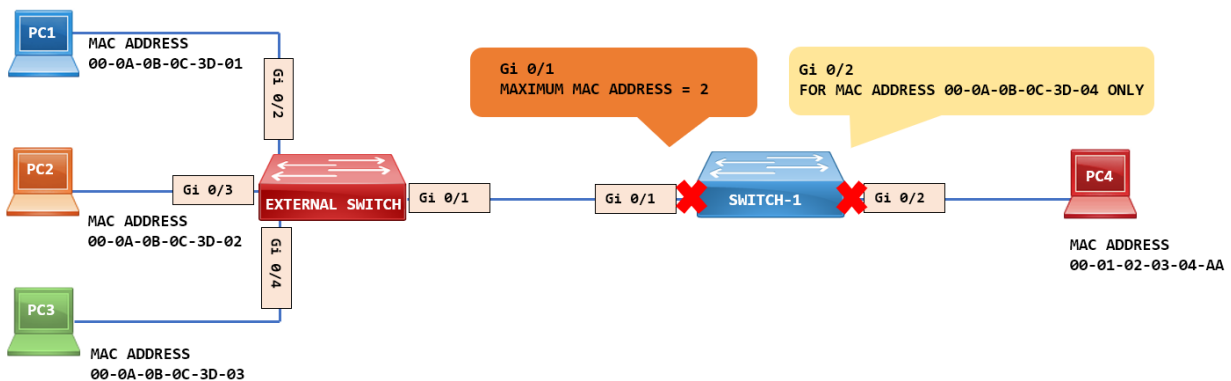


Port Security

เราจะสามารถจำกัดการใช้งาน โดยการตั้งค่าบน Port Switch เช่น จำกัดจำนวน MAC Address บน Port ของ Switch หรือกำหนดให้ Port Switch รับเฉพาะ MAC Address นี้เท่านั้น หรือ Fixed MAC Address จึงจะสามารถใช้งานได้ ซึ่งถ้าหากสามารถจำกัดการเข้าถึงเครือข่ายตามที่กล่าวมาข้างต้นแล้ว จะทำให้มีความปลอดภัยมากยิ่งขึ้น Port Security จะเข้ามามีส่วนช่วยในเรื่องนี้ ยกตัวอย่างรูป Diagram ด้านล่าง ถ้าหากมี MAC Address เกินกว่าจำนวนที่กำหนดไว้ หรือได้รับ MAC Address ผ่านมาทาง Port Switch นั้น ไม่ตรงกับ MAC Address ที่ตั้งค่ากำหนดไว้ Switch จะทำอย่างไรกับการละเมิดหรือฝ่าฝืนเหล่านั้น ซึ่งรายละเอียด จะขออธิบายเป็นลำดับถัดไป



เมื่อมีการใช้งาน Port Security แล้ว MAC Address ออกเป็น 3 ประเภท ภายใต้ Port Security

- Static: เป็นการระบุ MAC Address ที่ต้องการลงบน Port นั้นๆ โดยตรง ซึ่งจะทำให้ MAC Address นั้นถูกเก็บใน running-config

```
SWITCH-1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type               Ports    Remaining Age (mins)
-----
1       0050.7966.6801   SecureSticky      Gi0/0    -
