

제7장 ACL

(Access Control List-접근 제어 항목)

1. ACL

2. 와일드카드 마스크

- 서브넷마스크와 다르게 0과 1이 반대로 되어있다.
- 규칙이 없는 마스크

ACL 은 와일드카드 마스크를 이용하여 IP 주소 및 서브넷을 정의한다. 와일드카드 마스크는 서브넷 마스크처럼 '1'이 연속되어야 하는 규칙이 없는 마스크이기 때문에 서브넷 마스크로 간결하게 정의할 수 없는 서브넷 또는 IP 주소들을 간결하게 설정할 수 있다.

비트 처리	서브넷 마스크	와일드카드 마스크
크기	32bit	32bit
공통비트	1	0
비공통 비트	0	1
규칙	1 이 연속되어야 함	규칙이 없음

서브넷 마스크 → 와일드카드 마스크

ex1)

255.255.255.255	0.0.0.0
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255
255.0.0.0	0.255.255.255
0.0.0.0	255.255.255.255
255.255.255.252	0.0.0.3
255.255.255.248	0.0.0.7
255.255.255.240	0.0.0.15
255.255.255.224	0.0.0.31
255.255.255.128	0.0.0.127
255.255.254.0	0.0.1.255
255.255.240.0	0.0.15.255

Ex2) 192.168.1.0/24 ~ 192.168.255.0/24 중에 3 번째 옥텟이 홀수인 서브넷을 한줄로 설정하여라

```

192.168.00000000 1.0
192.168.00000001 1.0
192.168.00000010 1.0
~
192.168.11111111 1.0
-----> 192.168.1.0 0.0.254.255
0. 0.11111111 0.255 <- 0.0.254.255
  
```

Ex3) 192.168.1.0/24 ~ 192.168.255.0/24 중에 3 번째 옥텟이 짝수인 서브넷을 한줄로 설정하여라

```
192.168.00000001 0.0
192.168.00000010 0.0
192.168.00000011 0.0
~
192.168.11111111 0.0
-----> 192.168.0.0 0.0.254.255
0. 0.11111111 0.255 <- 0.0.254.255
```

Ex4) 192.168.112.32 ~ 192.168.112.63 IP 주소를 한줄로 설정하여라.

```
192.168.112.001 00000
192.168.112.001 00001
192.168.112.001 00010 I
~
192.168.112.001 11111
-----> 192.168.112.32 0.0.0.31
0. 0. 0.000 11111 <- 0.0.0.31
```

Ex5) A 클래스 IP 주소를 한줄로 설정하여라.

```
0.0.0.0 ~ 127.255.255.255
0 0000000. 0 1111111.
0 1111111.

0.0.0.0 127.255.255.255
```

Ex6) B 클래스 IP 주소를 한줄로 설정하여라.

```
128.0.0.0 ~ 191.255.255.255
10 000000. 10 111111.
00 111111.

128.0.0.0 63.255.255.255
```

Ex7) C 클래스 IP 주소를 한줄로 설정하여라.

192.0.0.0 ~ 223.255.255.255
110 00000. 1 110 11111.
000 11111.

192.0.0.0 31.255.255.255

Ex8) A 클래스 사설 IP 주소를 한줄로 설정하여라.

0.0.0.0 ~ 127.255.255.255
0 0000000. 0 1111111.
0 1111111.

0.0.0.0 127.255.255.255

Ex9) B 클래스 사설 IP 주소를 한줄로 설정하여라

172.16.0.0 ~ 172.31.255.255

172.0001 0000.0.0

172.0001 0001.0.0

172.0001 0010.0.0

~

172.0001 1111.0.0

-----> 172.16.0.0 0.15.255.255
0.0000 1111.255.255 <- 0.15.255.255^I

Ex10) C 클래스 사설 IP 주소를 한줄로 설정하여라.

192.168.0.0 ~ 192.168.255.255

192.168.0.0 0.0.255.255

Ex11) IP 주소 적체를 확줄로 설정하여라.

