제9장 NAT

(Network Address Translation)

1. NAT

NAT는 IP 주소 및 포트 번호를 변환하는 네트워크 서비스이며, 내부 사설 IP 주소를 사용하는 환경에서 데이터를 인터넷으로 전송할 때 출발지 사설 IP 주소를 공인 IP 주소로 변환한다. NAT를 구성하면 내부 네트워크는 다음과 같은 장점을 갖는다.

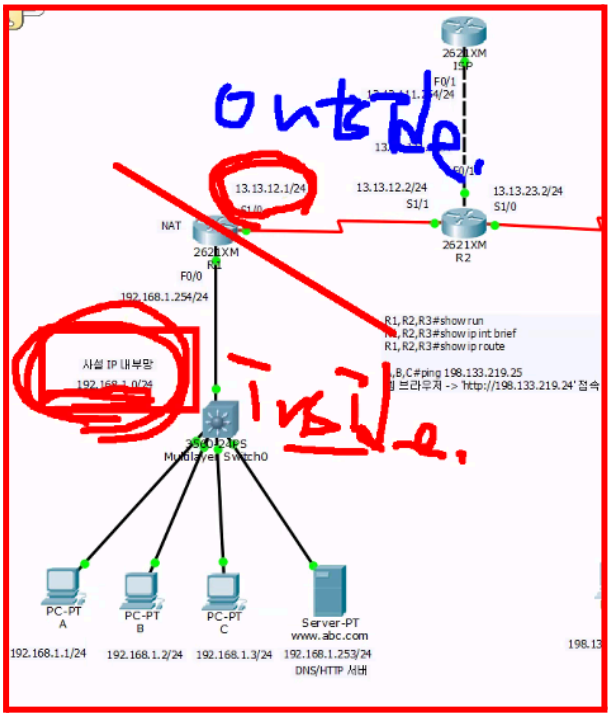
목적	내용
보안	사설 IP 주소를 사용하기 때문에 외부에서 접근 자체가 불가능하다.
IP 주소 고갈	사설 IP 주소를 사용해도 인터넷이 되기 때문에 공인 IP 주소를 사용할 필요가 없다.
데이터 전송	출발지 사설 IP 주소를 공인 IP 주소로 변환하기 때문에 응답 패킷이 다시 돌아 올 수 있다.

사설IP → 공인 IP 로 보낼때 문제는 없다 (목적지 IP만 잘 되어있으면 나간다)
하지만 다시 사설IP로 돌아올때 다른곳으로 보내진다.

- 따라서 NAT를 설정한다.
- 출발지 주소를 공인IP로 변경해서 내보낸다 (라우터로 유도한다.)

- 이렇게 사용하면 공인IP를 절약할 수 있다.
- 또한 보안 측면에서 사설 IP를 사용하면 더 안전하다 (외부에서 바로 접근이 불가하다)

2. NAT 구성 요소



- inside : inside local address (inside에서 쓰는 주소)
- outside : inside global address (outside에서 쓰는 주소)
- In → Out : 출발지 변경
- Out → In : 목적지 변경

