네트워크

■ Port Security(스위치에서의 포트 보안)
L2 기반의 장비인 스위치는 MAC주소를 기반으로 통신을 한다.
포트 당 학습할 수 있는 맥 주소를 제한 할 수 있다.
특정(ex)DDos 공격) 컴퓨터의 침입을 MAC주소를 통해 차단 할 수 있다.

[조건]
- 정적 액세스 포트에서만 가능
- 이더 채널에는 설정이 안됨
- 포트 보안만으로는 보안 문제는 완전히 해결이 되지는 않는다.

[설정방법]
- 인터페이스에 들어간다.
- access 모드 설정
- port security를 활성화
- 위의 인터페이스로부터 학습할 최대 MAC주소 개수 설정

[포트보안의 학습방식]
- static : 정적으로 MAC주소를 입력하여 포트보안 설정
- dynamic : 동적으로 MAC주소를 학습하여 포트보안 설정
  학습한 주소는 NVRAM에 저장 할 수 없다.
- sticky : 동적으로 학습하고 running-config에 기록을 한다.

[위반시 모드]
- protect : 현 상태 유지, 위반된 MAC주소의 장비로부터 오는 모든 프레임을 drop
- restrict : 현 상태 유지, 위반된 MAC주소의 장비로부터 오는 모든 프레임을 drop, 로그에 기록
- shutdown : 위반시 포트 상태를 비활성시킨다..

```
Switch>en
Switch#conf t
Switch(config)#int f 0/1
Switch(config-if)#sw m a
Switch(config-if)#sw port-security
Switch(config-if)#sw port ?
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>
Switch(config-if)#sw port mac-address 0000.0000.1111
```

```
Switch(config-if)#sw port maximum 1
Switch(config-if)#sw port vi ?
  protect    Security violation protect mode
  restrict   Security violation restrict mode
  shutdown   Security violation shutdown mode
Switch(config-if)#sw port vi p
```

■ ACL(Access List)

- Network에 접근 여부를 허용할지 말지를 결정하는 리스트(필터링)
- 라우터에서 설정한다고 네트워크 계층까지가 아니라 응용 계층의 부분까지 관리하기에 L3라고 단정할 수는 없다.(물리계층에서 응용계층까지 완벽히 막을 수 없기 때문에 더 많은 보안 기능이 있는 전문 방화벽 장비를 사용한다.)
- ACL은 크게 numbered와 named로 구분이 된다.

● Numbered ACL

1) Standard ACL (표준) : source address(출발지 주소)만 참조를 하여 필터링 (1~99)
2) Extended ACL (확장) : 출발지, 목적지, 프로토콜, 포트 등을 참조한다. (100~199)

<ACL 법칙>

1) ACL은 맨윗줄부터 순서대로 수행된다. 때문에 ACL은 좁은 범위 먼저 설정하고 넓은 범위로 설정해야 한다.
만약 아래처럼 넓은 범위를 먼저 설정하면 모든 패킷이 허용된다.(필터링 효과가 없다)

```
Router(Config)#access-list (1~99) permit any
Router(Config)#access-list (1~99) deny 125.101.1.0 0.0.0.255
```

2) ACL의 맨 마지막은 deny any가 생략되어 있다. 즉. 마지막 줄에 permit any가 없을 경우 ACL 조건에 없는 모든 주소는 deny된다.

```
Router(Config)#access-list (1~99) deny 125.101.1.0 0.0.0.255
Router(Config)#access-list (1~99) permit any
```

※ deny 설정하고 마지막 줄은 permit으로 해야 함.

3) 숫자형 ACL은 순서대로 입력되기 때문에 중간 삽입이나 중간 삭제는 불가능하다.
즉, 중간의 리스트 중 틀린 것이 있어도 수정 삽입 삭제가 안 된다.
별개의 에디터에서 미리 작업을 하고 검증 후 실행시켜야 한다.

4) Interface에 ACL을 정의해야 필터링이 동작한다.

<ACL 동작>

1) Inbound 설정

- 패킷이 라우터 내부로 들어올 때 필터링 여부를 결정

2) Outbound 설정
- 패킷이 라우터 외부로 나갈 때 필터링 여부를 결정

■ Standard ACL
- 출발지 주소를 보고 permit, deny 여부를 결정
- 출발지 주소가 일치하면 ACL의 내용을 수행한다.
- permit이면 패킷을 정해진 경로로 전송하고 deny면 흐름을 막고 'host unreachable'라는 ICMP 메시지를 뿌린다.

