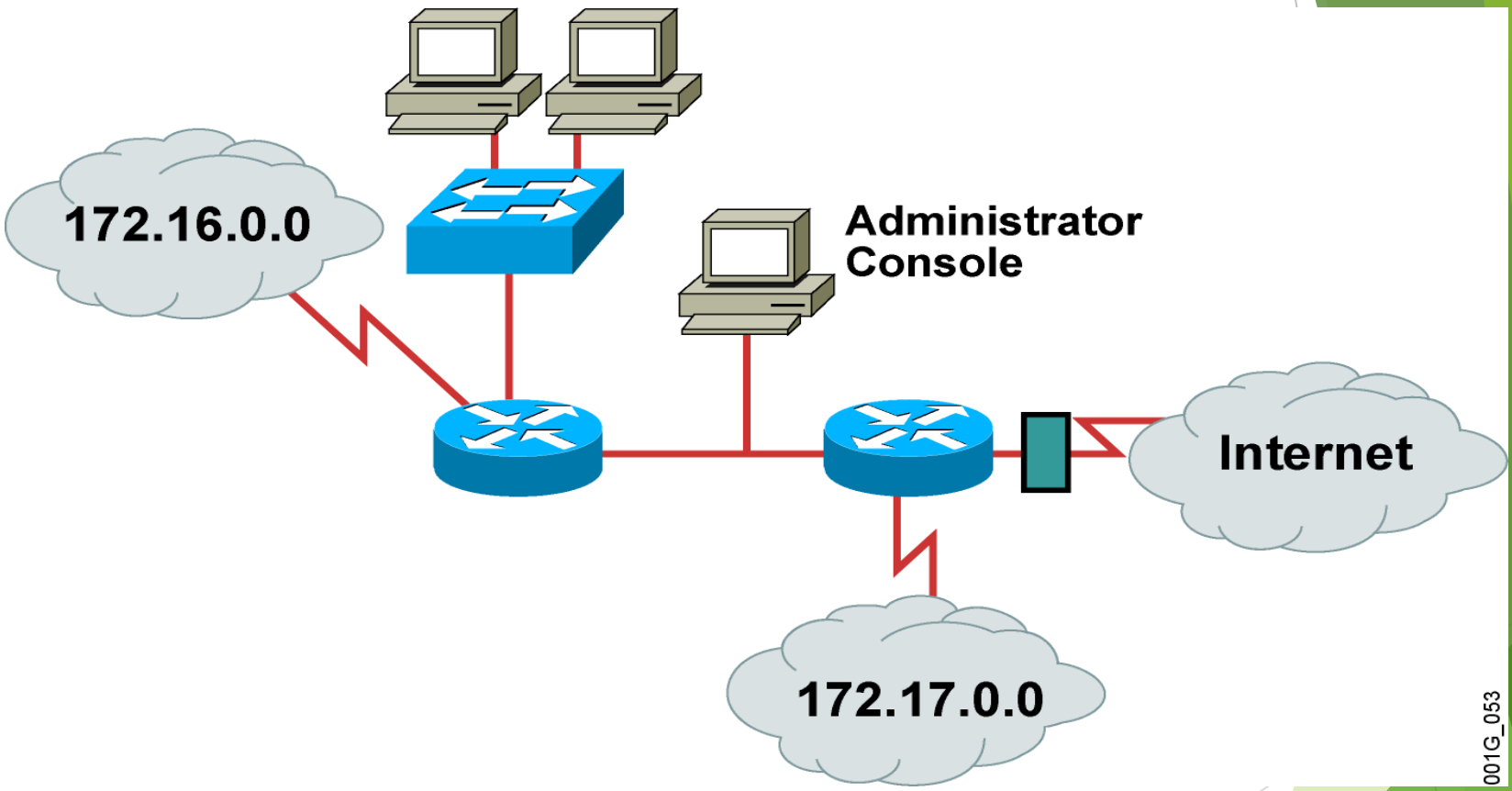
Traffic control과 NAT

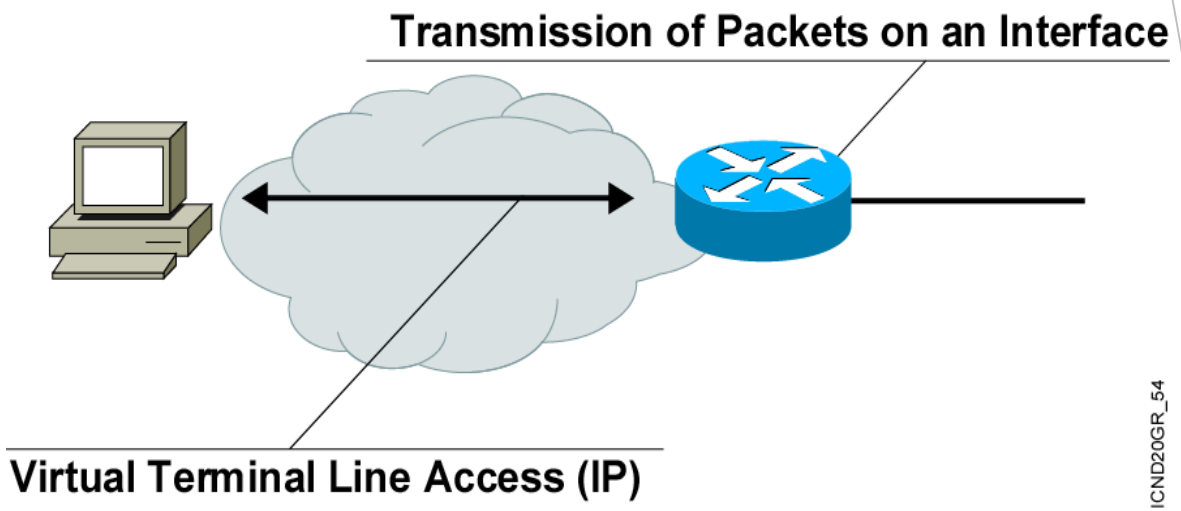
1.ACLs(Access Control Lists)

