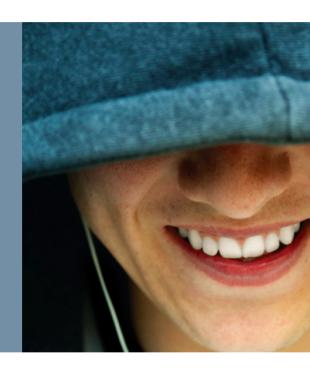
Port Security



MAC Flooding Attack

- 스위치로 구성된 네트워크 환경에서는 Frame이 MAC table을 기반으로 forwarding된다.
- MAC Flooding Attack의 특징
- . 스위치로 구성된 네트워크 환경에서 스위치의 dynamic address learning 동작을 이용해서 공격한다.
- . 네트워크 내에 존재하지 않는 MAC을 짧은 시간에 많이 등록하여,
 - MAC table에 할당된 메모리를 고갈시켜 실제 MAC 정보는 등록되지 못하게 한다.

[Port Security]

포트보안은 허락되지 않은 사용자가 몰래 스위치에 어떤 장치나 다른 호스트를 연결하는 것을 막는 방법이다. "switchport mode access, switchport mode trunk, L3 SVI 에 포트보안 잘 작동함"

- Port Security는 Port로의 접근하는 MAC주소의 수를 제한하여 MAC flooding attack을 차단한다.
- Port Security의 특징
- 1. 지정된 port와 연관되어 MAC table에 기록될 수 있는 MAC의 수를 제한한다.
- 2. 제한된 수의 MAC에 대한 정보는 static, dynamic, sticky한 방법으로 인식될 수 있다.
- 3. 이를 위반하는 상황이 발생했을 때 이에 대응하는 다양한 동작을 취할 수 있다.

Port Security "IOU 2d 작동함"

```
[ 동적 보안 ] SecureDynamic (Type)
                                      # show port-security address
                                                                      # copy run star
int fa0/1
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation (shutdown | protect | restrict)
[정적 보안] SecureConfigured (Type)
                                                                      # copy run star
                                      # show port-security address
int fa0/1
switchport mode access
switchport port-security
switchport port-security mac-address 0000.0000.0001
switchport port-security maximum 2
switchport port-security violation (shutdown | protect | restrict)
[sticky 보안] SecureSticky (Type)
                                      # show port-security address
                                                                      # copy run star
int fa0/1
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 2
switchport port-security violation (shutdown | protect | restrict)
```

sw1#sh port-security 1)Secure Port 2)MaxSecureAddr 3)CurrentAddr 4)SecurityViolation 5)Security Action (Count) (Count) (Count) Fa0/2 0 Shutdown Total Addresses in System (excluding one mac per port) : 0 Max Addresses limit in System (excluding one mac per port): 5120 1)포트보안이 동작중인 포트표시 2)최대등록가능하 맥주소(기본값 1) 별다른 설정값을 주지않으면 포트보안용 맥주소가 하나밖에 등록이 안됩니다. 3)현재등록중인 맥주소 4)보안침해횟수 5)위반시 동작모드(기본값 shutdown) protect, restrict, shutdown 세가지 옵션이 있습니다.

- 1. **Protect**: 보안 침해시 해당 장비의 접속만 차단하고, 접속이 허용된 장비들은 계속 포트를 사용할 수 있게 한다
- 2. **Restirict**: Protect 옵션과 같으나 추가적인 Logging Message를 발생시키거나 보안 침해 카운터를 증가 시킨다
- 3. Shutdown(Default): 보안 침해시 해당 포트를 Shutdown 시킨다.

sw1#show port-security interface f0/2 Port Security : Enabled Port Status : Secure-up Violation Mode : Shutdown : 0 mins Aging Time : Absolute Aging Type SecureStatic Address Aging: Disabled Maximum MAC Addresses : 1 <--- 최대 등록가능 포트보안용 MAC 주소의 개수. Total MAC Addresses : 1 <- 현재 포트보안용 MAC 주소로 등록된 개수를 표시해줍니다. Configured MAC Addresses : 1 <---static으로 등록한 보안용 MAC 주소의 개수(직접 보안용 MAC주소를 Sticky MAC Addresses : 0 직접등록했다는걸 알수있습니다.) Last Source Address: Vlan : 0002 b971.7c60:1 Security Violation Count : 0

Aging Type

1. Absolute: 지정 기간이 지나면 Secure Address 포트에서 삭제 된다

2. Inactivity: Inactive 상태로 지정 기간이 지나면 Secure Address 포트에서 삭제 된다

```
SW02(config-if)#switchport port-security aging static
SW02(config-if)#switchport port-security aging time ?
  <1-1440> Aging time in minutes. Enter a value between 1 and 1440
SW02(config-if)#switchport port-security aging time 1
SW02(config-if)#switchport port-security aging type ?
  absolute   Absolute aging (default)
  inactivity Aging based on inactivity time period
SW02(config-if)#switchport port-security aging type absolute
```

