NAT - 실습가이드

최초 작성일 : 2024/01/19

최종 제출일 : 2024/01/22

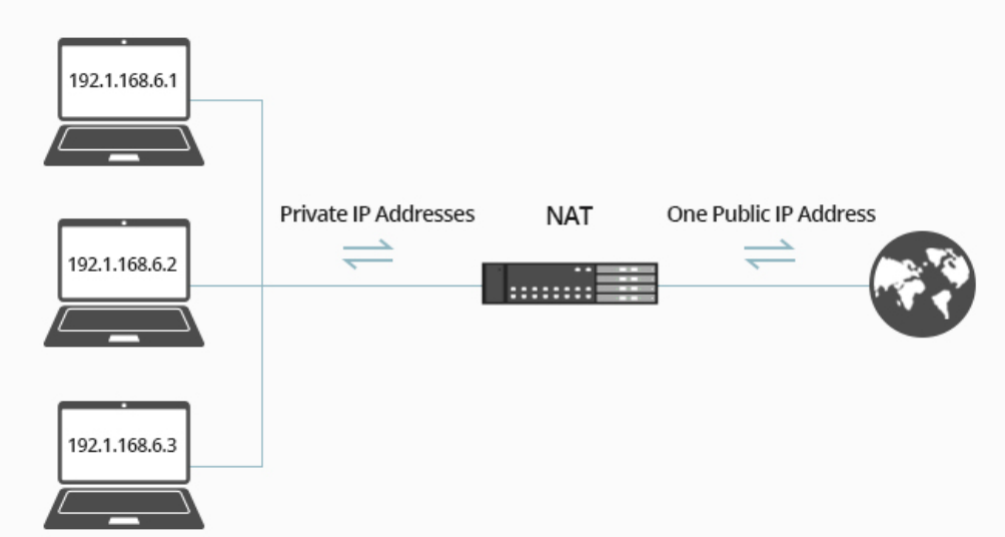
김민경

목차

Ⅰ. 개념정리

1. NAT

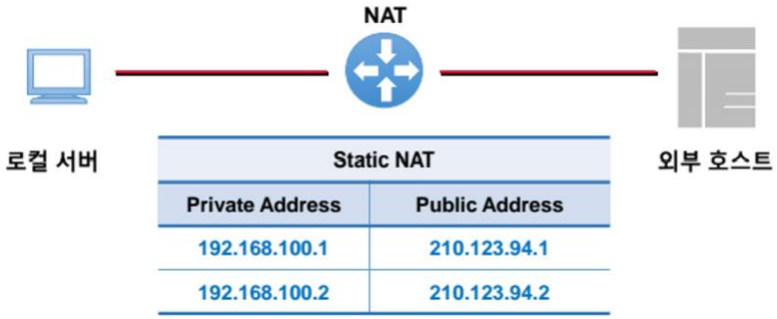
1) 정의



- Network Address Translation
- 주소 변환 기술
  - 공인 → 공인 or 사설
  - 사설 → 공인 or 사설

2) 종류

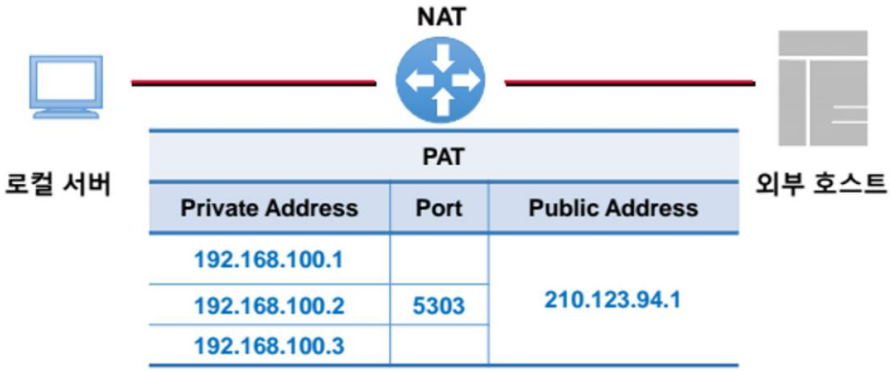
① Static NAT



Static NAT	
Private Address	Public Address
192.168.100.1	210.123.94.1
192.168.100.2	210.123.94.2

- 사설 ip 1개 & 공인 ip 1개 mapping

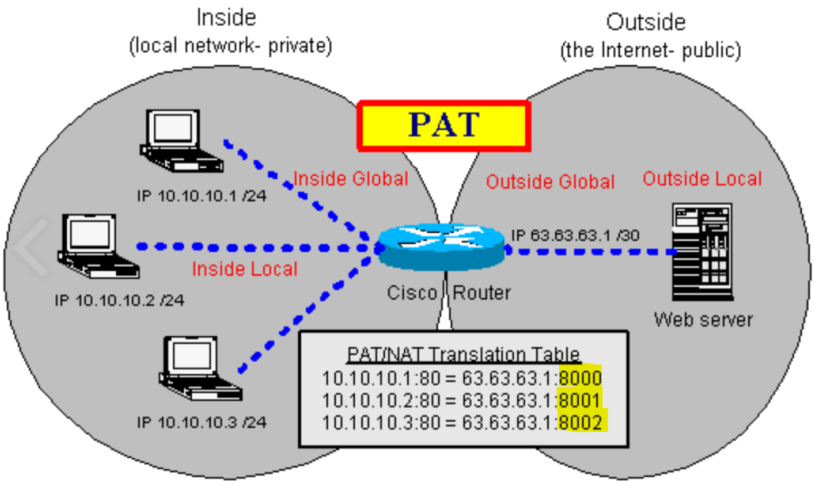
② Dynamic Nat



PAT		
Private Address	Port	Public Address
192.168.100.1		210.123.94.1
192.168.100.2	5303	
192.168.100.3		