ACLs(Access Control Lists)란



라우터를 통과하는 Packet중 불필요하거나 나쁜 의도를 가진 Packet은 접근을 제어하기 위해 사용하는 도구

Access Lists 특징



✓ACL 문장 기반 : Top-down 처리, First-Match, 암묵적 deny
✓전송 패킷 필터

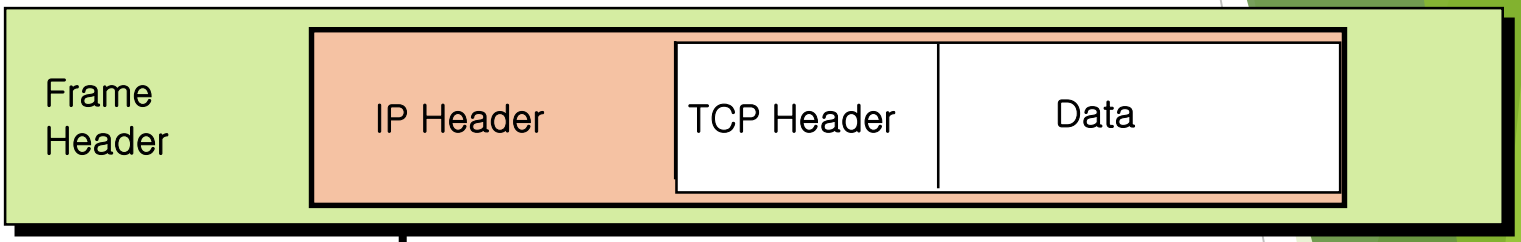
ACL의 기본 동작

- ✓**ACL에 의해 제어 되는 패킷**
  - ✓라우터를 통과하는 패킷
  - ✓라우터를 목적지로 하는 패킷
- ✓**ACL의 기본 동작**
  - ✓Top-down 처리
  - ✓First-Match
  - ✓암묵적 deny
  - ✓Protocol별, 방향별, interfac별 하나의 ACL 적용
- ✓**ACL 사용되는 곳**
  - ✓패킷 필터링
  - ✓NAT
  - ✓QoS, 경로 조정등

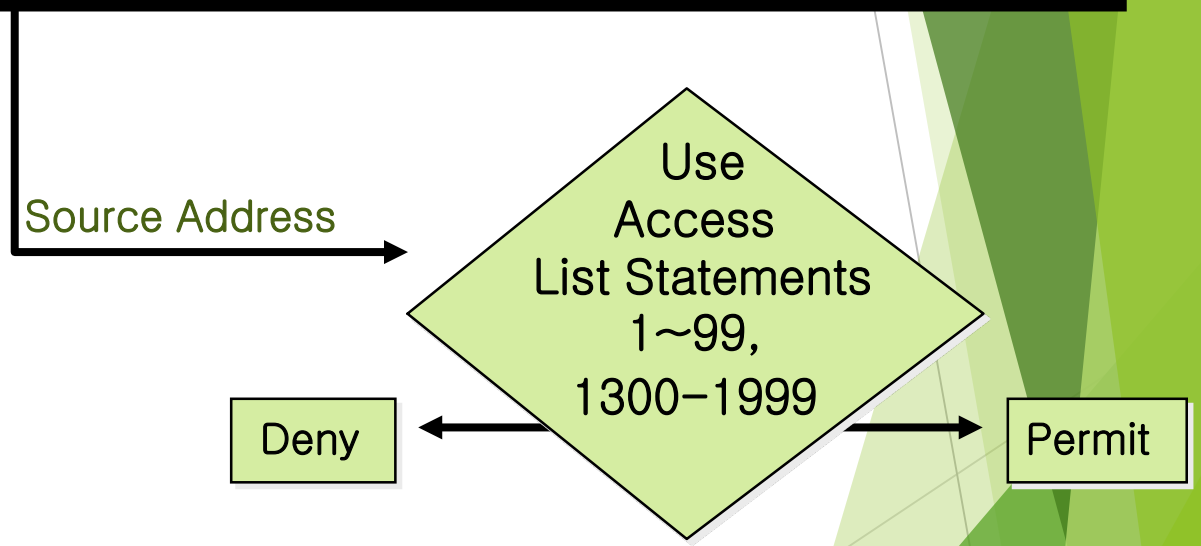
Access Lists 종류

- ✓조건식에 따라
  - ✓Standard ACL
  - ✓Extended ACL
- ✓**ACL**을 구분하는 방식에 따라
  - ✓Numbered ACL
  - ✓Named ACL
- ✓적용 방향에 따라
  - ✓Inbound ACL
  - ✓Outbound ACL

Standard Access List 특징



- ✓조건식
  - ✓Source 주소만 확인
- ✓**ACL의 숫자 범위**
  - ✓1-99
  - ✓1300-1999
- ✓적용 위치
  - ✓목적지에 가까운 곳
  - ✓Outbound Interface
- ✓**Protocol**
  - ✓IPv4