1       0050.7966.6803   SecureConfigured  Gi0/1    -
1       0050.7966.6806   SecureDynamic     Gi0/3    -
1       0050.7966.6807   SecureDynamic     Gi0/3    -
1       0050.7966.6808   SecureDynamic     Gi0/3    -
1       5000.0005.0003   SecureDynamic     Gi0/3    -
-----
Total Addresses in System (excluding one mac per port)  : 3
Max Addresses limit in System (excluding one mac per port) : 4096
```

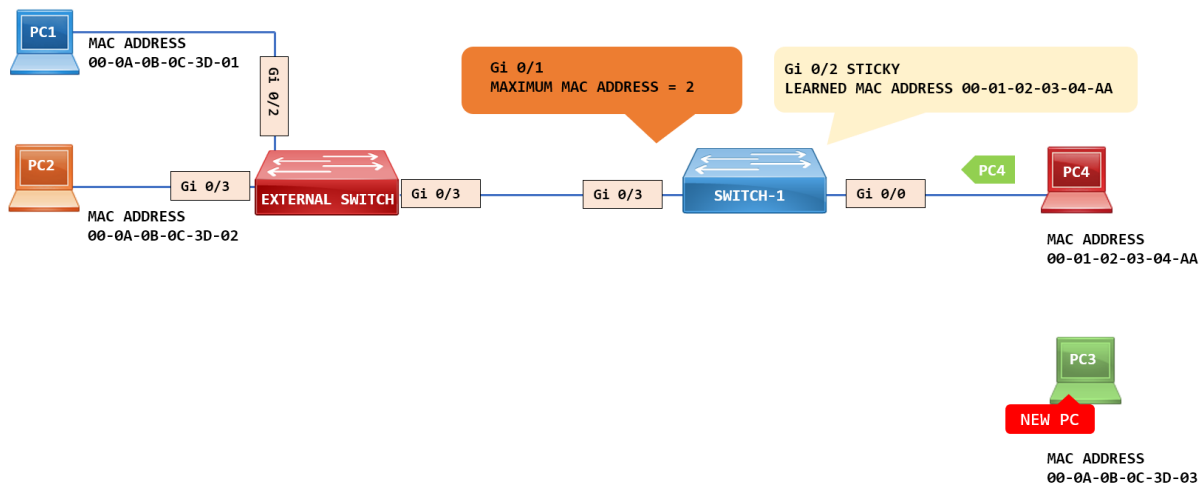
- Dynamic: จะทำการเก็บ MAC Address ของอุปกรณ์ที่เชื่อมต่อไว้ใน MAC Address Table ที่เป็นแบบ Static และจะไม่ถูกเก็บลงบน running-config ถ้าหาก Port ถูก Disable หรือ Port Down หรือ Switch Reboot ก็จะมีการเรียนรู้ MAC Address ใหม่อีกครั้ง

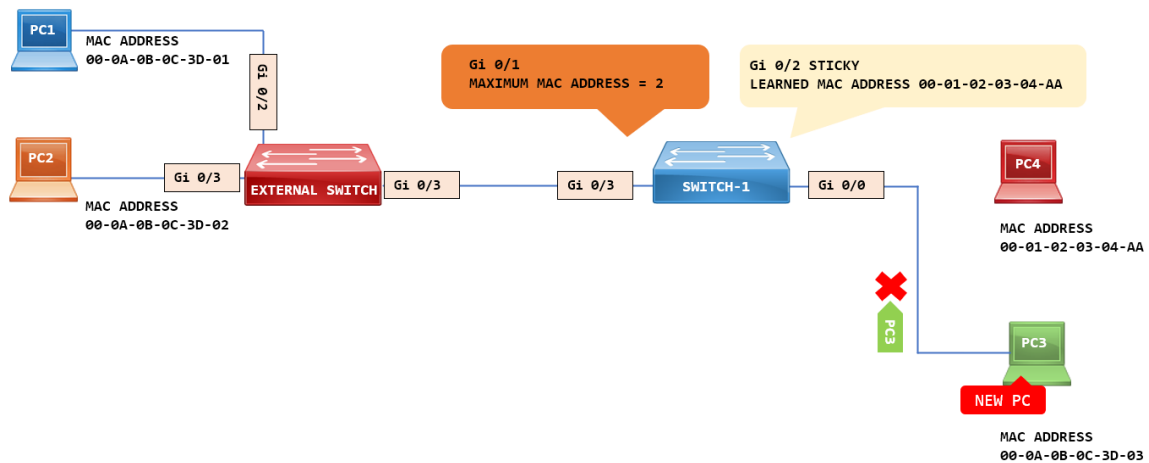
```
SWITCH-1#show port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0050.7966.6801	SecureSticky	Gi0/0	-
1	0050.7966.6803	SecureConfigured	Gi0/1	-
1	0050.7966.6806	SecureDynamic	Gi0/3	-
1	0050.7966.6807	SecureDynamic	Gi0/3	-
1	0050.7966.6808	SecureDynamic	Gi0/3	-
1	5000.0005.0003	SecureDynamic	Gi0/3	-

