Network

■ Port-Security
- 스위치 포트에 특정 MAC 주소만 수신되도록 하는 기능
◇ 설정 조건
- Dynamic Port(DTP)는 설정 불가
Native VLAN에 의해서 기본 VLAN인 VLAN1을 가지고 통신을 함.
VLAN1을 가지고 VTP 데이터가 돌아다님
※ show int switch 등 interface 확인해야 함
- EtherChannel 설정 불가
- Span Port는 설정 불가

◆ 포트보안시 MAC 설정방법
1. 정적 포트보안(Static)
- 관리자가 직접 MAC을 설정
<Interface를 활용하여 port-security 활성화>
Switch(config)#int f 0/1
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port. → DTP 상태이기 때문에 에러남.
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address [00D0.BAC4.24E8]

다른 PC로 옮기면 Port가 Down이 됨(Ping도 Request Timeout이 뜨게 됨)
Switch#show port-security
Switch#show port-security address
Switch#show port-security int f 0/1

Switch(config-if)#sw port-security mac-address [0002.179D.7411]
Total secure mac-addresses on interface FastEthernet0/1 has reached maximum limit.
Switch(config-if)#no switchport port-security mac-address [00D0.BAC4.24E8]
한 후 다시
Switch(config-if)#sw port-security mac-address [0002.179D.7411]
적용이 되는 것 확인이 됨(즉, 등록한 MAC 주소를 바꿀때는 덮어쓰기가 안 됨 새로 지우고 등록)

- 설정을 저장하면 Port-Security 목록도 같이 저장이 됨
- 여러개를 설정할 때는 Maximum 설정

2. 동적 포트보안(Dynamic)

- Switch가 MAC을 학습한 순서대로 등록을 함
Switch(config)#int f 0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2 → Port 보안 할 MAC 개수(최대 2개)를 지정
- 설정 저장 안 됨

3. Sticky 포트보안
- 동적(Dynamic)으로 받은 MAC 주소를 정적(Static)으로 변경
Switch(config-if)#switchport port-security sticky
- 설정 파일을 저장하면 Sticky로 등록된 MAC도 저장이 됨

◆ Violation Mode
- 설정 정책을 위반한 경우 Port의 동작 방법
1. Shutdown(Error Disable) : Port를 shutdown시킴
2. Protect : 등록된 MAC은 허용 나머지 MAC은 차단
3. Restrict : 등록된 MAC은 허용 나머지는 차단 + SecurityViolation Count 증가 + log 발생 + SNMP Trap이 동작하여 알림 발생

Switch(config-if)#switchport port-security violation ?
  protect Security violation protect mode
  restrict Security violation restrict mode
  shutdown Security violation shutdown mode

◆ Aging Time
- 등록된 MAC Address에 대한 유지 시간을 설정
- 설정 가능한 시간 0~1440분
- Absolute : Aging Time이 지나면 MAC이 삭제(시간이 지나면 그냥 삭제)
- Inactivity ; Aging Time동안 Traffic이 없는 경우 MAC 삭제(시간 동안 트래픽이 없으면 삭제)

◆ Span(port mirroring)
Source를 통과하는 Traffic이 Destination에 그대로 간다.
Packet 감시나 모니터링 할 때에 사용을 한다.
물리 interface 뿐만 아니라 VLAN Interface도 Source로 지정가능

- 특정 포트로 지나는 패킷(Source)을 복사하여 지정한 포트(Destination)로 전송하는 것
- 주로 감시장비나 모니터링 시스템 연결 시 사용
- 목적지 포트는 통신 불가
- Source Port는 여러개 지정 가능하나, Destination Port는 하나만 설정가능
- 하나의 Switch에 2개까지만 생성 가능

<Span 설정방법>

Switch# conf t

Switch(config)#monitor session ?

<1-2> → Monitor 넘버 지정

monitor session [1] source int f 1/2

monitor session [1] source int f 1/3

또는

monitor session [1] source int f 1/4-5

monitor session [1] destination int f 1/15

show monitor session

monitor session [1] source int f 1/6 ?

both (송 수신 모두)

rx received traffic(송신 switch 기준)

tx transmitted traffic(수신 switch기준)

Switch# conf t

Switch(config)#monitor session 1 source int f 1/2 – 5 [both/rx/tx]

Switch(config)#monitor session 2 destination int f 1/15

- 물리 Interface 뿐만 아니라 VLAN Interface도 가능