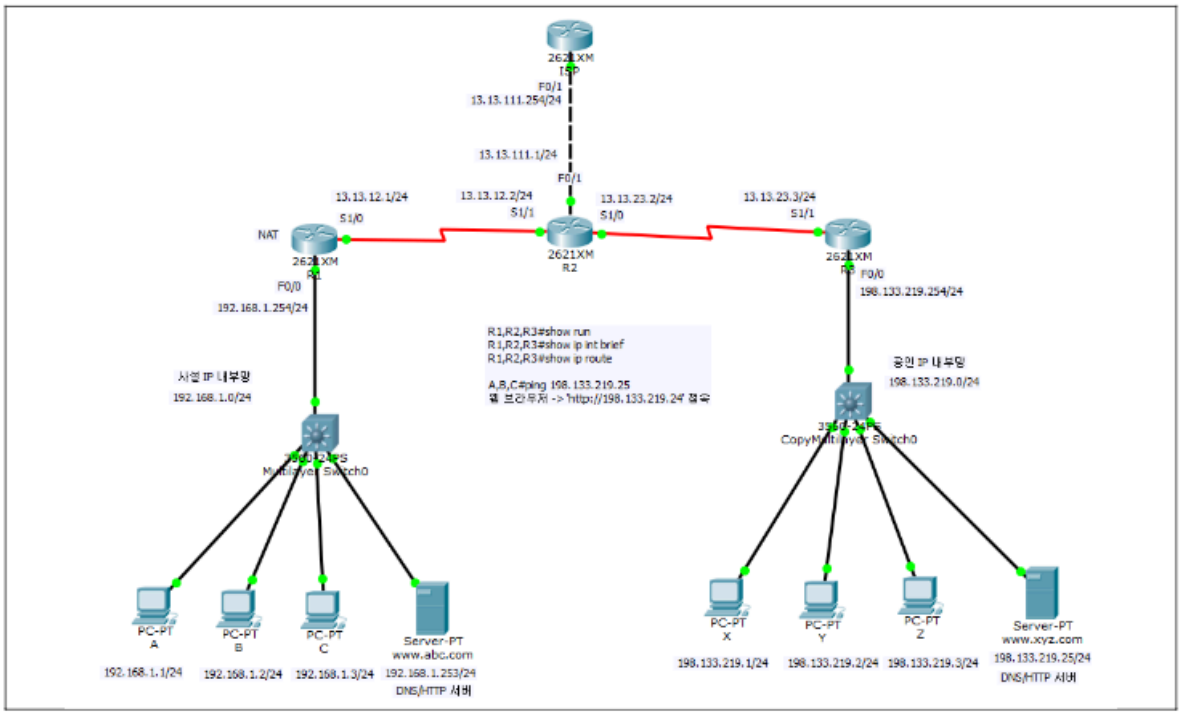
Cisco 라우터에서는 동적 NAT 와 정적 NAT 가 있다. 동적 NAT 는 내부 네트워크 시스템들이 인터넷을 하기 위해서 구성이 필요하며, 정적 NAT 는 외부 네트워크에서 내부 서버(Ex: 웹 서버)로 접근하기 위해서 구성이 필요하다. 리눅스에서 NAT 를 구현핬 경우, 동적 NAT 는 **'마스커레이드(Masquerade)'**라고 하며, 정적 NAT 는 **'포트 포워딩(Port Forwarding)'**이라고 한다.

Cisco 라우터에서 NAT 를 구성할 경우, 다음과 같은 NAT 구성 요소들을 파악해야 한다.

NAT 요소	내용
NAT Inside	- 출발지 주소를 변경할 시스템들이 있는 내부 네트워크 - Ex) 사설 IP 주소를 사용하는 내부망
NAT Outside	- 출발지 주소가 변환되어 패켓이 전송되는 외부 네트워크 - Ex) 공인 IP 주소를 사용하는 외부망
Inside Local 주소	- NAT Inside 에서 사용하는 로컬 네트워크 주소 - Ex) 사설 IP 주소
Inside Global 주소	- Nat Outside 로 패켓이 전송될때 변환되는 주소 - Ex) 공인 IP 주소
Inside -> Outside 패켓 전송	- 패켓의 출발지 주소를 변경한다.
Outside -> Inside 패켓 전송	- 패켓의 목적지 주소를 변경한다.

ex)

'17-1.NAT.pkt' 파일을 실행하여 R1 에서 NAT 를 구성한다.



- 콘솔 패스워드는 'ciscocon'이며, 관리자 패스워드는 'cisco'이다.
- A~C_PC 에서 '198.133.219.25'로 Ping 이 되는지 확인한다. (안되는게 정상이다.)
- A~C_PC 에서 브라우저를 실행하여 'http://198.133.219.25'로 접속되는지 확인한다. (안되는게 정상이다.)