Standard Access List 설정

✓설정단계
- ✓ACL 생성
- ✓ACL 적용

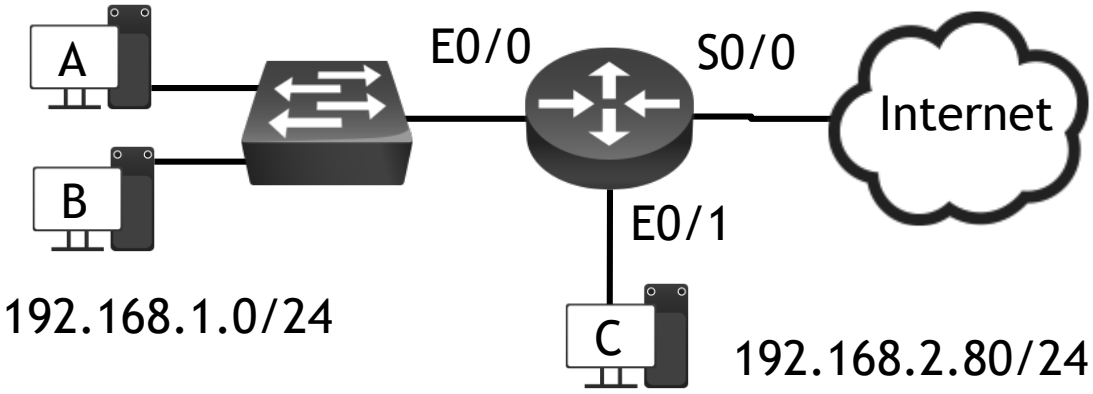
✓**ACL** 생성

Router(config)#access-list # permit/deny condition

✓**ACL** 적용

Router(config-if)#protocol access-group # in/out

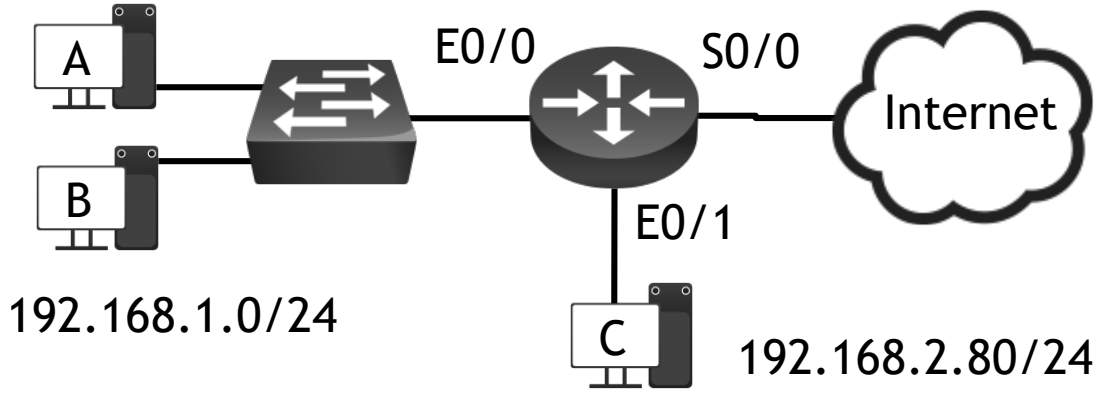
Standard Access List 설정 예1



✓**192.168.1.0/24** 과 **192.168.2.0/24**은 서로 접근 허용
✓**Internet** 망에서 내부망에 접근 불허
✓**Standard ACL**을 적용

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)#int e0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#int e0/1
Router(config-if)#ip access-group 1 out
```

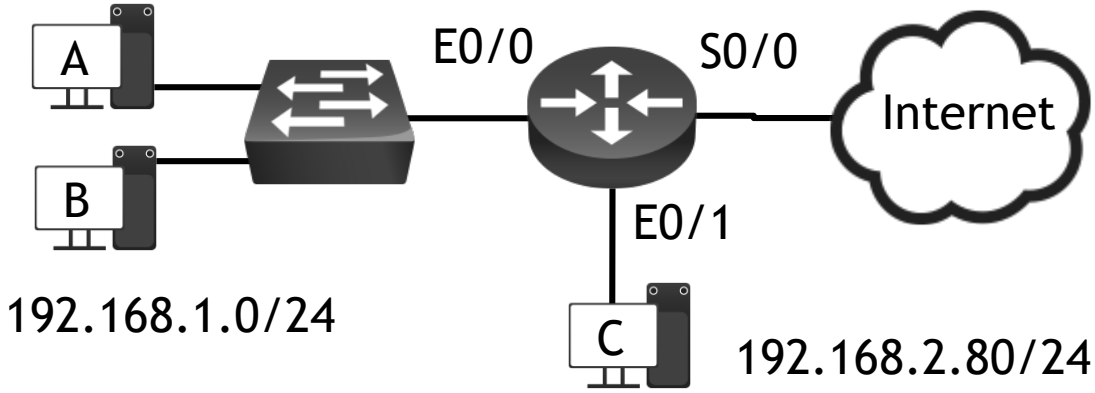
Standard Access List 설정 예2



✓**192.168.2.80/24**에서 **192.168.1.0/24**에 접근 불허
✓나머지 다 허용
✓**Standard ACL**을 적용