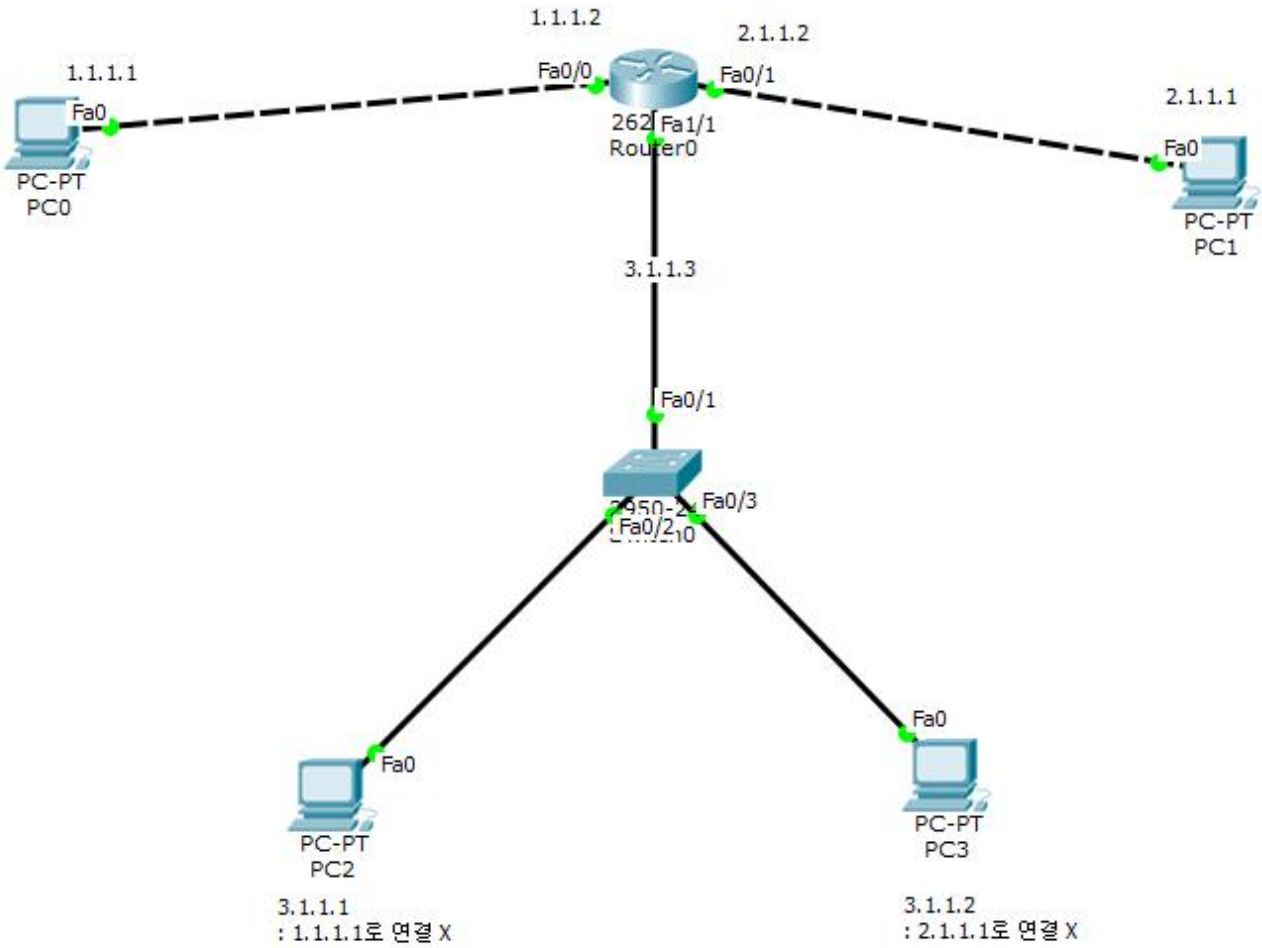
Router(Config)#access-list <list number> {permit | deny} {<source address><wildcardmask> | any}
Router(Config)#int s 0/0
Router(Config-if)#ip access-group <list number> <in | out>

★ 표준 ACL은 항상 목적지의 라우터 쪽에 설정이 되어야 한다.
중간 라우터에 설정을 하면 다른 라우터들까지 영향을 받아서 정상적인 패킷 전송이 안 될 수 있다.

ex1) 210.100.8.2 /32 출발지로 가진 패킷이 Router에 들어오지 못하게 차단하세요(s 0/0)
Router(Config)#access-list 10 deny 210.100.8.2 0.0.0.0
Router(Config)#access-list 10 permit any
Router(Config)#int s 0/0
Router(Config-if)#ip access-group 10 in

ex2) 190.150.82.21 /32 출발지로 가진 패킷만 Router에 들어오게 설정하세요(s 0/1)
Router(Config)#access-list 11 permit 190.150.82.21 0.0.0.0
Router(Config)#int s 0/1
Router(Config-if)#ip access-group 11 in

ex3) 51.100.92.8 /32 출발지인 가진 패킷을 Router를 통해 외부로 나가지 못하게 설정하세요(s 0/0)
Router(Config)#access-list 12 deny 51.100.92.8 0.0.0.0
Router(Config)#access-list 12 permit any
Router(Config)#int s 0/0
Router(Config-if)#ip access-group 12 out



