connect to a port.
* If someone tries to plug in an unauthorized device:
  + **In HR VLAN (VLAN 10)** → port should **shut down**.
  + **In Sales VLAN (VLAN 20)** → port should **drop the frame silently (protect)**.
  + **In IT VLAN (VLAN 30)** → port should **generate a log and alert (restrict)**.

**✅ Lab Topology:**

| **Device** | **Interface** | **VLAN** | **Connected Device** |
| --- | --- | --- | --- |
| Switch SW1 | Fa0/1 | 10 | HR-PC (MAC: AAAA) |
| Switch SW1 | Fa0/2 | 20 | Sales-PC (MAC: BBBB) |
| Switch SW1 | Fa0/3 | 30 | IT-PC (MAC: CCCC) |

You can simulate this in **Cisco Packet Tracer** or **GNS3** with 1 switch and 3 PCs.

**✅ Lab Tasks:**

**⚙️ 1. Configure VLANs:**

bash

CopyEdit

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# name HR

Switch(config)# vlan 20

Switch(config-vlan)# name Sales

Switch(config)# vlan 30

Switch(config-vlan)# name IT

**⚙️ 2. Assign interfaces to VLANs:**

bash

CopyEdit

Switch(config)# interface range fa0/1 - 3

Switch(config-if-range)# switchport mode access

Switch(config)# interface fa0/1

Switch(config-if)# switchport access vlan 10

Switch(config)# interface fa0/2

Switch(config-if)# switchport access vlan 20

Switch(config)# interface fa0/3

Switch(config-if)# switchport access vlan 30

**⚙️ 3. Enable port security globally:**

bash

CopyEdit

Switch(config)# interface range fa0/1 - 3

Switch(config-if-range)# switchport port-security

Switch(config-if-range)# switchport port-security maximum 1

Switch(config-if-range)# switchport port-security mac-address sticky

**⚙️ 4. Set different violation modes:**

* 🔴 **Fa0/1 (HR)** → **Shutdown**:

bash

CopyEdit

Switch(config)# interface fa0/1

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

* 🟡 **Fa0/2 (Sales)** → **Protect**:

bash

CopyEdit

Switch(config)# interface fa0/2

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

* 🟢 **Fa0/3 (IT)** → **Restrict**:

bash

CopyEdit

Switch(config)# interface fa0/3

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

**✅ Verification Commands:**

1. **Check port security settings**:

bash

CopyEdit

show port-security interface fa0/1

1. **Check sticky MAC address**:

bash

CopyEdit

show run interface fa0/1

1. **Check port security violations**:

bash

CopyEdit

show port-security

show port-security address

**🔁 Test Cases:**

* Plug an **unauthorized PC** (with different MAC) into each port and observe the behavior:
  + **HR port** (Fa0/1) → port should go **err-disabled**.
  + **Sales port** (Fa0/2) → no error but **frames are dropped**.
  + **IT port** (Fa0/3) → **syslog message** and **counter increases**.

**✅ Bonus: Recover port from shutdown (HR port):**

bash

CopyEdit

Switch(config)# interface fa0/1

Switch(config-if)# shutdown

Switch(config-if)# no shutdown

**🎯 Real-Time Use Case Summary:**

| **Department** | **Violation Mode** | **Behavior** |
| --- | --- | --- |
| HR | Shutdown | Highly secure, disables port |
| Sales | Protect | Low impact, no alerts, silently drops |
| IT | Restrict | Logs incident but port stays active |