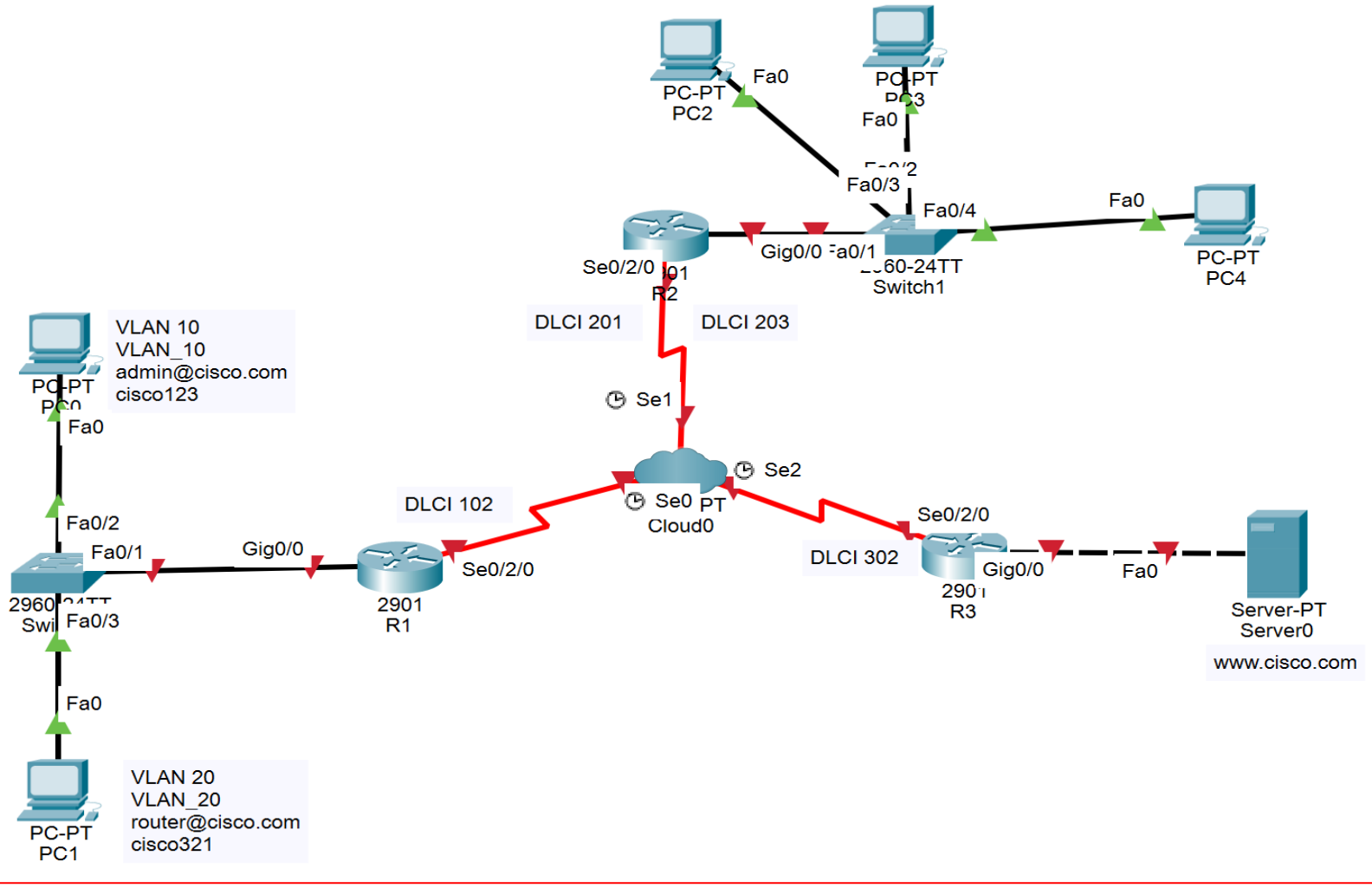
네트워크 운용관리 11주차

김정윤 교수

Frame-Relay 연습



네트워크 보안을 위한 접근제어 목록 1

1. ACL(Access Control List) 동작

1) ACL 이란?