Router(Config)#access-list 1 deny host 3.1.1.1
Router(Config)#access-list 1 permit any
Router(Config)#access-list 2 deny host 3.1.1.2
Router(Config)#access-list 2 permit any
Router(Config)#int f 0/0
Router(Config-if)#ip access-group 1 out
Router(Config)#int f 0/1
Router(Config-if)#ip access-group 2 out

■ Extended ACL

- 출발지와 목적지 주소 모두를 제어한다.
- Standard ACL(표준 ACL)은 TCP/IP만 제어하나 Extended ACL(확장 ACL)은 ip, tcp, udp, icmp 등 상세 프로토콜을 선택할 수 있다.
- 100~199

Router(Config)#access-list <list number> {permit | deny} <protocol> <source address><wildcardmask><destination address> <wildcardmask> <port number>

● Well Known-Port
TCP : FTP(20, 21), TELNET(23), SMTP(25), HTTP(80), HTTPs(443)
UDP : DNS(53), TFTP(69), DHCP(67,68)
※ IP주소 + 포트번호 = 소켓번호

ex1) Router에 들어오는 트래픽 중 목적지가 210.150.6.0 /24인 네트워크에 있는 트래픽을 모두 차단 하세요
Router(Config)#access-list 101 deny ip any 210.150.6.0 0.0.0.255
Router(Config)#access-list 101 permit ip any any
Router(Config)#int s 0/0
Router(Config-if)#ip access-group 101 in

ex2) 들어오는 트래픽 중 출발지가 200.101.52.0/24 네트워크 만이 129.29.31.0/24 네트워크에 있는 FTP와 Telnet 서버에 접속할 수 있도록 하세요
Router(Config)#access-list 110 permit tcp 200.101.52.0 0.0.0.255 129.29.31.0 0.0.0.255 equal 20
Router(Config)#access-list 110 permit tcp 200.101.52.0 0.0.0.255 129.29.31.0 0.0.0.255 equal 21
Router(Config)#access-list 110 permit tcp 200.101.52.0 0.0.0.255 129.29.31.0 0.0.0.255 equal 23
Router(Config)#int s 0/1
Router(Config-if)#ip access-group 110 in

ex3) 197.2.13.1/32에서 나가는 트래픽 중 HTTP와 TFTP만을 차단하고 그 외에는 모두 허용하세요.
Router(Config)#access-list 111 deny tcp host 197.2.13.1 any equal 80
→ Router(Config)#access-list 111 deny tcp 197.2.13.0 0.0.0.255 any equal 80과 같음
Router(Config)#access-list 111 deny tcp host 197.2.13.1 any equal 69
Router(Config)#access-list 111 permit ip any any
Router(Config)#int s 0/0
Router(Config-if)#ip access-group 111 in

ex4) Router로 들어오는 트래픽 중 목적지가 HTTP서버(210.11.102.10) FTP서버(190.20.81.1)인 트래픽만 들어올 수 있도록 설정하세요.
Router(Config)#access-list 120 permit tcp any host 201.11.102.10 equal 80
Router(Config)#access-list 120 permit tcp any host 190.20.81.1 equal 20
Router(Config)#access-list 120 permit tcp any host 190.20.81.1 equal 21
Router(Config)#int s 0/1
Router(Config-if)#ip access-group 120 in

■ Named ACL
- 번호로 계속해서 ACL을 생성할 경우 서로 구분하기 어렵다. 이 때 문자로 구성하게 되면 구분이 쉽다.
- 표준과 확장이 있다.

- show ip access-list(sh ip ac)

<설정 방법>
Router(Config)#ip access-list standard <text-name>
Router(Config-std-nacl)#{permit | deny} <source address> <wildcard mask>
Router(Config-std-nacl)#exit
Router(Config)#int s 0/0
Router(Config-if)#ip access-group <ACL text name> {in | out}

ex) 출발지가 210.100.10.10/32인 패킷을 Named ACL을 사용하여 라우터에 들어오지 못하게 차단하세요
Router(Config)#ip access-list standard Deny_210
Router(Config-std-nacl)#deny host 210.100.10.10
Router(Config-std-nacl)#permit any
Router(Config-std-nacl)#exit
Router(Config)#int s 0/0
Router(Config-if)#ip access-group Deny_210 in