```
Router(config)#access-list 1 deny 192.168.2.80 0.0.0.0
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
Router(config)#int e0/0
Router(config-if)#ip access-group 1 out
```

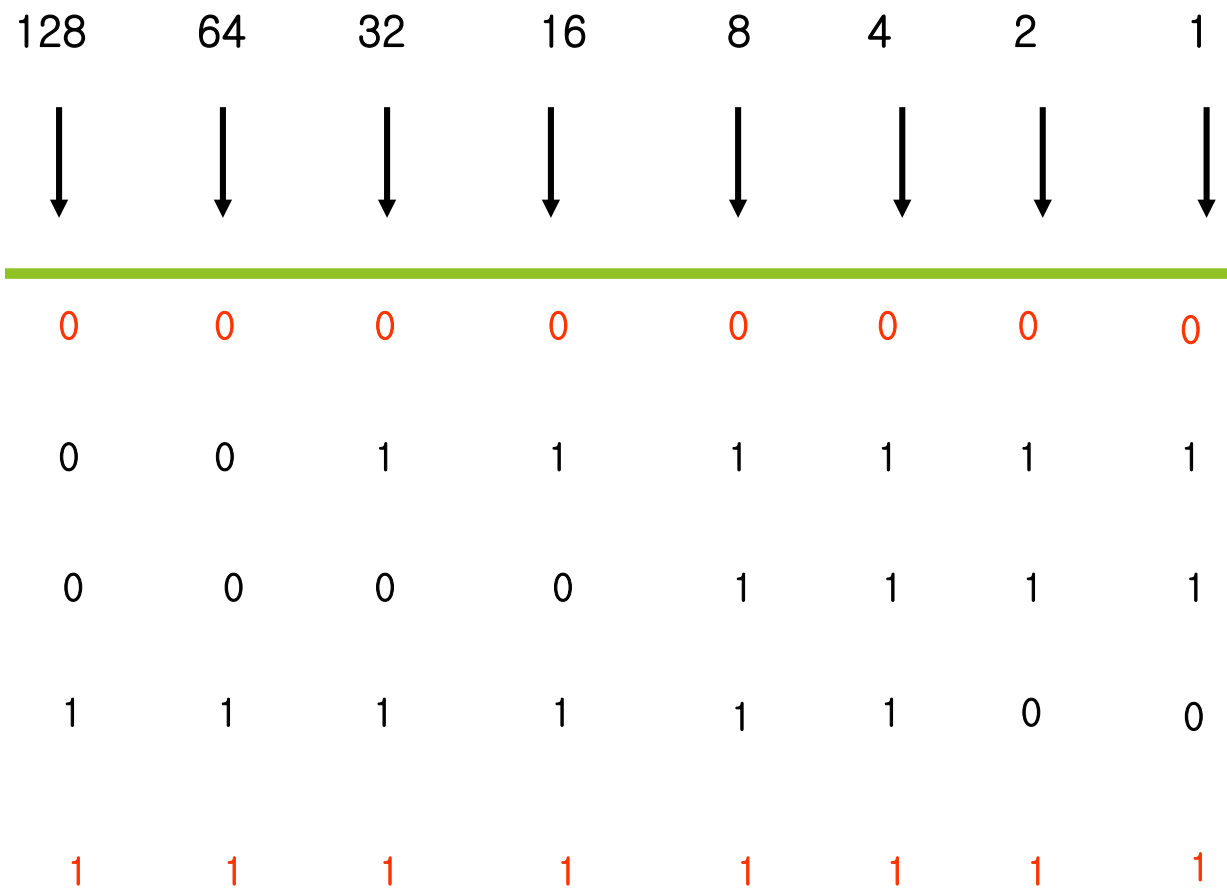
Standard Access List 설정 예3



✓**192.168.1.0/24** 에서 **192.168.2.0/24**에 접근 불허
✓나머지 다 허용
✓**Standard ACL**을 적용

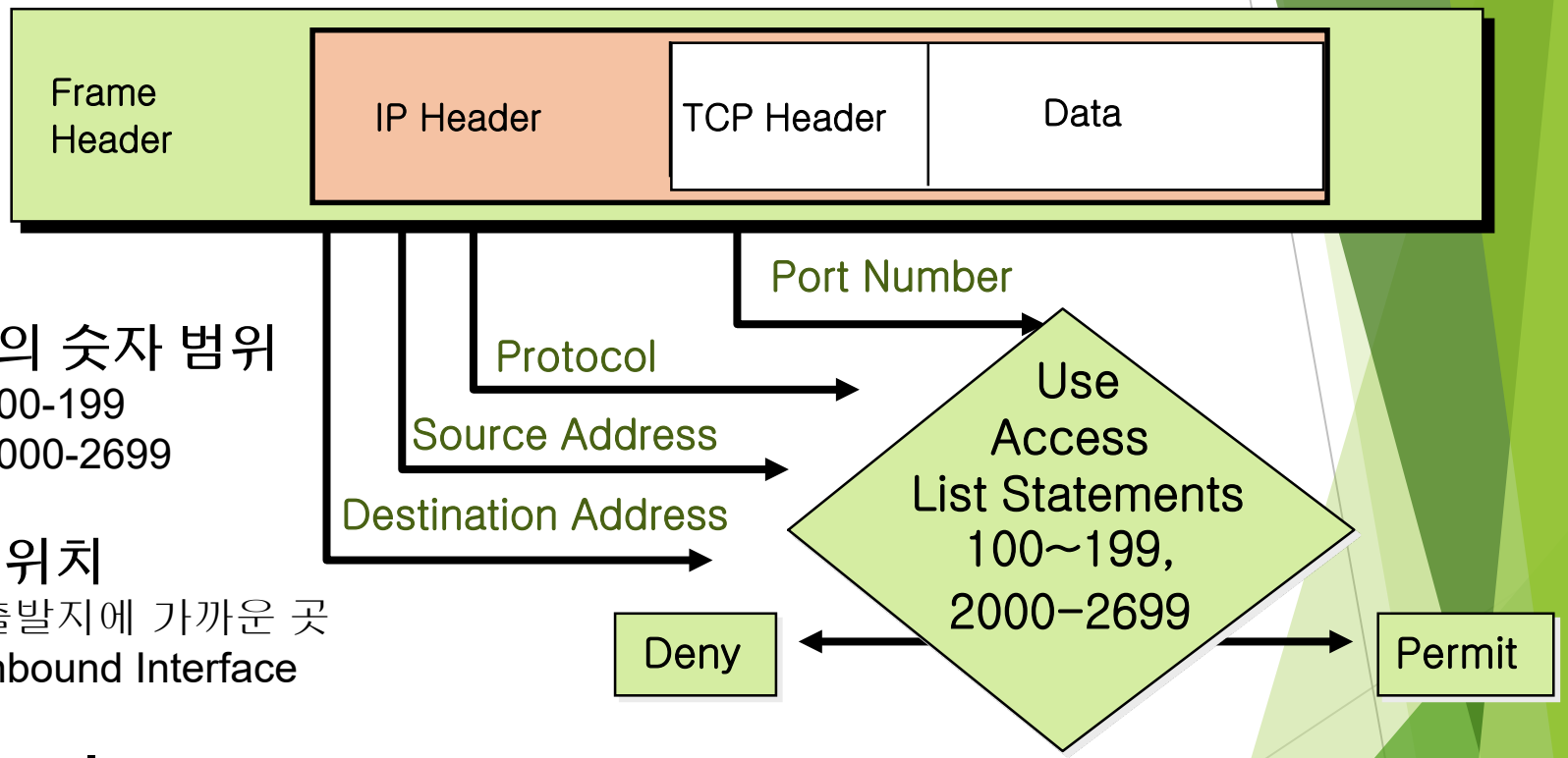
```
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#int e0/1
Router(config-if)#ip access-group 1 out
```

Wildcard Bits(주소 매핑 방법)



- ✓**Wildcard Mask Bit=0**
  - ✓IP 주소 Bit와 반드시 일치
- ✓**Wildcard Mask Bit=1**
  - ✓Don’t Care

Extended Access List 특징



- ✓**ACL의 숫자 범위**