0.0.0.0 255.255.255.255 -> any

Ex12) 13.13.10.100 IP 주소 1 개를 설정하여라

13.13.10.100 0.0.0.0 -> host 13.13.10.100

Ex13) 199.172.1.0/24, 199.172.3.0/24 를 한줄로 설정하여라

```
199.172.000000 0 1.0
199.172.000000 1 1.0
-----> 199.172.1.0 0.0.2.255
0. 0. 000000 1 0.255 ← 0.0.2.255
```

Ex14) 199.172.1.0/24 ~ 199.172.3.0/24, 199.172.8.0/24 ~ 199.172.11.0/24 를 확줄로 설정하여라

```
199.172.0000 0 0 01.0
199.172.0000 0 0 10.0
199.172.0000 0 0 11.0
199.172.0000 1 0 00.0
199.172.0000 1 0 01.0
199.172.0000 1 0 10.0
199.172.0000 1 0 11.0
-----> 199.172.0.0 0.0.11.255
0. 0. 0000 1 0 11.255 ← 0.0.11.255
```

Ex15) 199.172.5.0/24, 199.172.7.0/24, 199.172.10.0/24, 199.172.14.0/24 를 두줄로 설정하여라.

```
199.172.000001 0 1.0
199.172.000001 1 1.0
-----> 199.172.5.0 0.0.2.255
0. 0. 000000 1 0.255 ← 0.0.2.255

199.172.00001 0 10.0
199.172.00001 1 10.0
-----> 199.172.10.0 0.0.4.255
0. 0. 00000 1 00.255 ← 0.0.4.255
```

ACL (Access Control List) - 접근 제어 항목

네트워크에서 전송되는 트래픽을 제어하는 것은 보안적인 관점에서 중요한 이유이다. 이때, ACL은 트래픽 필터링과 방화벽을 구축하는데 가장 중요한 요소일 뿐만 아니라 라우팅 환경에서 서브넷과 호스트를 정의하는 경우에도 필요하다

3. ACL 설정시 파악할 요소

- ① 출발지와 목적지를 파악한다.
- ② 패킷을 허용(permit) 할 것인지, 차단(deny) 할 것인지 파악한다.
- ③ ACL 를 인바운드로 적용할 것인지, 아웃바운드로 적용할 것인지 파악한다.
- ④ 추가적으로 파악할 요소로는 서비스 유형 및 포트 번호, TCP 플래그 정보, IP Fragments 정보 등이 있다.
- ⑤ ACL 은 패킷을 허용하거나 차단할때, IP 헤더부터 IP 상위 계층 헤더 정보까지만 검사한다.


프로토콜	계층	보안 정책
HTTP, FTP, TELNET....	L7	IDS/IPS(snort, suricata), WAF(웹 애플리케이션 방화벽)
TCP, UDP, ICMP, EIGRP, OSPF....	L4	ACL, Firewall, IDS/IPS(snort, suricata)
IP	L3	ACL, Firewall, IDS/IPS(snort, suricata)

- 1,2,3 은 기본적으로 파악해야한다.
- ACL은 검사할 수 있는 범위가 있다 (L4까지만 검사가 가능하다)
 - IP header, TCP header, UDP, ICMP 까지만 검사를 한다.
 - HTTP 안에 들어있는건 검사를 못한다. (L7쪽은 불가능하다)

4. ACL 처리 과정 및 주의 사항

- 1) 서브넷 범위가 작은 항목부터 설정해야 한다.

13.13.0.0/16	차단
13.13.30.0/24	허용
13.13.0.0/16	허용
13.13.30.0/24	차단



설정된 순서대로 동작을 한다. 따라서 순서가 중요하다.

ex) 범위가 큰 서브넷을 먼저 설정:

```
R1#conf t
R1(config)#access-list 10 permit 13.13.0.0 0.0.255.255
R1(config)#access-list 10 deny 13.13.30.0 0.0.0.255
R1(config)#int s1/0
R1(config-if)#ip access-group 10 in
R1(config-if)#end
R1#show ip access-lists
```

```
Standard IP access list 10
 10 permit 13.13.0.0 0.0.255.255
 20 deny 13.13.30.0 0.0.0.255
```

- 범위가 큰 서브넷을 허용하는 설정이 순서 번호 10 번에 있기 때문에 F(13.13.30.3)를 차단하지 않는다.
 - 따라서 범위가 크게 앞에 있으면 안된다. (뒤에 있는 범위까지 닿지 않는다.)
- 10, 20은 검사하는 순서이다. (sequence number, 10→20)
- 설정한 아이피는 출발지이다.

