네트워크 운용관리 12주차

김정윤 교수

네트워크 보안을 위한 접근제어 목록 2

1. 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 2

⑥ R1(config)#interface serial 0/2/0

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

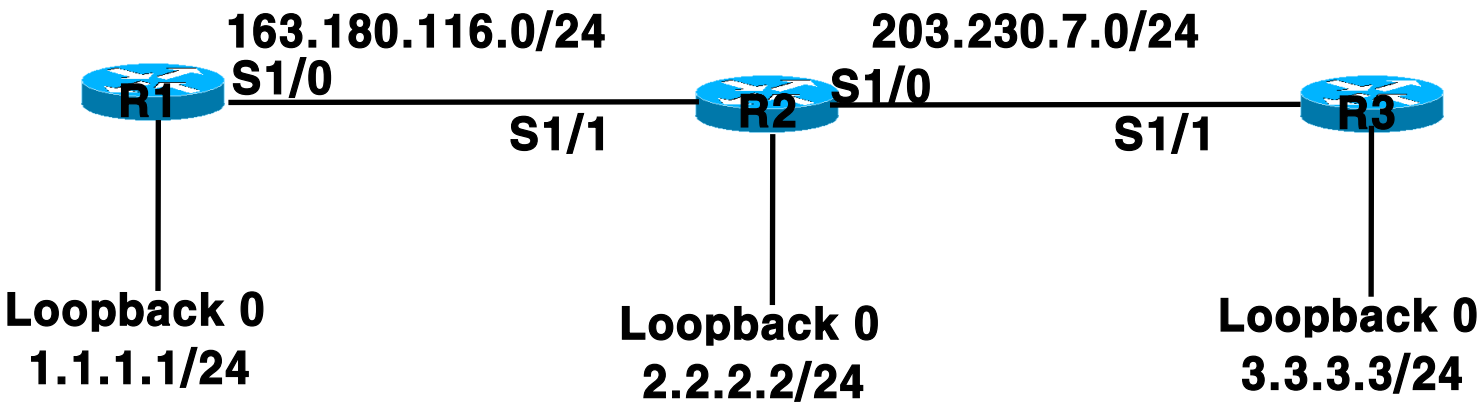
- 1 : access-list-number를 사용하여 앞서 작성한 ACL을 불러온다
- 2 : in | out 에서 in은 패킷이 들어오는 것이고, out 은 패킷이 나가는 것을 의미

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 2



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 2

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 2

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 2

④ Interface 적용

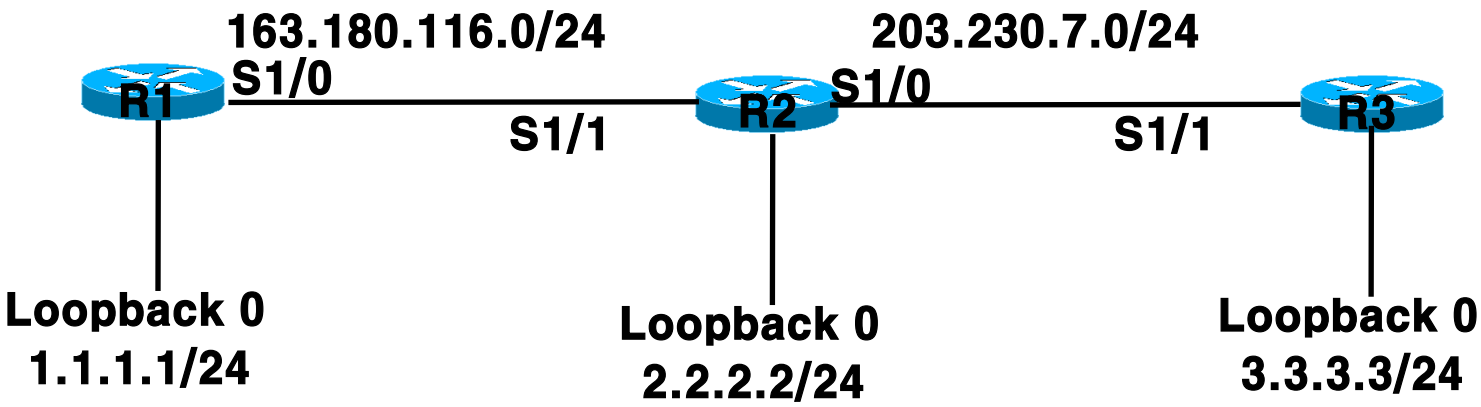
```
R1(config)#interface serial 0/0
R1(config-if)#ip access-group <access-list-number> {in | out}
                                        1              2
```

- 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 2



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 2

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

네트워크 보안을 위한 접근제어 목록 2

3) Named Access-list

① 번호를 사용하지 않고 관리지가 정한 이름을 사용하여 Access-list를 정의함

② Named standard Access-list와 Named Extended Access-list 두 종류가 있으며, Standard와 Extended의 특성은 똑같고, 단지 이름 정의를 하여 사용한다는 점만 다름.