  - ✓100-199
  - ✓2000-2699
- ✓적용 위치
  - ✓출발지에 가까운 곳
  - ✓Inbound Interface
- ✓**Protocol**
  - ✓IPv4, IPv6
- ✓조건식
  - ✓Source/Destination 주소, protocol, port 확인

Extended Access List 설정

✓설정단계
- ✓ACL 생성
- ✓ACL 적용

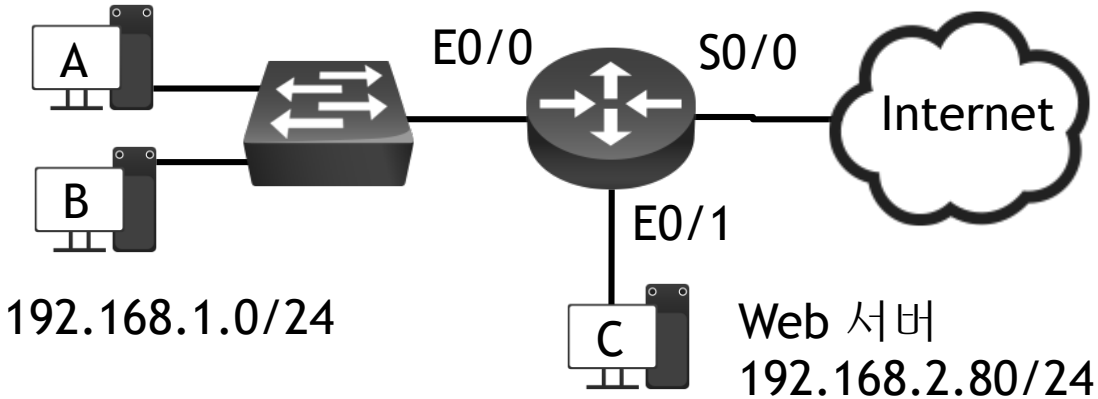
✓**ACL** 생성

Router(config)#access-list # permit/deny protocol source source-wc eq port# destination destination-wc eq port# [established/log]

✓**ACL** 적용

Router(config-if)#protocol access-group # in/out

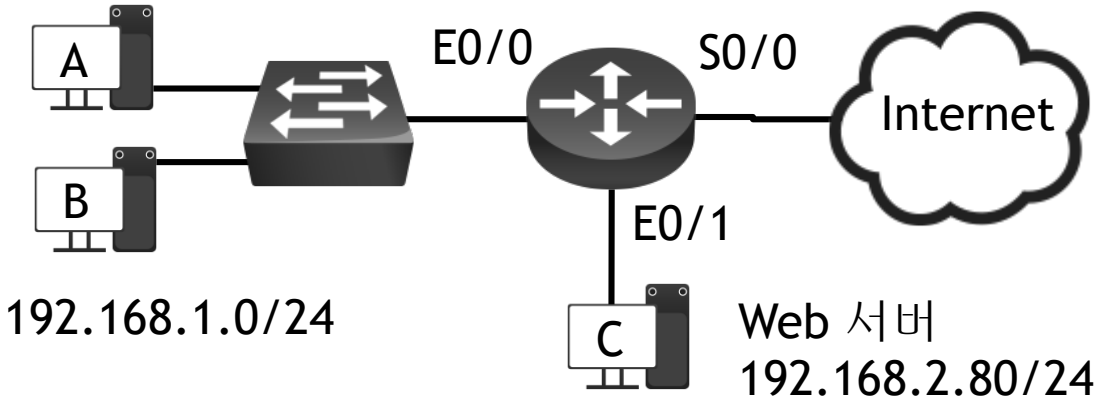
Extended Access List 설정 예1



✓**192.168.1.0/24**에서 **192.168.2.80/24**의 **web** 서비스에만 접근 허용**(e0/1**에서 **outbound**로 적용**)**
✓**Extended ACL**을 적용

