ACL

(Access Control List)

■ 엑세스 리스트(Access List, ACL)

- 엑세스 리스트 제어방법에 따른 분류

Standard Access List	출입 통제 시 출발지 주소만을 참고
Extended Access List	출발지, 목적지, 프로토콜, 사용 포트 번호 참고

- 엑세스 리스트 숫자 와 이름에 따른 분류

Standard Access List	1-99, 1300~1999
Extended Access List	100-199, 2000~2699
Named Access List	이름 사용

- access-list 문 정의

. access-list 는 Interface별, Direction(in,out)별, Protocol별로 각각 하나씩 적용 가능

. 액세스 리스트는 명시한 순서대로 윗줄부터 순차적으로 수행한다

. 액세스 리스트는 암묵적으로 deny any 이 마지막으로 적용된다.

. 따라서 해당하지 않는 주소를 허용하려면 permit any를 명시해주어야 한다.

- access-list 문 갱신

. 엑세스리스트는 추가 될 경우 맨 마지막 라인에 추가 된다.

. 숫자 형태의 액세스리스트는 삭제한 액세스리스트 다음 모든 것이 삭제되나,
named 액세스리스트는 부분추가 삭제가 가능다.

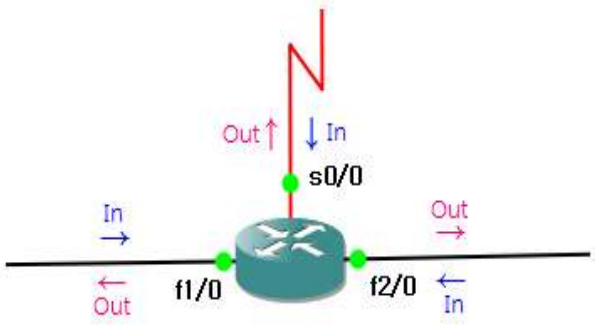
. Wildcard Mask 는 생략이 가능하지만,
생략이 가능한 경우는 0.0.0.0 인 경우다. (host 특정주소)

- access-list 문 interface 에 적용

. 인터페이스에 대한 엑세스 리스트의 정의가 되어 있지 않은 경우 결과는 permit any가 된다.

. Interface 의 기본값은 out 이다.

▶ 라우터 IN 과 OUT의 구분



※ Subnet Mask 와 Wildcard Mask 비고

. SubNet Mask -> 0 : 호스트 자리
-> 1 : 네트워크 자리

. Wildcard Mask -> 0 : 무엇이 오든 검사해라
-> 1 : 무엇이 오든 무시해라

<연습> 192.168.2.1 0.0.0.255
<연습> 192.168.2.2 0.0.0.255
<연습> 192.168.2.0 0.0.0.255

<연습> 192.168.10.4 0.0.0.3

▶ Standard Access-list

- 스텐더드 액세스 리스트 명령 형식

Router(config)#access-list access-list-number {permit | deny} {source-wildcard | any}

엑세스 리스트 번호 (0~99)또는(1300~1999) 허용 또는 거부 와일드카드 마스크 또는 모든주소

Router(config-if)#ip access-group access-list-number {in | out}

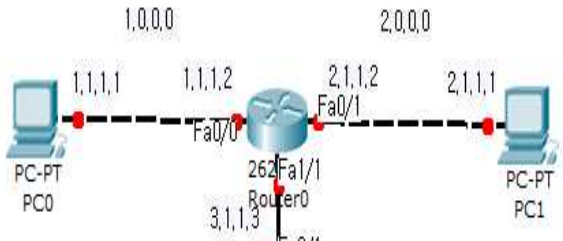
엑세스 리스트 번호 in 또는 out (디폴트값 out)

<주의>

access-list 1 deny 0.0.0.0 255.255.255.255
access-list 1 deny any

access-list 1 deny 1.1.1.1 0.0.0.0
access-list 1 deny host 1.1.1.1

[실습]




```
access-list 1 deny 3.1.1.1 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group 1 out
-----------------------------------
ip access-list standard cisco
deny 3.1.1.1 0.0.0.0
permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group cisco out
```

```
access-list 2 deny 3.1.1.2 0.0.0.0
access-list 2 permit 0.0.0.0 255.255.255.255

int f0/1
ip access-group 2 out
-----------------------------------
ip access-list standard itwill
deny 3.1.1.2 0.0.0.0
permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group itwill out
```

```
# show   access-list
# show  ip   access-lists
# show  ip  interface  [interface]   인터페이스에 액세스리스트 설정 확인
```

※ telnet 접근 제한

```
line  vty  0  4
 login
 password  cisco
 access-class   1   in   <---3.1.1.1 만  접속 불가
```

▶ Extended Access-list

- 스탠더드 액세스 리스트는 출발지 주소(Source Address)만으로 제어하는 반면, 익스텐디스 액세스리 리스트는 출발지 주소, 목적지 주소(Destination Address)까지 제어할 수 있다.