Ex) Named Standard Access-list

```
R1(config)#ip access-list standard mega
R1(config-std-nacl)#deny 1.1.1.0 0.0.0.255
R1(config-std-nacl)#permit any
R1(config-std-nacl)#exit
R1(config)#int s1/0
R1(config-if)#ip access-group mega out
```

네트워크 보안을 위한 접근제어 목록 2

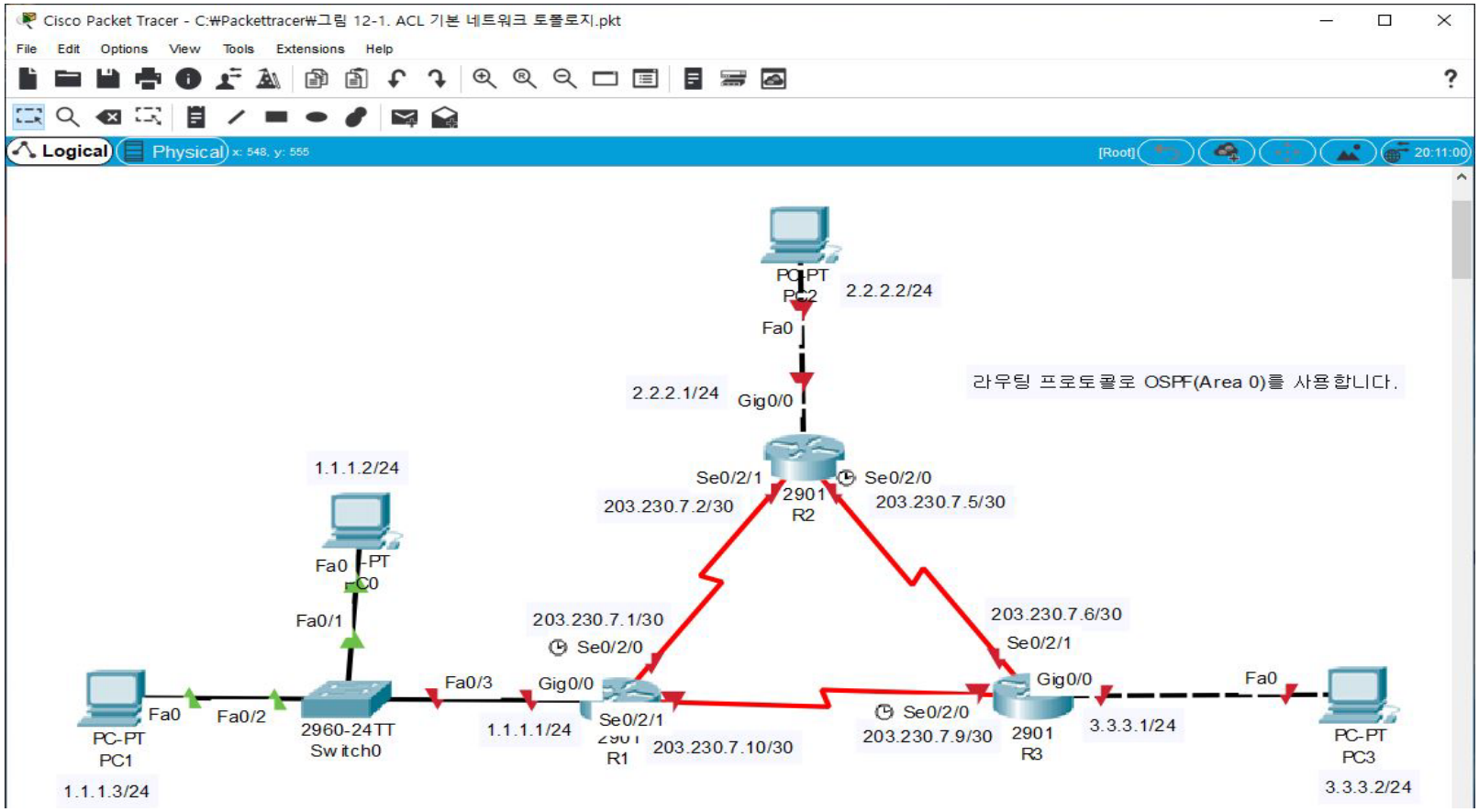
Ex) Named Extended Access-list

```
R1(config)#ip access-list extended mega
R1(config-ext-nacl)#deny tcp any any eq telnet
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int s1/0
R1(config-if)#ip access-group mega in
R1(config-if)#
```