```
Router(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.80
0.0.0.0 eq 80
Router(config)#int e0/1
Router(config-if)#ip access-group 101 out
```

Extended Access List 설정 예2



✓**192.168.2.0/24**에서 **192.168.1.0/24**에 **telnet** 접근 불허
✓나머지 다 허용
✓**Extended ACL**을 적용

```
Router(config)#access-list 101 deny tcp 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255 eq telnet
Router(config)#access-list 101 permit ip any any
Router(config)#int e0/1
Router(config-if)#ip access-group 101 in
```

Named ACL

✓특징
- ✓Std.와 Ext. ACL 모두에 적용
- ✓좀 더 유연하고 직관적인 ACL 설정
- ✓시퀀스 번호를 이용하여 리스트의 각 문장 추가, 삭제, 수정 가능 (IOS 12.3부터는 numbered ACL도 적용)

✓설정단계
- ✓Named ACL 생성
- ✓조건문 설정
- ✓ACL 적용

✓**Named ACL** 생성

Router(config)#ip access-list standard/extened name

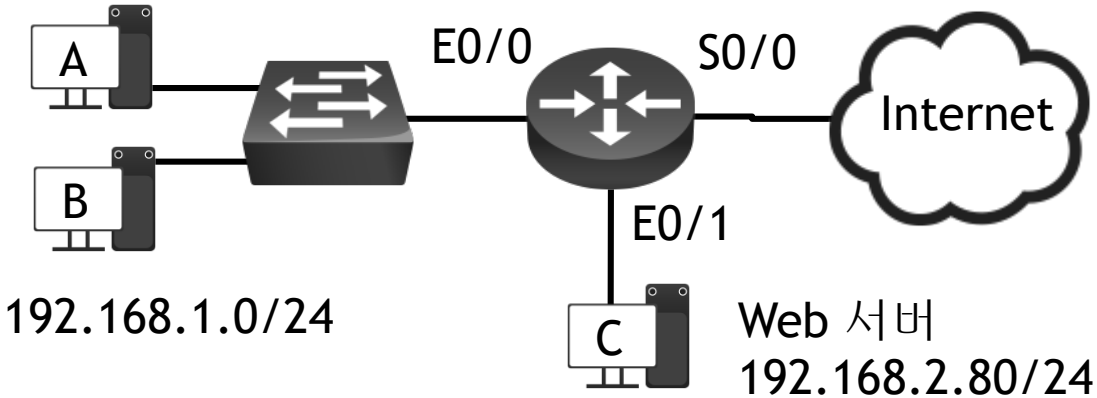
✓조건문 설정

Router(config std/ext-nacl)#[sequence#] permit/deny condition

✓**ACL** 적용

Router(config-if)#ip access-group name in/out

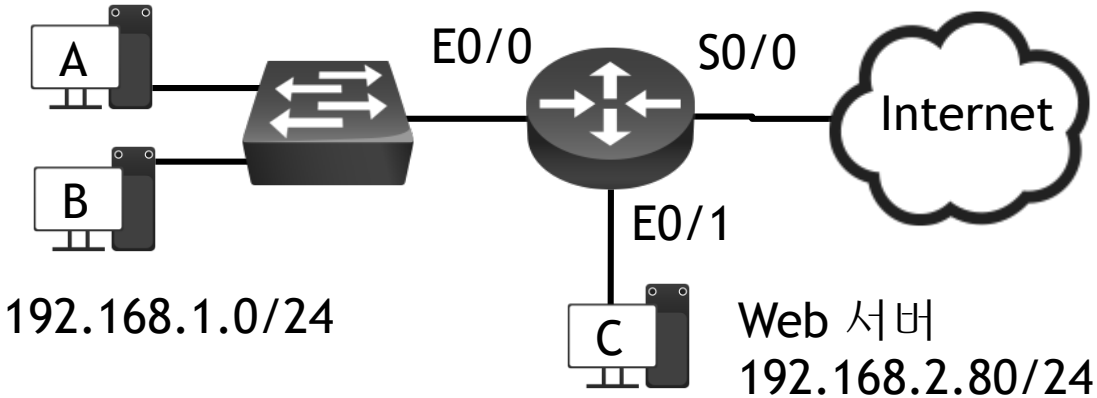
Named ACL 설정예1



✓**192.168.2.80/24**에서 **192.168.1.0/24**에 접근 불허
✓나머지 다 허용
✓**Standard Named ACL**을 적용

```
Router(config)#ip access-list standard noAccessHost
Router(config std-nacl)#remark deny 192.168.2.80 to 192.168.1.0/24
Router(config std-nacl)#deny 192.168.2.80 0.0.0.0
Router(config std-nacl)#permit 0.0.0.0 255.255.255.255
Router(config)#int e0/0
Router(config-if)#ip access-group noAccessHost out
```

Named ACL 설정예2



✓**192.168.2.0/24**에서 **192.168.1.0/24**에 **telnet** 접근 불허
✓나머지 다 허용
✓**Extended Named ACL**을 적용

```
Router(config)#ip access-list extended noTelnet
Router(config ext-nacl)#deny tcp 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255 eq telnet
Router(config ext-nacl)#permit ip any any
Router(config)#int e0/1
Router(config-if)#ip access-group noTelnet in
```

VTY ACL

✓특징
- ✓Std ACL 사용
- ✓Router로 Telnet 접근하거나 다른 장비로 telnet 접근하는 것 제어

✓설정단계
- ✓ACL 생성
- ✓ACL 적용

✓**ACL** 생성

Router(config)#access-list #(standard ACL#) permit/deny condition

✓**ACL** 적용

Router(config)#line vty 0 4
Router(config-line)#access-class # in/out

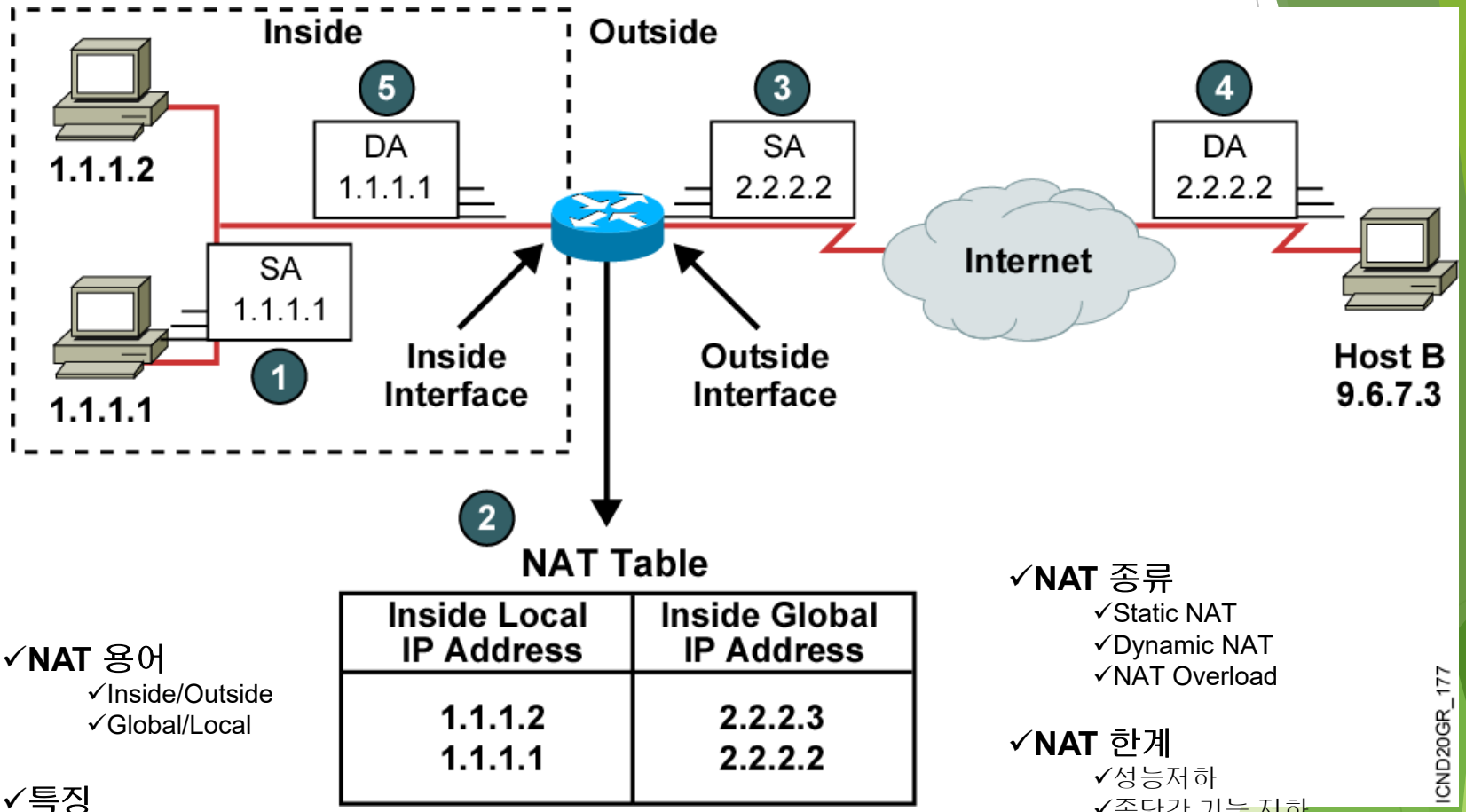
ACL 확인