- 스탠더드 액세스 리스트는 전체 TCP/IP에 대한 제어만을 하는 반면, 익스텐디드 엑세스 리스트는 TCP, IP, udp, icmp, ftp 등 특정 프토토콜까지 지정하여 제어할 수 있다.

- 스탠더드 액세스 리스트는 (1~99), (1300~1999) 사용하고, 익스텐디드 액세스 리스트는 (100~199), (2000~2699) 사용한다.

- Well Known Port

20 (TCP)	File Transfer Protocol 데이타
21 (TCP)	FTP Control Data
23 (TCP)	Telnet
25 (TCP)	SMTP (Simple Mail Transport Protocol)
53 (TCP, UDP)	Domain Name System (DNS)
69 (UDP)	Trivial File Transfer Protocol(TFTP)
80 (TCP)	HyperText Transfer Protocol (HTTP)

- 익스텐디드 액세스 리스트 명령 형식

Router(config)#access-list access-list-number {permit | deny}
액세스 리스트 번호 허용 또는 거부
(100~199)또는(2000~2699)

protocol source source-wildcard [operator port]
프로토콜 출발지 출발지 와일드카드마스크
지정 주소

destination destication-wildcard [operator port] [established] [log]
도착지 주소 도착지 와일드 카드마스크

Router(config-if)#ip access-group access-list-number { in | out }
액세스 리스트 번호 in 또는 out

※ 암묵적으로 존재 :

access-list 100 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 100 deny ip(tcp|udp|icmp) any any

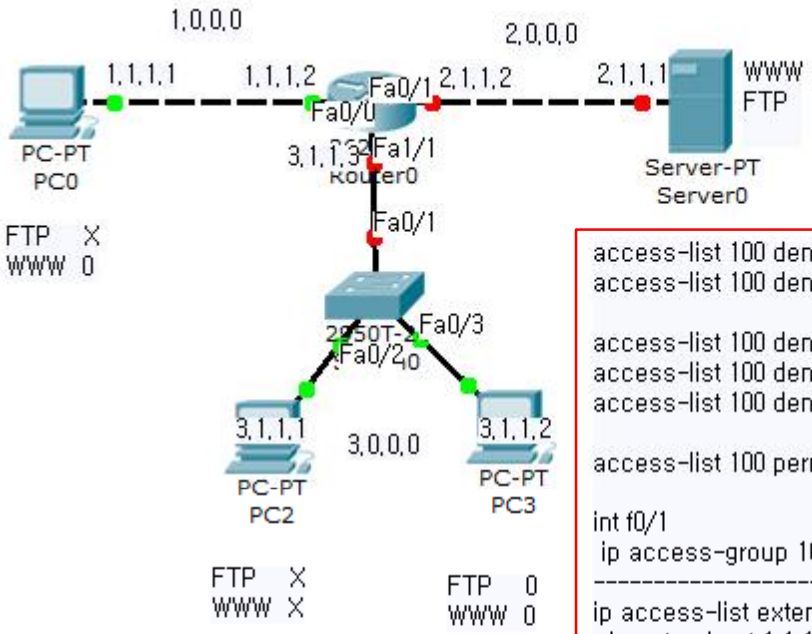
- protocol

IP 패킷에 실려서 전송될수 있는 상위계층 프로토콜을 필터링하며, ICMP, TCP, UDP 등을 지정한다.

- operator

gt (greater than)	~ 보다 크다.
lt (less than)	~ 보다 작다.
eq (equal)	~ 와 같다.
neq (not equal)	~ 와 같지 않다.

[실습]




```
access-list 100 deny tcp host 1.1.1.1 host 2.1.1.1 eq 21
access-list 100 deny tcp host 1.1.1.1 host 2.1.1.1 eq 20

access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 21
access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 20
access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 80

access-list 100 permit ip any any

int f0/1
 ip access-group 100 out
-----------------------------------------------
ip access-list extended cisco
 deny tcp host 1.1.1.1 host 2.1.1.1 eq 21
 deny tcp host 1.1.1.1 host 2.1.1.1 eq 20

 deny tcp host 3.1.1.1 host 2.1.1.1 eq 21
 deny tcp host 3.1.1.1 host 2.1.1.1 eq 20
 deny tcp host 3.1.1.1 host 2.1.1.1 eq 80

 permit ip any any

int f0/1
 ip access-group cisco out
```

access-list 100 deny icmp any host 2.1.1.1 echo