Inside Local 192.168.1.0/24
Outside 13.13.12.1

@ R1
conf t
access-list 10 permit 192.168.1.0 0.0.0.255
!
ip nat inside source list 10 interface s1/0 overload
!
int fa0/0
 ip nat inside
!
int s1/0
 ip nat outside
 end
!

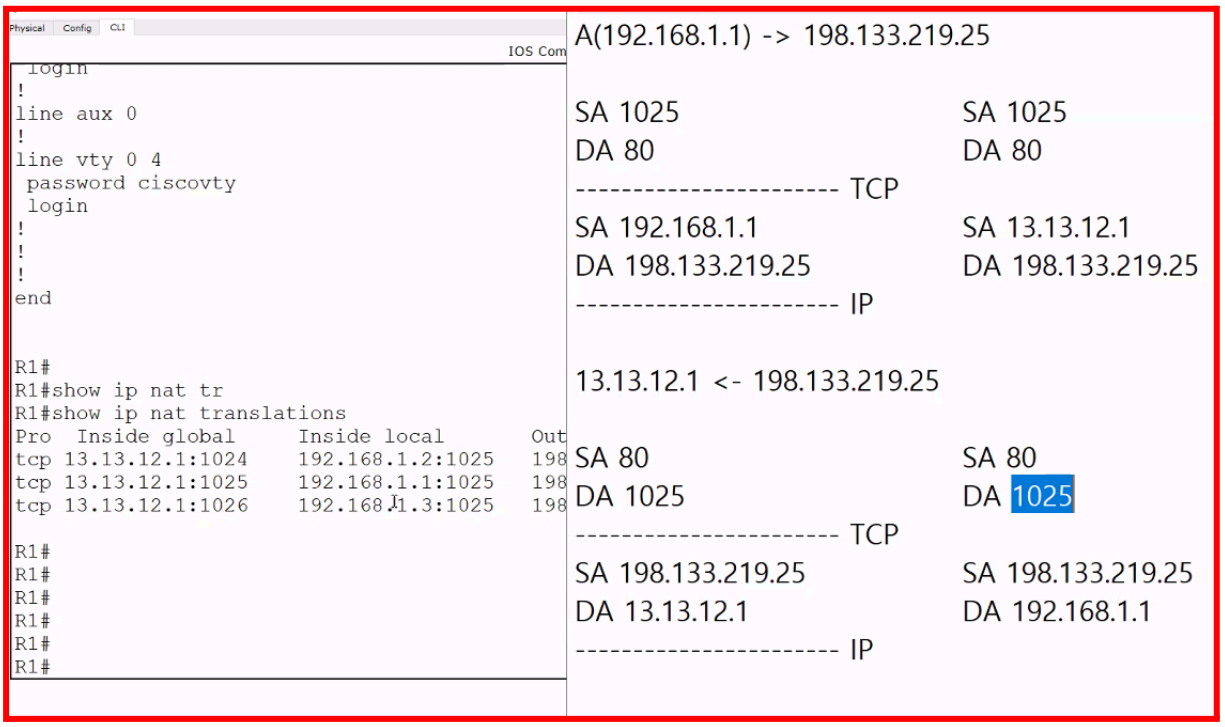
```
R1#show run
~ 중간 생략 ~
!
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 13.13.12.1 255.255.255.0
 ip nat outside
!
~ 중간 생략 ~


!
ip nat inside source list 10 interface Serial1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 13.13.12.2
!
```