```
Router#show access-lists
Standard IP access list 1
    permit 192.168.1.10
    permit 192.168.1.20
    permit 192.168.1.30
    permit 192.168.1.40
Extended IP access list 101
    permit tcp host 192.168.1.10 any eq telnet
    permit tcp host 192.168.1.20 any eq ftp
    permit tcp host 192.168.1.30 any eq ftp-data
```

```
Router#show ip int e0/0
Ethernet0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  <text ommitted>
```

2.NAT

NAT



✓**NAT 용어**
- ✓Inside/Outside
- ✓Global/Local

✓**특징**
- ✓RFC 3022
- ✓사설 IP 주소(RFC1918) 이용하여 공인 IP 주소 절약
- ✓내부 IP 주소를 외부에 숨김
- ✓ISP 변경 가능

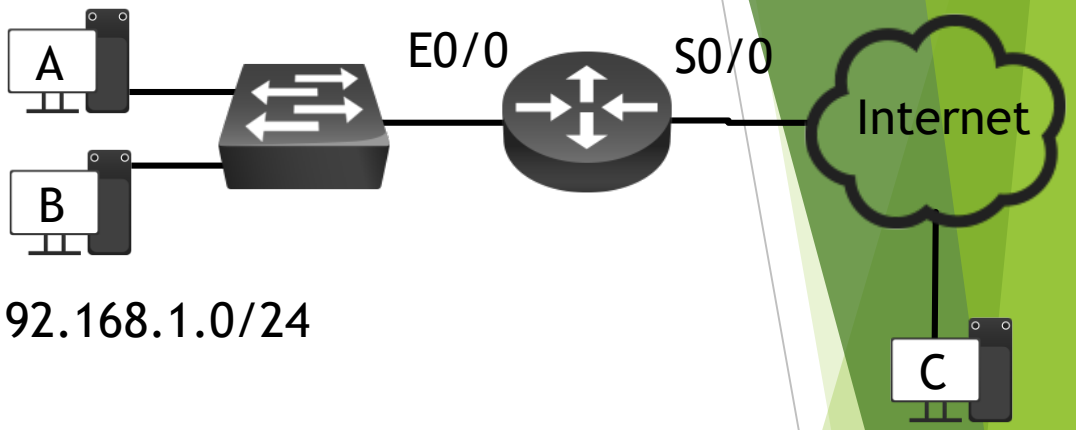
✓**NAT 종류**
- ✓Static NAT
- ✓Dynamic NAT
- ✓NAT Overload

✓**NAT 한계**
- ✓성능저하
- ✓종단간 기능 저하
- ✓종단간 IP 추적 안됨
- ✓복잡한 터널링
- ✓서비스 중단

Static NAT 설정

✓특징
- ✓1:1 연결
- ✓외부 접근 가능
- ✓외부에 내부 서버 서비스 가능

✓설정단계
- ✓Static NAT 설정
- ✓Inside interface 지정
- ✓Outside interface 지정



✓**Static NAT 설정**

Router(config)#ip nat inside source static 192.168.1.80 203.239.185.80

✓**Inside interface 지정**

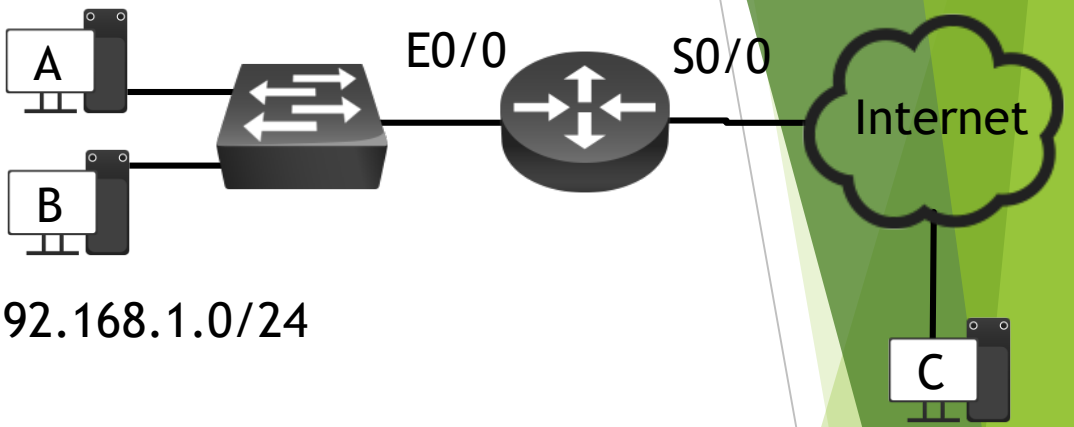
Router(config)#int e0/0
Router(config-if)#ip nat inside

✓**Outside interface 지정**

Router(config)#int s0/0
Router(config-if)#ip nat outside

Dynamic NAT 설정

✓특징
- ✓n:m 연결
- ✓외부 접근 불가능
- ✓내부 IP 주소를 외부에 숨김
- ✓주소 pool 사용



✓설정단계
- ✓NAT pool 구성: global address
- ✓Std. ACL 구성 : 변환될 주소
- ✓Dynamic NAT 설정
