스위치 ACL 보안

1. ACL 보안

○ 스위치에서도 라우터와 마찬가지로 ACL를 이용하여 다양한 보안 정책을 구현할 수 있다. ACL는 내용에 따라 IP ACL과 MAC ACL로 구분할 수 있다.

[표 ACL 종류 및 적용위치]

ACL 종류	제어 프로토콜	적용 위치
MAC ACL	MAC	L2 Port
IP ACL	IP	L2/L3 Port
Port ACL	MAC, IP	L2/L3 Port
Router ACL	IP	L3 Port
VLAN ACL	MAC, IP	VLAN
PBACL	IP	L3 Port

2. MAC ACL

○ IP Packet을 제외한 트래픽을 제어할 때 사용하며, Port ACL과 VLAN Map에서 사용

○ 기본 설정

- mac access-list extended 이름
- deny 출발지주소 와일드카드 목적지주소 와일드카드
- permit any any

- 출발지 MAC 주소, Wildcard, 목적지 MAC 주소, Wildcard 사용
- 특정 주소 하나만을 지정하려면 Wildcard Mask 대신 주소 앞에 Host 옵션을 사용한다. 복수개의 주소를 지정하려면 와일드카드를 사용한다.
- 예를 들어 0000.0c로 시작하는 모든 MAC 주소를 지정하려면 0000.0c00.0000 0000.00ff.ffff와 같이 와일드 카드를 사용한다.
- 조건에 해당되지 않은 모든 프레임을 허용하려면 permit any any 명령어를 사용한다.
- 다른 ACL와 마찬가지로 MAC ACL도 마지막에는 deny any any가 적용된다.

[설정 MAC ACL 적용]

구분	설정
예	MAC 주소가 2222.2222.2222과 3333.3333.333인 장비간의 트래픽을 차단하는 MAC ACL은?
SW1	mac access-list extended MAC22-33 deny host 2222.2222.2222 host 3333.3333.3333

	permit any any

3. Port ACL

○ Layer 2 Port에 ACL를 적용하는 것

▪ MAC ACL과 IP ACL를 모두 사용할 수 있다.

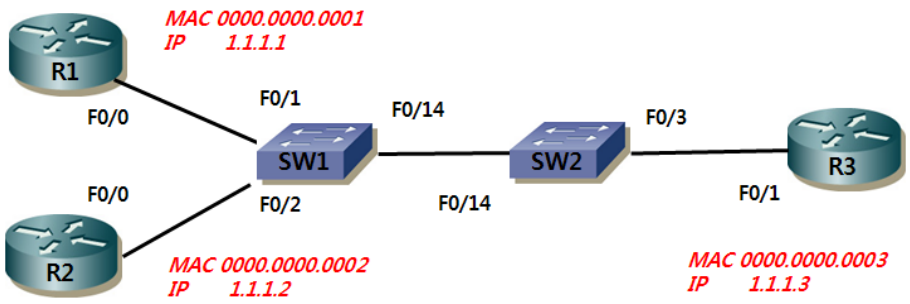
1) 스위치가 Port에서 프레임을 수신할 때만 적용할 수 있다. 즉, in 옵션만 사용할 수 있다.

2) 특정 스위치에서 VLAN Map이나 Inbound 라우터 ACL이 설정되어 있으면 Port ACL을 사용할 수 없다.

○ 기본 설정

▪ interface …

▪ **mac access-group** MAC_ACL_이름 **in**



[설정 MAC ACL을 이용한 Port ACL]

구분	설정
예	R1(0000.0000.0001)에서 R2(0000.0000.0002)로 가는 프레임을 차단하고자 하는 경우
SW1	mac access-list extended MAC1-2 deny host 0000.0000.0001 host 0000.0000.0002 permit any any ! int f0/1 mac access-group MAC1-2 in

[설정 IP ACL을 이용한 Port ACL]

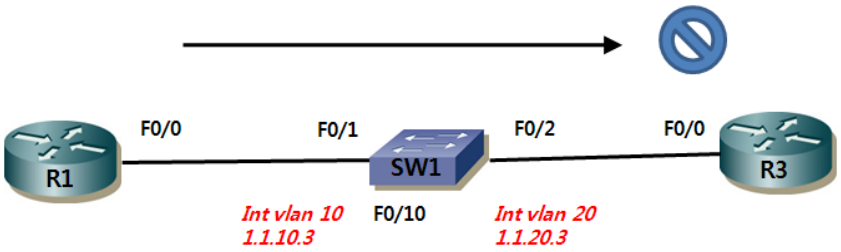
구분	설정
예	R1에서 R2로 가는 IP 프레임을 차단하고자 하는 경우
SW1	ip access-list extended IP1-2 deny ip host 1.1.12.1 host 1.1.12.2 permit any

	! int f0/1 ip access-group IP1-2 in

4. Router ACL

○ Routed Port나 SVI와 같은 Layer 3 Port에 ACL을 적용하는 것

- Router ACL에는 IP ACL만 사용할 수 있다. 즉 MAC ACL은 사용할 수 없다.