- ACL 을 삭제한다.

```
R1#conf t
R1(config)#no access-list 10
```

ex) 범위가 작은 서브넷을 먼저 설정:

```
R1(config)#access-list 10 deny 13.13.30.0 0.0.0.255
R1(config)#access-list 10 permit 13.13.0.0 0.0.255.255
R1(config)#
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip access-list
Standard IP access list 10
 10 deny 13.13.30.0 0.0.0.255
 20 permit 13.13.0.0 0.0.255.255
R1#
```

- 범위가 작은 서브넷 → 큰 서브넷으로 확장되었음으로 차단된다.

2) ACL 마지막 항목 'deny any' 처리

1. 전체차단하는 경우

```
R1#conf t
R1(config)#access-list 10 deny 13.13.30.0 0.0.0.255
R1(config)#end
R1#show ip access-lists
```

```
Standard IP access list 10
  10 deny 13.13.30.0 0.0.0.255
    // 마지막에 'deny any' 처리 실시
```

- 보이지는 않지만 마지막에 모든 아이피를 차단시킨다.

2. 나머지 전체 허용이 필요한 경우

```
R1#conf t
R1(config)#access-list 10 deny 13.13.30.0 0.0.0.255 // 설정되어 있음
R1(config)#access-list 10 permit any // 설정 추가
R1(config)#end
R1#show ip access-lists
```

```
Standard IP access list 10
  10 deny 13.13.30.0 0.0.0.255 (11 match(es))
  20 permit any
```

- 전체차단을 걸고 허용하는 문구를 써줘야 그 아이피 대역을 제외한 나머지 대역들을 허용시켜준다.
- access-list 10 permit any

3) 항목 부분 추가 및 부분 삭제 불가능

1. 항목 추가 불가능

- 출발지 '13.13.20.x'인 패킷을 차단하는 ACL 설정을 추가한다.

```
R1#conf t
```

```
R1(config)#access-list 10 deny 13.13.20.0 0.0.0.255
```

```
R1(config)#end
```

```
R1#show ip access-lists
```

```
Standard IP access list 10
```

```
10 deny 13.13.30.0 0.0.0.255 (11 match(es))
```

```
20 permit any (9 match(es))
```

```
30 deny 13.13.20.0 0.0.0.255
```

- 30번에 추가가 되었음으로 차단이 되지 않는다 (전 20번에서 다 허용을 시켜버린다 -전체허용)

2. 항목 부분 삭제 불가능

```
R1#conf t
```

```
R1(config)#no access-list 10 deny 13.13.20.0 0.0.0.255
```

```
R1(config)#end
```

```
R1#show ip access-lists
```

```
// ACL 항목 1 개를 삭제하면 ACL 전체 항목을 삭제하기 때문에 특정 항목만 삭제할 수 없다.
```

- 하나삭제하면 전체가 다 삭제된다.
- 부분삭제가 되지 않는다

4) Named ACL 을 이용한 항목 부분 추가 및 삭제

- Named ACL 를 이용하면 순서 번호를 직접 입력할 수 있기 때문에 ACL 항목을 부분 추가하거나 부분 삭제를 할 수 있다

1) 순서 번호를 이용한 항목 부분 추가

① 순서 번호를 이용한 항목 부분 추가

```
R1#conf t
```

```
R1(config)#ip access-list standard 10
```

```
R1(config-std-nacl)#?
```

```
<1-2147483647> Sequence Number
```

default	Set a command to its defaults
deny	Specify packets to reject
exit	Exit from access-list configuration mode
no	Negate a command or set its defaults
permit	Specify packets to forward
remark	Access list entry comment

```
R1(config-std-nacl)#15 deny 13.13.20.0 0.0.0.255
```

```
R1(config-std-nacl)#end
```

```
R1#show ip access-lists
```

```
Standard IP access list 10
```

```
10 deny 13.13.30.0 0.0.0.255
```

```
15 deny 13.13.20.0 0.0.0.255
```

```
20 permit any
```

2) 순서 번호를 이용한 부분 삭제

```
R1#conf t
```

```
R1(config)#ip access-list standard 10
```

```
R1(config-std-nacl)#no 15
```

```
R1(config-std-nacl)#end
```

```
R1#show ip access-lists
```