Total Addresses in System (excluding one mac per port) : 3
Max Addresses limit in System (excluding one mac per port) : 4096

- Sticky: มีรูปแบบที่ผสมผสานกันระหว่างแบบ Static และแบบ Dynamic โดยการเรียนรู้ MAC Address นั้นจะเรียนรู้แบบอัตโนมัติเหมือนกับแบบ Dynamic โดยจะนำเอา MAC Address แรกที่เรียนรู้มาได้ และนำ MAC Address นั้นลงบน Running-Config ด้วย ตามรูป Diagram ด้านล่าง





จะเห็นได้ว่า PC3 ไม่สามารถส่งข้อมูลได้ เนื่องจาก SWITCH-1 ได้เรียนรู้ MAC Address ของ PC4 เป็นลำดับแรก

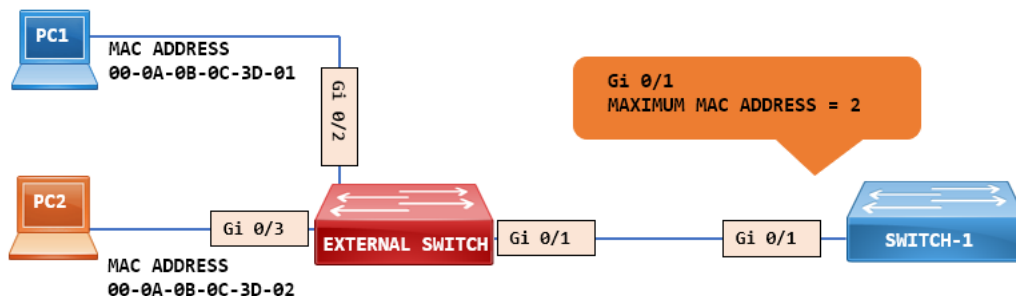
```
SWITCH-1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       0050.7966.6801   SecureSticky        Gi0/0    -
1       0050.7966.6803   SecureConfigured    Gi0/1    -
1       0050.7966.6806   SecureDynamic        Gi0/3    -
1       0050.7966.6807   SecureDynamic        Gi0/3    -
1       0050.7966.6808   SecureDynamic        Gi0/3    -
1       5000.0005.0003   SecureDynamic        Gi0/3    -
-----
Total Addresses in System (excluding one mac per port)    : 3