- ✓Inside interface 지정
- ✓Outside interface 지정

✓**NAT pool 구성**

Router(config)#ip nat pool Sample 203.239.185.1 203.239.185.50 netmask 255.255.255.0

✓**Std. ACL 구성**

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

✓**Dynamic NAT 설정**

Router(config)#ip nat inside source list 1 pool Sample

✓**Inside interface 지정**

Router(config)#int e0/0
Router(config-if)#ip nat inside

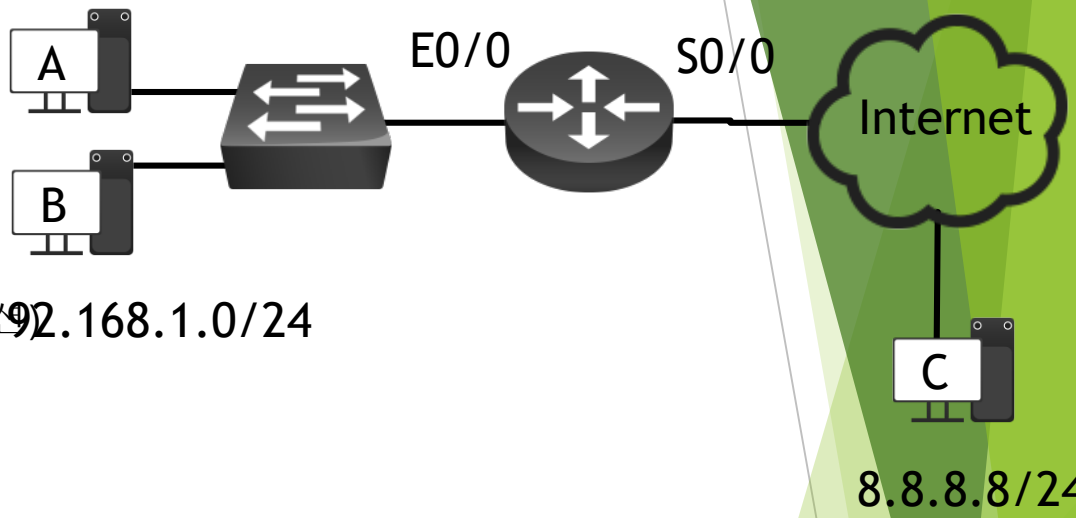
✓**Outside interface 지정**

Router(config)#int s0/0
Router(config-if)#ip nat outside

NAT Overload 설정

✓특징
- ✓m:1 연결
- ✓PAT
- ✓Dynamic NAT와 비슷

✓설정단계
- ✓NAT pool 구성: global address(옵션)
- ✓Std. ACL 구성 : 변환될 주소
- ✓Dynamic NAT 설정
- ✓Inside interface 지정
- ✓Outside interface 지정



✓**Std. ACL 구성**

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

✓**NAT Overload 설정**

Router(config)#ip nat inside source list 1 int s0/0 overload

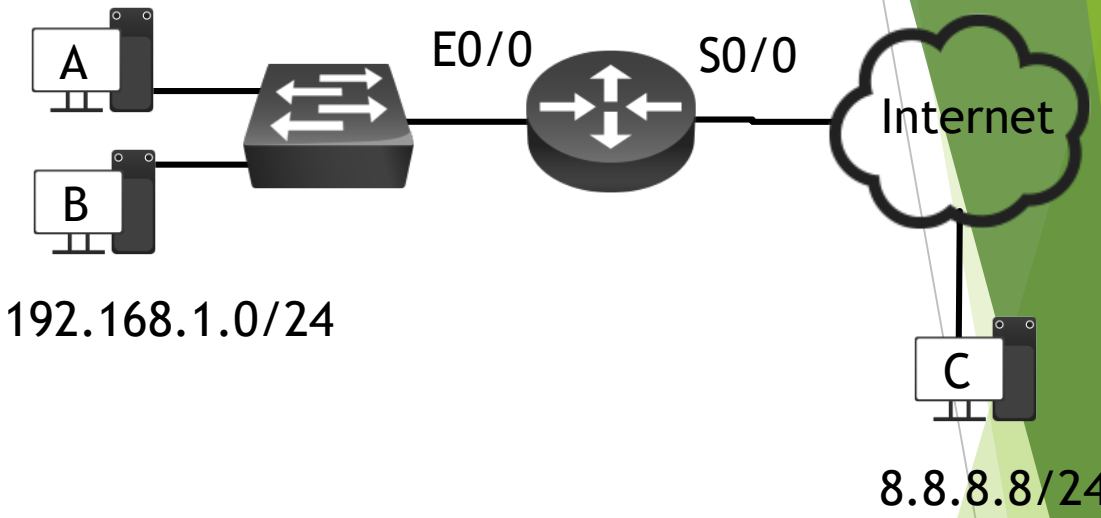
✓**Inside interface 지정**

Router(config)#int e0/0
Router(config-if)#ip nat inside

✓**Outside interface 지정**

Router(config)#int s0/0
Router(config-if)#ip nat outside

NAT 확인




```
Router# show ip nat translations
Pro Inside global         Inside local    Outside local Outside global
--- 203.239.185.1         192.168.1.1  ---         ---
tcp 203.239.185.10:47392 192.168.1.10:47392 8.8.8.8:80 8.8.8.8:80
tcp 203.239.185.10:50243 192.168.1.10:50243 8.8.8.8:80 8.8.8.8:80
```