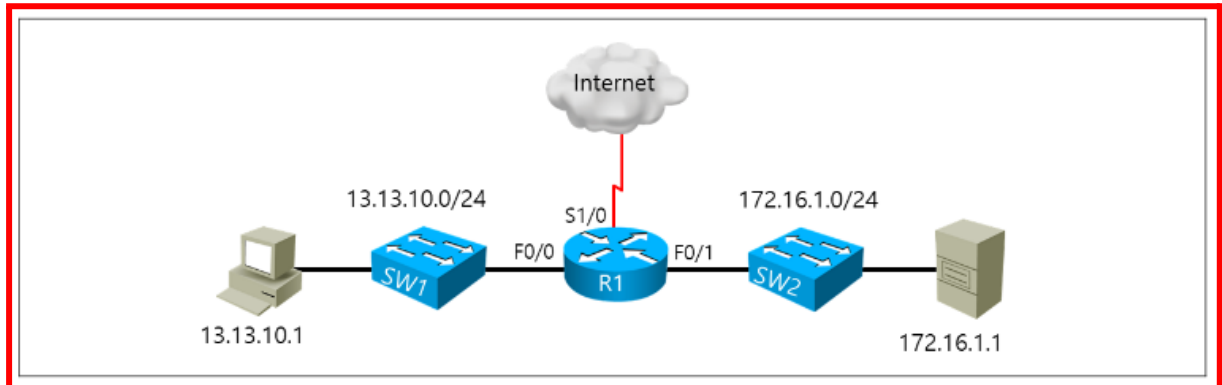
```
Standard IP access list 10
```

```
10 deny 13.13.30.0 0.0.0.255
```

```
20 permit any
```

5. Standard ACL

- ACL 번호는 1~99 까지이며, 패킷의 출발지만 검사하여 패킷을 허용하거나 차단한다
- IP header의 출발지만 검사한다. (Source)



Ex1) '13.13.10.0/24' 사용자들이 '172.16.1.1' 서버에 접근하는 것을 차단한다. 단, 인터넷은 되어야한다.

```
access-list 10 deny 13.13.10.0 0.0.0.255
access-list 10 permit any
!
int fa0/1
ip access-group 10 out
```

- 출발지 10점대는 차단
- 나머지는 허용
- fa0/1에 적용을 시켜서 외부에는 접근가능하게 허용

Ex2) '13.13.10.0/24' 사용자에게 대해서 인터넷 사용을 제한하며, '172.16.1.1' 서버로는 접근이 가능하도록 한다.

```
access-list 10 deny 13.13.10.0 0.0.0.255
access-list 10 permit any
!
int fa0/1
ip access-group 10 out
```

- s1/0이다. 틀림.

Ex3) '172.16.1.1' 서버는 인터넷과 연결된 외부 사용자에게 서비스가 되지 않도록 하며, 오직 '13.13.10.0/24' 사용자에게만 서비스가 가능하도록 한다.

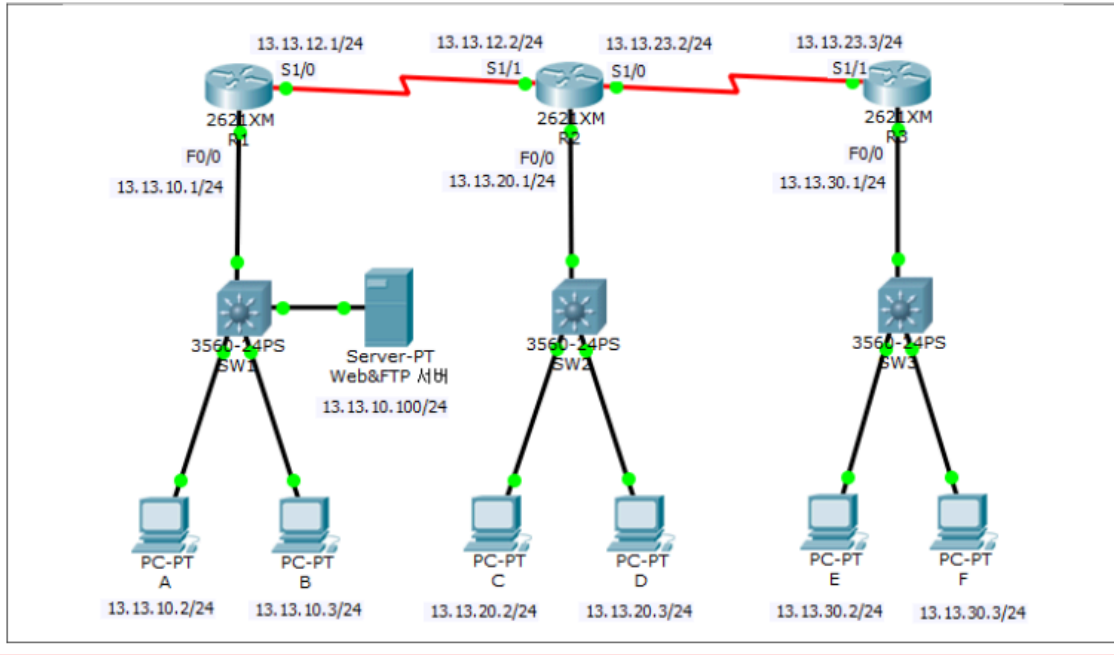
응답 패킷을 아웃바운드로 차단한 경우	요청 패킷을 아웃바운드로 차단한 경우
<pre>access-list 10 deny host 172.16.1.1 access-list 10 permit any ! int s1/0 ip access-group 10 out</pre>	<pre>access-list 10 permit 13.13.10.0 0.0.0.255 ! int fa0/1 ip access-group 10 out</pre>