Max Addresses limit in System (excluding one mac per port) : 4096
```

Violation

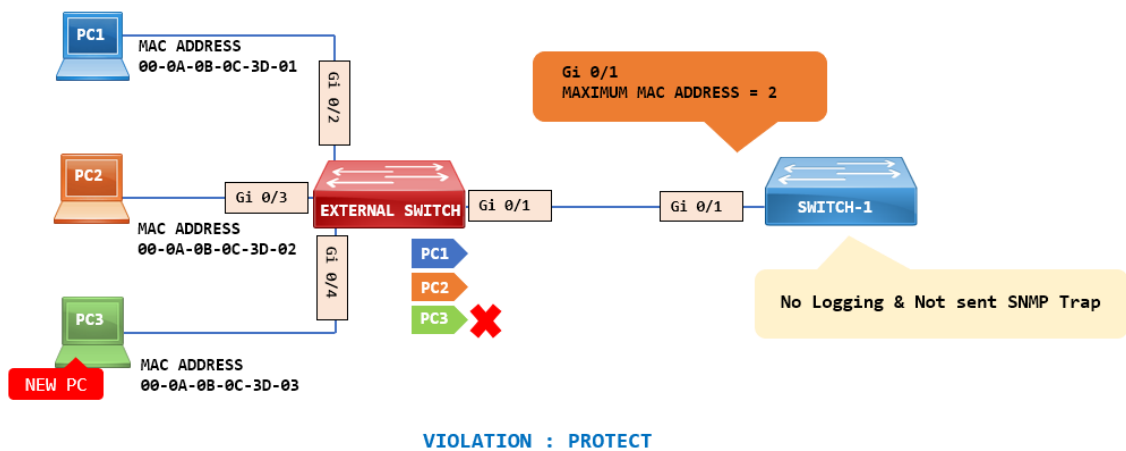
หากมีการละเมิดเกิดขึ้น เช่น MAC Address ที่ได้รับเข้ามานั้น ไม่ตรงกันกับที่ได้ตั้งค่าไว้ภายใต้ Port หรือ MAC Address มีจำนวนที่มากกว่าที่กำหนดไว้ Switch จะมีมาตรการอย่างไรบ้าง ถ้าหากมีการฝ่าฝืนหรือการละเมิดเกิดขึ้น

สำหรับ Port Security นั้น จะมี Violation ทั้งหมด 3 รูปแบบ ถ้าหากมีการฝ่าฝืน ดังนี้

- **Protect:** ถ้าหากมีการฝ่าฝืนเกิดขึ้นภายใต้ Port ที่ทำการตั้งค่า Violation แบบนี้ Switch จะไม่ทำการส่ง Traffic ถ้าหาก MAC Address นั้นไม่ได้อยู่ใน MAC Address Table ตัวอย่างเช่น ถ้าหาก มี MAC Address ที่นอกเหนือจากจำนวนของ Maximum MAC Address ของ Port นั้น Switch จะไม่ทำการส่งข้อมูล หรือ Traffic ของ MAC Address ที่เกินมาออกไป ตัวอย่าง เช่นรูปด้านล่าง



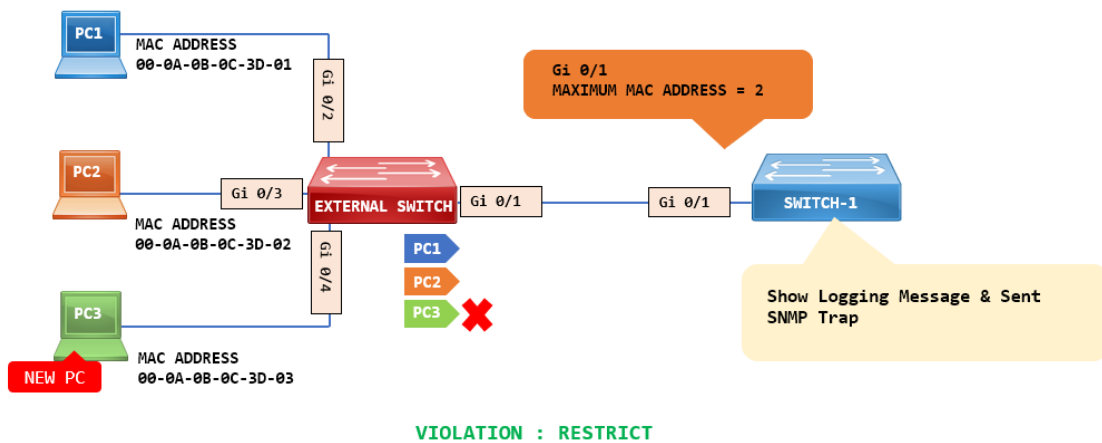
SWITCH-1 ได้ตั้งค่า Maximum MAC Address เท่ากับ 2 ภายใต้ Interface Gi 0/1 ซึ่งตอนนี้ Switch ได้เรียนรู้ MAC Address ของ PC1 และ PC2 แล้ว ซึ่งครบตามจำนวนที่ได้ตั้งค่าไว้แล้ว



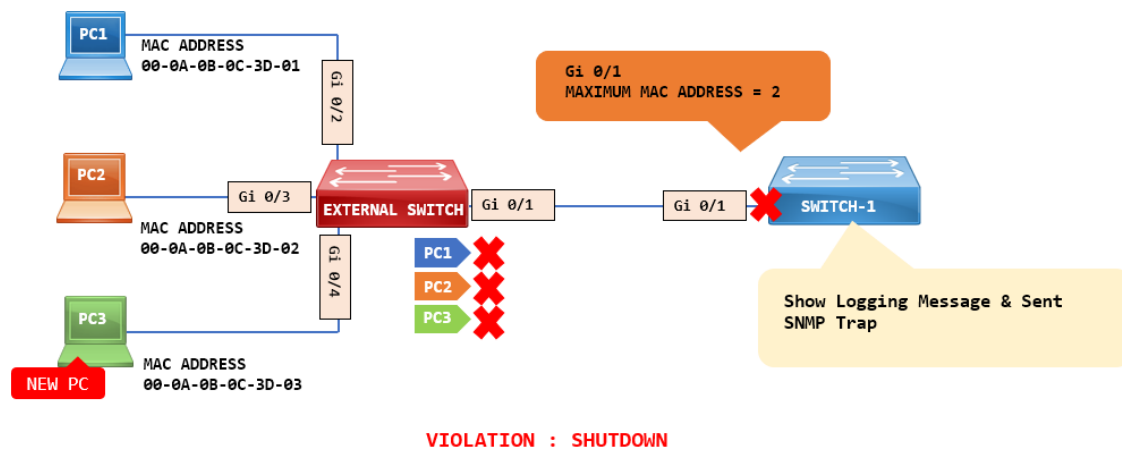