네트워크 보안을 위한 접근제어 목록 2

4) Access-list 기본 토폴로지

① Access-list를 실습하기 위하여 아래와 같이 토폴로지를 구성한다

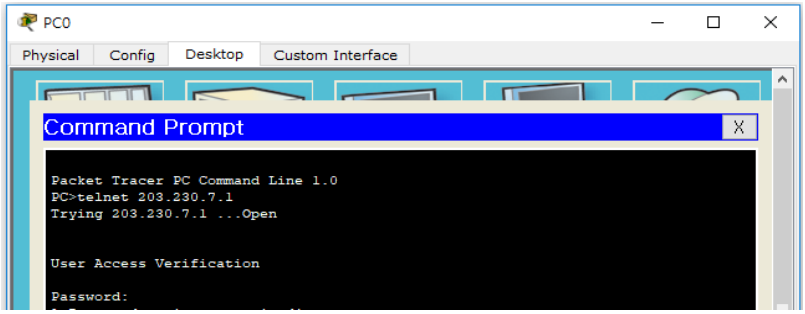


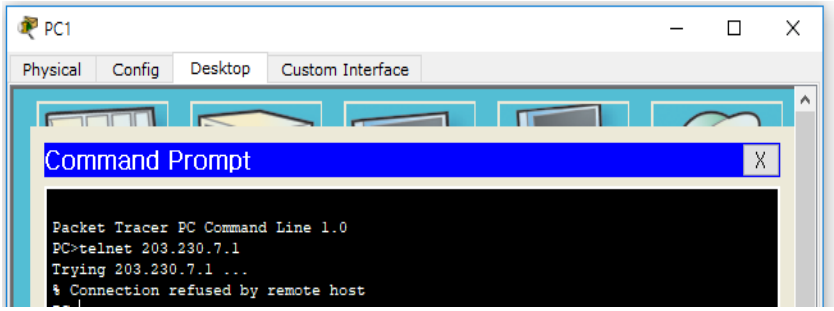
네트워크 보안을 위한 접근제어 목록 2

② R2에 PC0번만 Telnet 접속이 가능하도록 설정하시오

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 permit 1.1.1.2 0.0.0.0
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#access-class 1 in
R2(config-line)#exit
R2(config)#
```

- 결과 확인



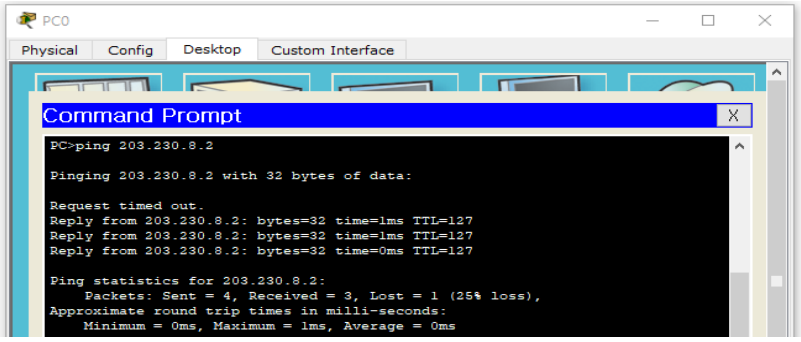


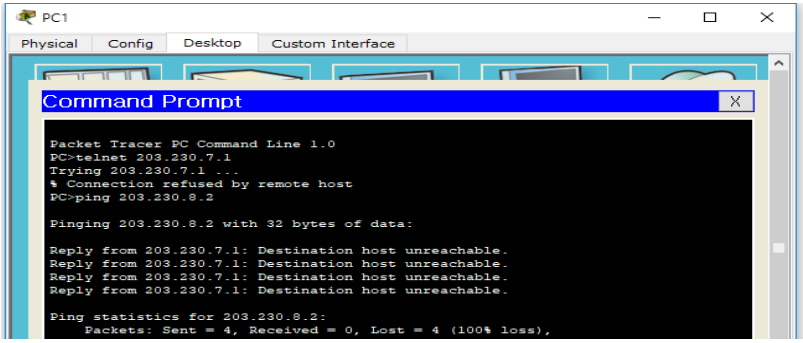
네트워크 보안을 위한 접근제어 목록 2

③ PC0번만 PC3에게 Ping을 보낼 수 있도록 ACL을 작성하시오

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 1 permit 1.1.1.2 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#int gi0/0
R1(config-if)#ip access-group 1 in
R1(config-if)#exit
R1(config)#
```

- 결과 확인





고생하셨습니다.

다음 수업시간에 뵙겠습니다.