- 오른쪽이 조금 더 낫다.

Ex4)

Ex4) Standard ACL 예제

- 출발지 '13.13.30.0/24'인 패킷만 '13.13.10.0/24' 서브넷으로 접근하는 것을 차단한다.
- 나머지 패킷들은 허용한다. R1에서 ACL을 구성하도록 한다.



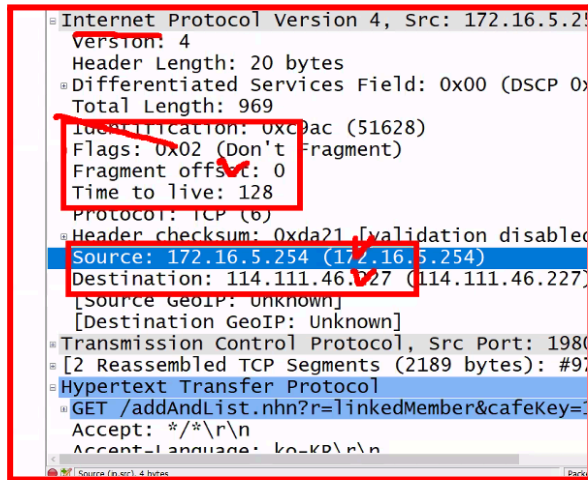
```
@ R1
conf t
access-list 10 deny 13.13.30.0 0.0.0.255
access-list 10 permit any
!
int s1/0
ip access-group 10 in
end
```

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 deny 13.13.30.0 0.0.0.255
R1(config)#access-list 10 permit any
R1(config)#!
R1(config)#int s1/0
R1(config-if)# ip access-group 10 in
R1(config-if)# end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip access-lists
Standard IP access list 10
 10 deny 13.13.30.0 0.0.0.255
 20 permit any
R1#show ip access-lists
Standard IP access list 10
 10 deny 13.13.30.0 0.0.0.255 (96 match(es))
 20 permit any
R1#
```

6. Extended ACL

- ACL 항목으로 사용할 수 있는 범위는 '100~199'까지이며, **출발지 및 목적지를 정의할뿐만 아니라, 패킷이 사용하는 프로토콜과 애플리케이션 프로토콜 포트 번호를 정의하기 때문에 네트워크를 통하여 전송하는 다양한 트래픽들을 검사할 수 있다.** 그리고 다양한 옵션이 제공되므로 시간대별 ACL 필터링, TCP Flag 제어, QoS 관련 설정에서도 사용할 수 있다



- Standard와 달리 다양한 패킷 검사가 가능하다.

Ex1) 출발지 '13.13.10.1'인 PC 가, FTP 서버 '172.16.1.1'로 접근하는 트래픽만 차단한다.

프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
tcp	13.13.10.1	any	172.16.1.1	20, 21

```

access-list 110 deny tcp host 13.13.10.1 host 172.16.1.1 range 20 21
access-list 110 permit ip any any
!
int fa0/0
ip access-group 110 in
  
```

Ex2) 출발지 '13.13.10.1'인 PC 가, 웹-서버 '172.16.1.1'로 접근하는 트래픽만 허용한다.

프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
tcp	13.13.10.1	any	172.16.1.1	80