หลังจากนั้นได้มี PC3 ทำการเชื่อมต่อเข้ามาใหม่ เมื่อมีเหตุการณ์นี้เกิดขึ้น PC1 และ PC2 ยังคงสามารถส่งข้อมูลได้ปกติ แต่ PC3 จะไม่สามารถส่งข้อมูลได้

สำหรับ Violation แบบ Protect นั้น จะไม่มีการส่ง Log ไปยัง SNMP Server และไม่แสดง Syslog แจ้งเตือนบน Switch ถึงแม้จะมีการฝ่าฝืนเกิดขึ้นแล้วก็ตาม

- Restrict: สำหรับ Mode นี้จะมีความทำงานเหมือนกับแบบ Protect แต่จะมีความแตกต่างในส่วนของการแจ้งเตือน ซึ่งใน Mode นี้จะทำการส่ง Log ไปยัง SNMP Server และแสดง Syslog แจ้งเตือนบน Switch ด้วย ถ้าหากมีการฝ่าฝืนเกิดขึ้น



- Shutdown ใน Mode นี้ถ้าหากมีการละเมิดเกิดขึ้น เช่นมี MAC Address เข้ามาเกินจำนวนที่ได้กำหนดไว้ หรือ ได้รับ MAC Address ไม่ตรงกับที่ Config ไว้ Port นั้นจะถูก Shutdown และ LED ที่แสดงสถานะของ Port นั้นก็จะดับลงไปด้วย พร้อมทั้งสถานะของ Port จะอยู่ในสถานะ err-disable (Error Disable) สำหรับ Log นั้นจะแสดง Syslog ที่เกิดขึ้นและทำการส่ง Log ไปยัง SNMP Server ด้วยเช่นกัน



หลักๆ แล้ว Port Security ได้เพิ่มความปลอดภัยให้กับเครือข่ายมากยิ่งขึ้น แต่ก็มีข้อควรระวังสำหรับการตั้งค่า Violation ให้เหมาะสมต่อการใช้งานของผู้ใช้ [User] ด้วยเช่นกัน