① 라우터는 출발지 주소와 목적지 주소를 참고하여 라우팅 테이블을 기초해 패킷 전달 장치이며, ACL은 이러한 주소를 기반으로 하여 만든 패킷 출입 통제 문장

② ACL을 이용하면 IP 주소 기반으로 패킷의 전달 여부를 통제할 수 있을 뿐만 아니라 특정 프로토콜을 사용하는 패킷을 전달하지 않을 수 있는데, 이러한 일련의 과정을 패킷 필터링(Packet Filtering)이라고 한다

③ 특정 프로토콜을 사용하는 패킷의 전달 유무는 포트 번호를 기반으로 한다

④ ACL을 사용하는 목적은 라우터 보안 이기도 하지만, 네트워크의 트래픽을 제어하는 목적도 있다

ex) 내부 사용자들이 외부의 FTP로 부터 많은 파일을 다운로드 받거나, 비디오 스트리밍 서비스를 통해 외부에서 내부로 트래픽이 많이 들어온다면, 이를 제한할 수 있다

네트워크 보안을 위한 접근제어 목록 1

⑤ 네트워크 트래픽은 2가지가 존재하는데 하나는 들어오는 트래픽(Inbound Traffic)이며, 또 다른 하나는 나가는 트래픽(Outbound Traffic)이다

⑥ ACL은 패킷이 나가거나 들어오는 방향에 관리자가 선택한 라우터 인터페이스에 설정 된다

⑦ Inbound Traffic

- 패킷이 라우터 내부로 들어올 때 Filtering 여부를 결정한다
- 라우터 인터페이스로 패킷이 들어올 경우 패킷을 수신 하는 인터페이스에 ACL이 설정되어 있는지 확인하고, 설정이 되어 있지 않으면 그냥 통과
- 만약 ACL이 설정되어 있다면, 들어온 패킷의 정보와 ACL의 설정 내용을 비교 후, 패킷의 통과 여부를 결정

⑧ Outbound Traffic

- 패킷이 라우터 외부로 나갈 때 Filtering 여부를 결정한다
- 라우터 인터페이스에서 패킷이 나갈 경우 패킷이 나가는 인터페이스에 ACL이 설정되어 있는지 확인하고 설정되어 있지 않으면 그냥 통과

네트워크 보안을 위한 접근제어 목록 1

⑨ Permit은 허용을 의미하며, Deny는 거절을 의미한다

⑩ ACL은 윗줄부터 순서대로 수행 하기 때문에 문장의 순서가 매우 중요하며, 따라서 반드시 좁은 범위부터 작성이 되어야 한다. 만약 잘못 작성이 되면 Filtering이 되지 않아 ACL이 동작하지 않게 되므로 유의 한다

ex) permit any => 모든 것을 허용한다

deny 203.230.7.0 0.0.0.255 => 203.230.7.0/24 네트워크는 거절한다

- 위의 문장에서 permit any가 먼저 선언되었음으로, deny 203.230.7.0 0.0.0.255 문장은 동작하지 않게 된다. 그러므로 위의 문장은 순서가 바뀌어야 제대로 동작하게 된다

ex) deny 203.230.7.0 0.0.0.255

permit any

⑪ 발신지 주소와 목적지 주소, 그리고 TCP와 UDP의 포트번호를 기반으로 통신이 되므로, 이를 사용하여 ACL을 작성할 수 있다

네트워크 보안을 위한 접근제어 목록 1

2. ACL(Access Control List) 종류

1) Standard Access-list

① 단순히 Source IP 주소만을 판단해 Traffic을 제어하고자 할 때 사용

② ACL 번호로 1-99번, 1300-1999 사이의 번호를 사용

③ 특정 프로토콜을 사용하는 패킷을 제어할 수 없음. 이유는 단순히 Source IP 주소만 판단해 Traffic을 제어

④ Permit 이면 패킷을 전송하고, Deny면 패킷을 드롭 시켜 흐름을 차단한다

⑤ R1(config)#access-list <list-number> {permit|deny} source [mask]

1 2 3 4

- 1 : list-number는 1-99, 또는 1300-1999 사이의 번호를 사용
- 2 : permit|deny는 패킷을 전달할지 드롭 시킬지 결정
- 3 : 출발지 주소 입력
- 4 : 출발지 주소의 와일드카드마스크 입력