```

access-list 110 permit tcp host 13.13.10.1 host 172.16.1.1 eq 80
!
int fa0/0
ip access-group 110 in
  
```

Ex3) '172.16.1.1'로 전송하는 ICMP 를 차단하고 나머지는 허용한다. 단, 서버는 외부로 Ping 이 되어야 한다.

프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
icmp	any	-	172.16.1.1	-

```

access-list 110 deny icmp any host 172.16.1.1 echo
access-list 110 permit ip any any
!
int fa0/1
ip access-group 110 out
  
```

- 서버로 가는 echo만 차단하면 서버로 가는 응답만 차단되고 돌아오는 내용은 차단되지 않는다.

안다.	
프로토콜	출발지 IP 주소
icmp	any
	출발지 포트
	-
	1
access-list 110 deny icmp any host 172.16.1.1 echo	13.13.10.1
access-list 110 <u>permit ip any any</u>	ICMP Echo-Reply
!	ICMP Echo
int fa0/1	-----
	SA 13.13.10.1
	DA 172.16.1.1
	SA 172.16.1.1
	DA 13.13.10.1

- 외부에서 오는 에코만 차단시킨다.

Ex4) 출발지 '13.13.10.1'인 PC 가, '172.16.1.0/24'로 접근하는 트래픽을 차단하고 나머지는 허용한다.				
프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
ip	13.13.10.1	-	172.16.1.0/24	-
access-list 110 deny ip host 13.13.10.1 172.16.1.0 0.0.0.255				
access-list 110 permit ip any any				
!				
int fa0/0				
ip access-group 110 in				

Ex5) '13.13.10.1' PC 가 웹-서버 '172.16.1.1'로부터 다운로드하는 트래픽을 차단하고 나머지는 허용한다.				
프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
tcp	172.16.1.1	80	13.13.10.1	any
access-list 110 deny tcp host 172.16.1.1 eq 80 host 13.13.10.1				
access-list 110 permit ip any any				
!				
int fa0/1				
ip access-group 110 in				

Ex6) '13.13.10.0/24' 네트워크에서 '172.16.1.1'로 접근하는 것을 차단하고 나머지는 허용한다.				
프로토콜	출발지 IP 주소	출발지 포트	목적지 IP 주소	목적지 포트
ip	13.13.10.0/24	0	172.16.1.1	-
access-list 110 deny ip 13.13.10.0 0.0.0.255 host 172.16.1.1				
access-list 110 permit ip any any				
!				
int fa0/0				
ip access-group 110 in				

Ex7) Extended ACL

- ① 출발지 '13.13.10.0/24' 서브넷이 FTP 서버 '172.16.1.1'로 접근하는 것을 허용한다.
- ② 단, 출발지 '13.13.10.1' 호스트가 FTP 서버 '172.16.1.1'로 접근하는 것을 차단한다.
- ③ 외부 사용자가 인터넷을 통하여 '172.16.1.1' 서버로 Telnet 접속하는 것을 차단한다.
- ④ 나머지 패킷들은 접근이 가능하도록 허용한다.

