Port Security

1. Port Security란

스위치의 특정 포트에 특정 MAC 주소를 가진 장비만 접속할 수 있게 하는 것

○ 종류

- **Static Port Security**
- **Dynamic Port Security**
- **Port Sticky**

2. Port Security Port

○ **사용 가능 포트**

Access Port, Trunk Port, Tunnel Port

○ **사용 불능 포트**

Routed Port, SVI, EtherChannel

3. Port Security 설정 (모두 인터페이스 모드 설정)

○ **정적 MAC 주소 지정**

Port Security용 MAC 주소를 정적으로 직접 지정

```
switchport port-security mac-address 0000.0000.0001
switchport port-security
```

*** switchport port-security 명령어를 먼저 사용하면 스위치의 MAC 주소 테이블에 있는 주소를 사용하여 동적인 Port Security MAC 주소가 먼저 지정된다.**

○ **동적 MAC 주소 지정**

설정시 MAC 주소 테이블에 있거나 해당 포트를 통해 수신되는 프레임의 MAC 주소가 Port Security용 MAC 주소가 된다.

```
switchport port-security
```

○ **Port Sticky**

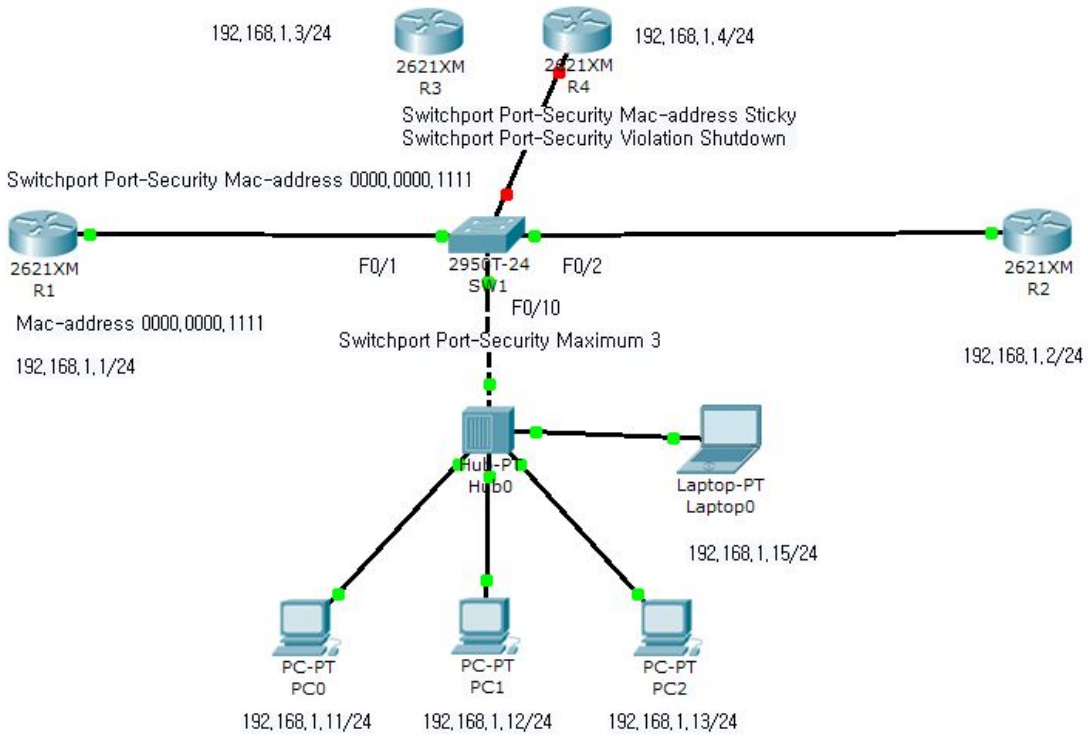
- 동적 Port Security MAC 주소를 정적 주소로 변경시키는 것
- 동적 Port Security MAC 주소는 스위치의 전원을 다시 켜면 다 삭제된다.
- **Port Sticky 방식을 사용하면 설정 파일을 저장할 때 Port Security MAC 주소도 함께 저**

장되어 전원을 꺼도 삭제되지 않는다.

- 액세스 포트에 동시에 다수 개의 Port Security MAC 주소를 설정시 편리

switchport port-security
switchport port-security maximum 숫자
switchport port-security mac-address sticky

* DTP를 사용하는 동적 포트에서는 Port Security를 설정할 수 없다.



4. 확인 명령어

○ show port-security

포트 보안 설정 상황

- Secure Port: 포트 보안이 설정된 포트
- MaxSecureAddr: 최대허용 보안 MAC 주소의 수량
- CurrentAddr: 현재 동작하고 있는 보안 MAC 주소의 수량
- SecurityViolation: 포트 보안 침해횟수
- Security Action: 포트 보안 침해시의 동작

○ show port-security address

포트 보안용 MAC 주소 확인

○ **show port-security interface ...**
포트 보안 설정 확인

5. Port Security 침해시 동작 설정

○ 기본 동작
포트 보안용 MAC 주소가 아닌 프레임을 수신했을 때 기본적으로 해당 포트를 셧다운시킨다. 네트워크 관리자가 해당 포트를 한번 더 shutdown 시킨 후에 다시 no shutdown 명령어를 사용해야 한다.

○ Port Security 침해시 동작 변경
switchport port-security violation [protect | restrict | shutdown]

- **protect**
  보안 침해시 해당 장비 접속만 차단하고, 접속이 허용된 장비들은 계속 포트를 사용할 수 있다.
- **restrict**
  Protect 옵션과 같으나, 추가적으로 로그 메시지를 발생시키고 보안 침해 카운터를 증가시킨다.
- **shutdown**
  기본 설정이며, 보안 침해 발생시 포트를 셧다운시킨다.

6. Err-disabled

장비가 command에 의해서 shutdown 상태로 전환되면 Err-disabled mode로 변경
'no shutdown'을 입력해도 활성화 상태로 전환되지 않음

○ Solution
- 수동
  해당 port를 수동으로 shutdown상태로 전환 후 다시 'no shutdown'을 사용하여 활성화
- 자동 (설정 모드)
  errdisable recovery cause security-violation
  errdisable recovery interval [30 ~ 86400 초]

- 확인
  show errdisable recovery