네트워크 보안을 위한 접근제어 목록 1

⑥ R1(config)#interface serial 0/2/0

R1(config)#ip access-group <access-list-number> {in | out}

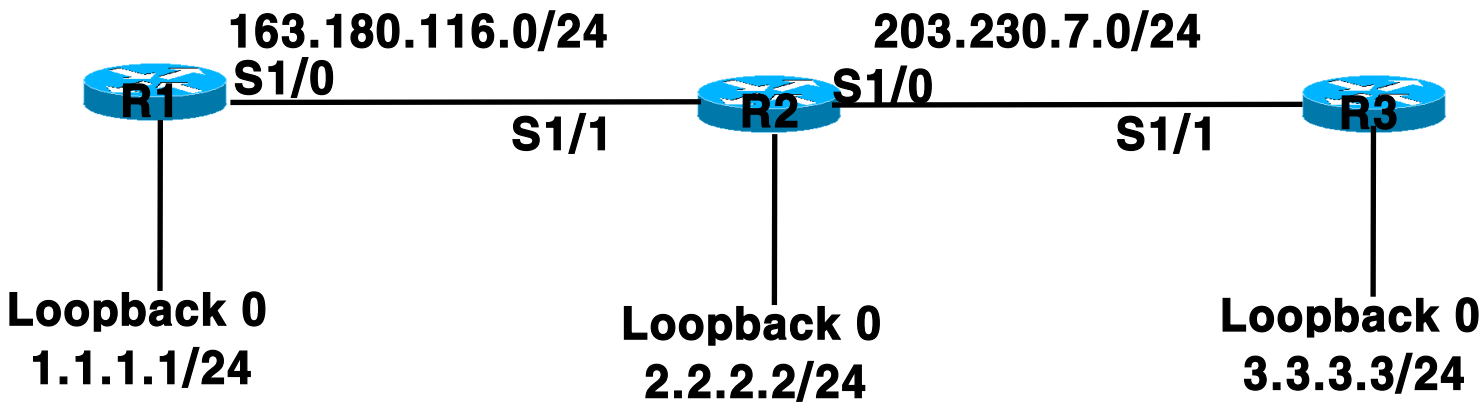
- 1 : access-list-number를 사용하여 앞서 작성한 ACL을 불러온다
- 2 : in | out 에서 in은 패킷이 들어오는 것이고, out 은 패킷이 나가는 것을 의미

⑦ Standard ACL은 항상 목적지 라우터 쪽에 설정되어야 한다. 만약 중간 라우터에 설정하면 다른 라우터까지 ACL의 영향을 받아 정상적으로 패킷 전송이 이루어지지 않을 수 있다

⑧ Standard ACL은 순서대로 입력되기 때문에 중간에 ACL 문장을 삽입하거나 삭제하는 것이 불가능하다

⑨ 만약 ACL 작성이 잘못되었으면 기존에 작성된 ACL 문장을 다 지우고 처음 부터 다시 작성하여야 한다

네트워크 보안을 위한 접근제어 목록 1



Ex) R1의 Loopback 0가 출발지 주소일 경우 R3에게 Ping을 보낼 수 없도록 R2에 Standard ACL을 설정해보자.

1) R2(config)# access-list 1 deny 1.1.1.0 0.0.0.255
2) R2(config)# access-list 1 permit any
   R2(config)# int S1/1
3) R2(config-if)# ip access-group 1 in

네트워크 보안을 위한 접근제어 목록 1

Ex) 결과 확인

R1#ping 3.3.3.3 source 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

U.U.U

Success rate is 0 percent (0/5)

- Standard Access-list는 패킷이 들어오면 단순히 IP 주소만으로 Permit 과 Deny를 결정한다.
- 위의 토폴로지에서는 ICMP만 확인하였지만, 다른 프로토콜도 마찬가지로 패킷을 전송할 수 없다.
- 이러한 이유로 Extended Access-list를 사용한다.