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 13.13.12.1:1024    192.168.1.3:1025   198.133.219.25:80  198.133.219.25:80
tcp 13.13.12.1:1025    192.168.1.2:1025   198.133.219.25:80  198.133.219.25:80
tcp 13.13.12.1:1026    192.168.1.1:1026   198.133.219.25:80  198.133.219.25:80
```

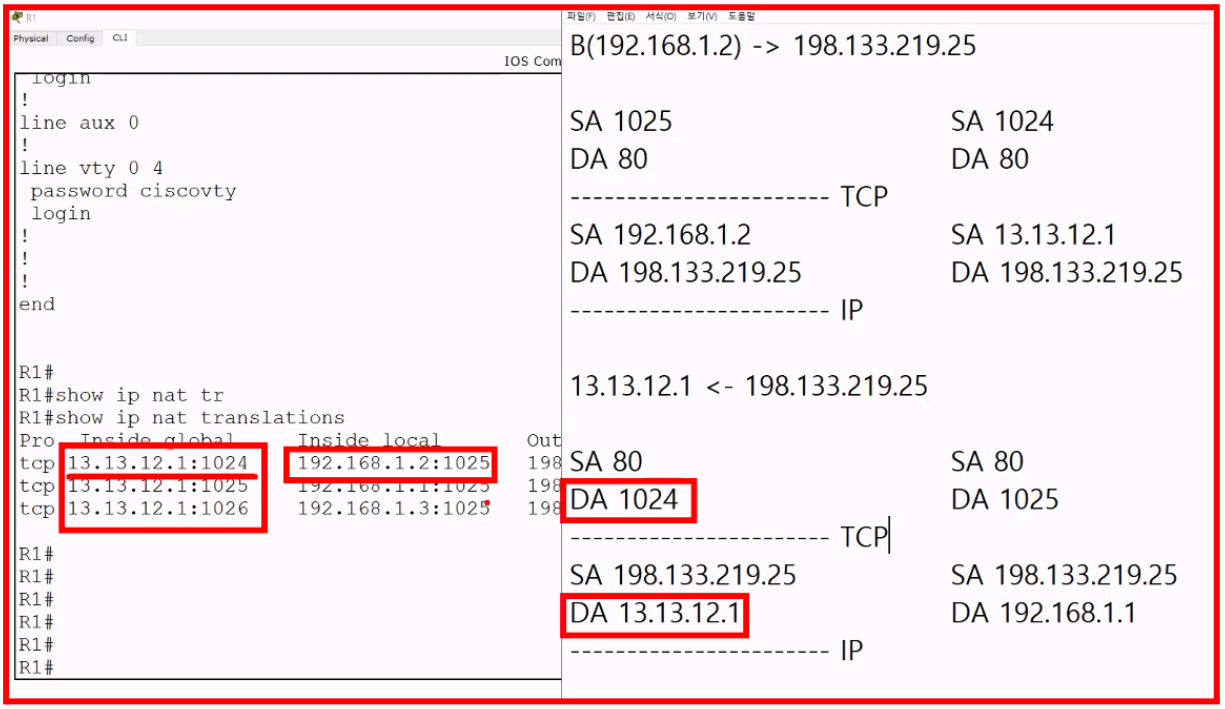
- NAT table
- NAT가 작동되는지 확인할 수 있는 테이블이다.

A PC:



- 포트번호를 이용해서 정확하게 inside local 주소를 알 수 있다.

B PC:



- overload 명령어가 포트번호를 담당한다.

포트번호까지 담당하면:
PNAT 라고한다. 또는 리눅스에서는 포트포워딩이라고 한다.

4. 정적 NAT 구성

외부 네트워크에서 내부 서버로 접근이 필요한 경우, 정적 NAT 를 구성해야 한다.

Inside Local : 192.168.1.253(웹 서버)
Inside Global : 13.13.12.100

```
R1#conf t
R1(config)#ip nat inside source static 192.168.1.253 13.13.12.100
R1(config)#
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#int s1/0
R1(config-if)#ip nat outside
R1(config-if)#end
R1#
```

R1#**show run**

```
~ 중간 생략 ~
!
ip nat inside source list 10 interface Serial1/0 overload
ip nat inside source static 192.168.1.253 13.13.12.100
ip classless
ip route 0.0.0.0 0.0.0.0 13.13.12.2
```

R1#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	13.13.12.100	192.168.1.253	---	---
tcp	13.13.12.1:1024	192.168.1.3:1025	198.133.219.25:80	198.133.219.25:80
tcp	13.13.12.1:1025	192.168.1.2:1025	198.133.219.25:80	198.133.219.25:80
tcp	13.13.12.1:1026	192.168.1.1:1026	198.133.219.25:80	198.133.219.25:80