```
access-list 110 deny tcp host 13.13.10.1 host 172.16.1.1 range 20 21
access-list 110 permit tcp 13.13.10.0 0.0.0.255 host 172.16.1.1 range 20 21 // 마지막에 전체 허용이 있기
access-list 110 deny tcp any host 172.16.1.1 eq 23 // 때문에 설정할 필요 없음
access-list 110 permit ip any any
!
int fa0/1
ip access-group 110 out
```

- 범위 작은 2번부터 설정

Ex8) Extended ACL

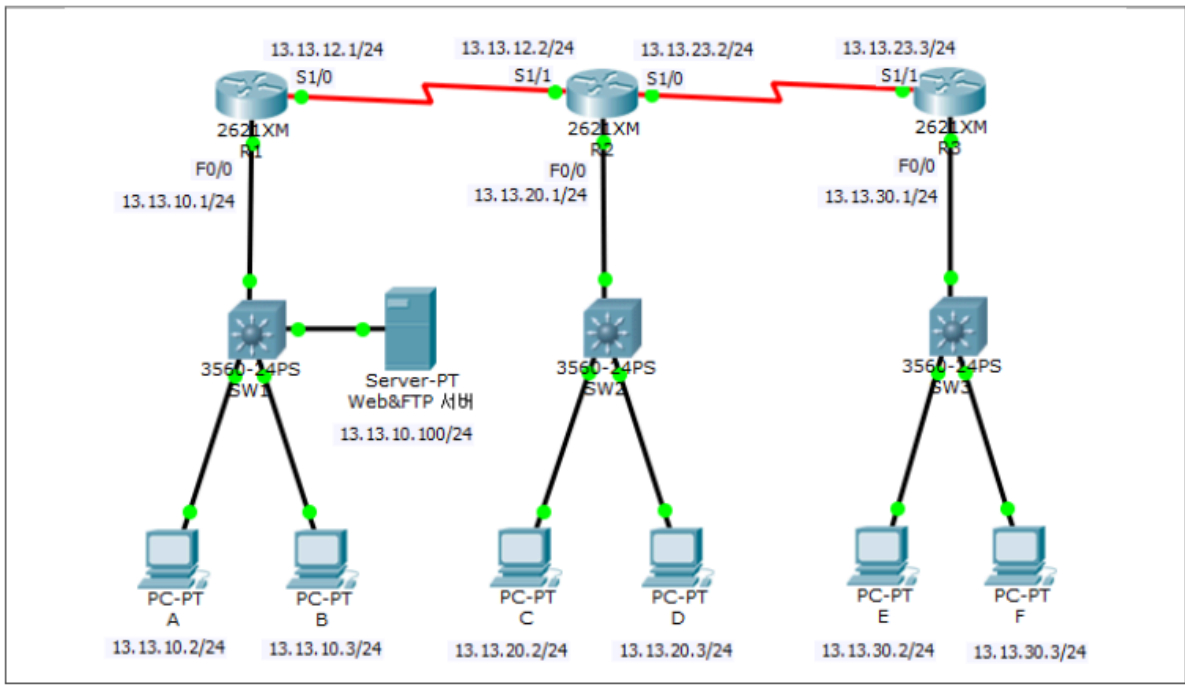
- ① 출발지 '13.13.10.1' 호스트가 웹-서버 '172.16.1.1'로 접근하는 것을 차단한다.
- ② 출발지 '13.13.10.0/24' 서브넷이 웹-서버 '172.16.1.1'로 접근하는 것은 허용한다.
- ③ 외부 사용자가 인터넷을 통하여 '172.16.1.1' 서버로 전송하는 ICMP 패킷을 차단한다.
- ④ 단, '172.16.1.1' 서버는 외부로 Ping 이 되어야 한다.
- ⑤ 나머지 패킷들은 접근이 가능하도록 허용한다.

```
access-list 110 deny tcp host 13.13.10.1 host 172.16.1.1 eq 80
access-list 110 permit tcp 13.13.10.0 0.0.0.255 host 172.16.1.1 eq 80 // 마지막에 전체 허용이 있기
access-list 110 deny icmp any host 172.16.1.1 echo // 때문에 설정할 필요 없음
access-list 110 permit ip any any
!
int fa0/1
ip access-group 110 out
```

- 범위 작은 1번부터 설정

Ex9) Extended ACL 예제

- 출발지 '13.13.30.0/24'인 패킷이 내부 로컬 네트워크 '13.13.10.1'로 Telnet 접속되는 것을 차단한다.
- 외부에서 내부 서버 '13.13.10.100'으로 Ping 되는 것을 차단하여라. 단, 서버는 외부로 Ping 이 되어야 한다.
- 출발지 '13.13.20.0/24'인 패킷이 내부 웹서버 '13.13.10.100'으로 접근하는 것을 차단하여라.
- 나머지 패킷은 허용한다.
- R1 에서 ACL 을 최대한 간결하게 구성하며, R1 Serial 1/0 인터페이스에 적용하여라.



@ R1

conf t

access-list 110 deny tcp 13.13.30.0 0.0.0.255 host 13.13.10.1 eq 23

access-list 110 deny icmp any host 13.13.10.100 echo

access-list 119 deny tcp 13.13.20.0 0.0.0.255 host 13.13.10.100 eq 80

access-list 110 permit ip any any

!

int s1/0

ip access-group 110 in

end

!

[확인 작업]

차단 F -> Desktop -> Command Prompt -> telnet 13.13.10.1

차단 D, F -> Desktop -> Command Prompt -> ping 13.13.10.100

허용 내부 서버 -> Desktop -> Command Prompt -> ping 13.13.20.3, ping 13.13.30.3

차단 D -> Desktop -> Web Browser -> http://13.13.10.100