네트워크 보안을 위한 접근제어 목록 1

2) Extended Access-list

① 출발지와 목적지의 IP 주소 모두를 조건으로 보고 제어한다

② 이와 더불어 IP, TCP, UDP, ICMP등의 상세 프로토콜을 선택해서 제어할 수 있다

③ ACL 번호로 100-199번, 2000-2699 사이의 번호를 사용

```
R1(config)#access-list <list-number>   {permit|deny}   <protocol>
                                  1              2            3
source [mask] destination [mask]   [operator port]
   4                  5                  6
```

1 : list-number는 100-199, 2000-2699까지의 번호를 사용한다.

2 : 조건에 맞는 트래픽을 permit할지 deny할지 결정한다.

3 : Filtering을 할 프로토콜을 정의한다. (TCP, UDP, IP 등)

4 : source address를 지정한다. 5 : destination address를 지정한다.

6 : 목적지 TCP/UDP 포트 이름 및 번호를 지정한다.

네트워크 보안을 위한 접근제어 목록 1

④ Interface 적용

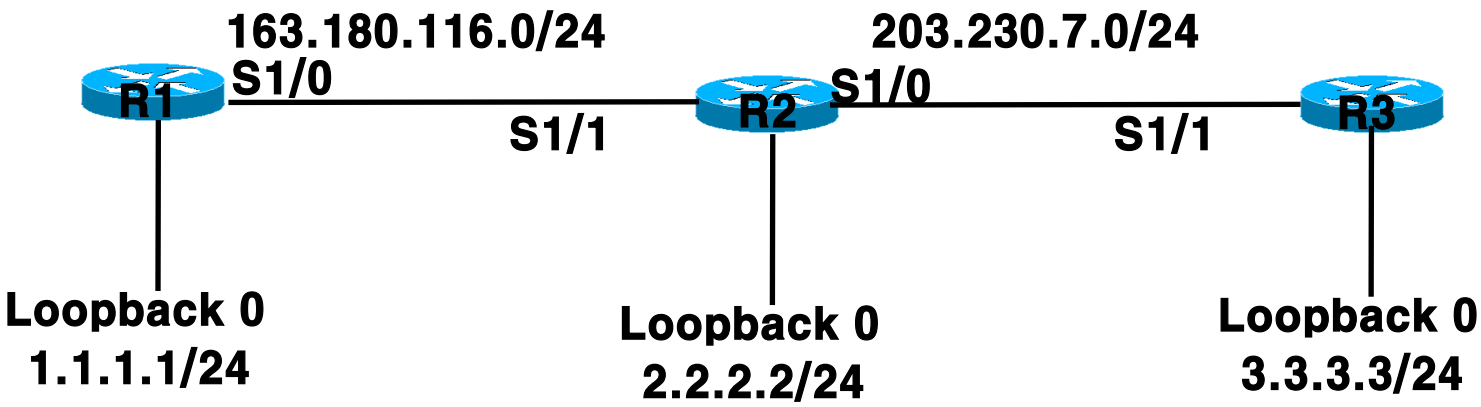
```
R1(config)#interface serial 0/0
R1(config-if)#ip access-group <access-list-number> {in | out}
                                        1              2
```

- 1 : 앞에서 정의한 ACL을 불러와서 filtering 내용을 인터페이스에 적용한다.
- 2 : inbound와 outbound 설정.
- in은 라우터의 인터페이스로 packet이 들어오는 경우, out은 packet이 라우터 인터페이스에서 나가는 경우

⑤ Extended ACL은 순서대로 입력되기 때문에 중간에 ACL 문장을 삽입하거나 삭제하는 것이 불가능하다

⑨ 만약 ACL 작성이 잘못되었으면 기존에 작성된 ACL 문장을 다 지우고 처음 부터 다시 작성하여야 한다

네트워크 보안을 위한 접근제어 목록 1



Ex) R1은 R3에게 Ping을 보내지 못하도록 R2에 ACL을 설정하여라

1) R2(config)#access-list 100 deny icmp any any echo log-input
2) R2(config)#access-list 100 permit ip any any
   R2(config)#int s1/1
3) R2(config-if)#ip access-group 100 in
   R2(config-if)#exit

네트워크 보안을 위한 접근제어 목록 1

Ex) 결과 확인

R1#ping 3.3.3.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

R3#ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5)

- R1에서 R3로 ping을 보낼 수 없지만, R3에서 R1으로 Ping을 보낼 수 있는 상황을 잘 살펴보자

고생하셨습니다.

다음 수업시간에 뵙겠습니다.