[설정 SVI에 Router ACL 적용]

구분	설정
예	1.1.10.1에서 1.1.20.2로 가는 패킷을 거부하는 IP ACL을 만든 다음에 인터페이스 Vlan 10에 설정하는 경우
SW1	ip access-list extended RACL1-2 deny ip host 1.1.10.1 host 1.1.20.2 permit ip any any ! int vlan 10 ip access-group RACL1-2 in

5. Vlan Map

○ Vlan에서 설정하는 ACL로 Vlan ACL이라고도 한다.

- MAC ACL과 IP ACL을 모두 사용할 수 있다.
- VLAN 맵을 사용하면 VLAN간의 트래픽뿐만 아니라 VLAN 내부에 있는 장비간의 트래픽도 제어할 수 있다.

○ **VLAN Map 설정 방법**

1) VLAN 맵에서 사용할 ACL을 생성

2) Vlan Access-map 생성

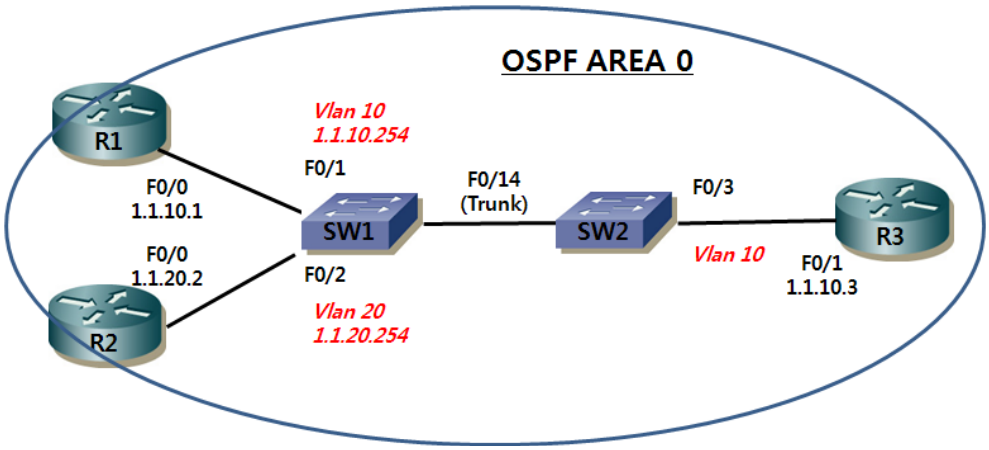
- vlan access-map 이름

- **match** 조건
- **action** [forward | drop]

* 맵 이름만 정의하고 match와 forward/drop 명령어를 사용하지 않으면 나머지 모든 것은 허용한다는 의미

3) **Vlan Filter Vlan-list** 명령어 사용

- **vlan filter** 이름 **vlan-list** VLAN번호
- VLAN 맵을 하나 또는 복수 개의 VLAN에 적용



[설정 VLAN Map]

구분	설정
예	Vlan 10의 R1과 Vlan 20의 R2에서 R3로 접근하는 Telnet 트래픽을 차단하고자 할 경우
SW1	access-list 100 permit tcp host 1.1.1.1 host 3.3.3.3 eq telnet access-list 100 permit tcp host 2.2.2.2 host 3.3.3.3 eq telnet access-list 101 permit ip any any ! vlan access-map NO-R1R2 10 match ip address 100 action drop ! vlan access-map NO-R1R2 20 match ip address 101 // 생략 가능 action forward // 생략 가능 ! vlan filter NO-R1R2 vlan-list 10,20

○ **확인 명령어**

- **show vlan access-map**

- show vlan filter

6. PBACL(Policy-based ACL)

○ IP주소나 Port 번호를 Object Group으로 정의하고 ACL을 만들 때 이들을 불러 사용하는 것
- Object Group은 IP 주소 그룹이나 프로토콜 포트 그룹별로 정의할 수 있다.
- PBACL은 L3 Interface(Routed, SVI)에 적용되며, IPv4만 제어할 수 있고, 이름을 사용한 ACL만 사용할 수 있다. Low End 스위치에서는 지원되지 않는다.

○ IP 주소 Object Group 설정
- object-group ip address MYO1
- host 1.1.1.1
- host 2.2.2.2
- 1.1.3.0 255.255.255.0

○ 프로토콜 Port Object Group 설정
- object-group ip port MYO2
- eq 200
- gt 500
- neq 700

○ PBACL 만들기
- ip access-list extended PBACL
- permit tcp addrgroup MYO1 portgroup MYO2 any
- deny tcp any

○ 적용
- ip access-group PBACL in

○ 확인
- show ip access-lists
- show ip access-lists PBACL expand