- 여러 개의 사설 ip & 1개의 공인 ip를 동적으로 mapping
- 정해준 범위 내의 ip를 자동으로 mapping

③ NAT PAT



- PAT : Port Address Translation
- 공인 ip 1개에 여러 사설 ip를 mapping
- 변환된 ip 주소로 각 호스트를 구분할 수 x → 포트번호를 부여해 구분함

2. OSPF

1) 정의

- Open Shortest Path First
- 내부 라우터들끼리 라우팅 정보를 교환하는 라우팅 프로토콜

2) 명령어

- OSPF 설정 명령어

① 각 라우터에서 Process ID를 1로 설정하여 OSPF 구동시키기

R1(config)#router ospf 1

R1(config-router)#

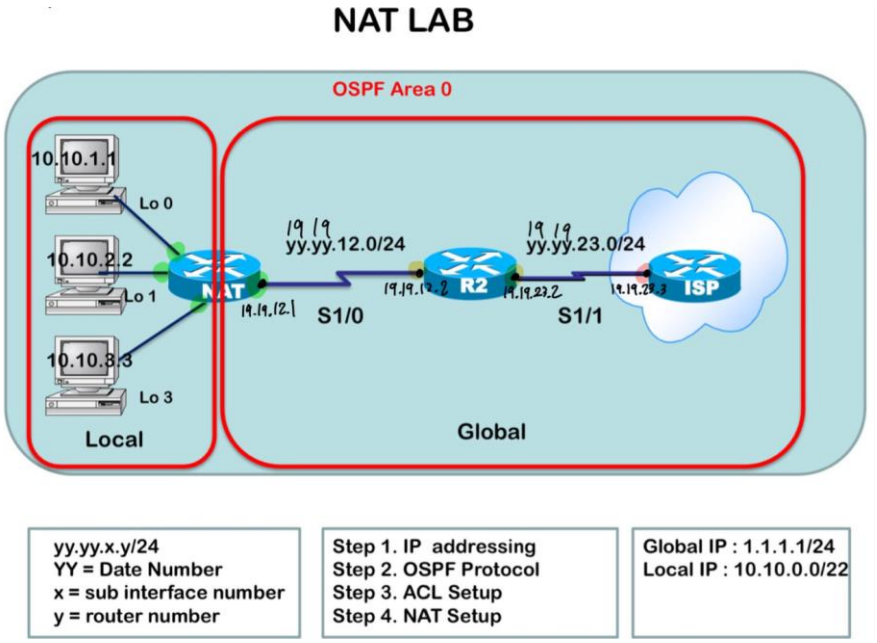
② OSPF로 광고할 네트워크 설정하기

R1(config-router)#network 192.168.10.1 0.0.0.0 area 0

R1(config-router)#

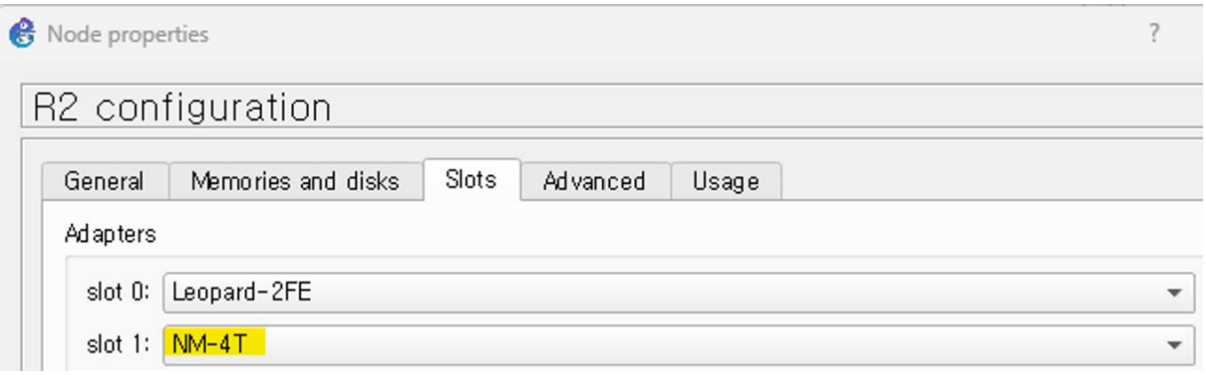
Ⅱ. 실습과정

1. 시나리오



2. 문제 1번 – IP 부여하기

1) 라우터 3개 다음과 같이 설정하고, 환경 구성하기



2) 각 라우터 인터페이스에 IP주기 (인접한 라우터끼리의 ping 통신 확인)

3) 루프백 설정하기

```
NAT(config-if)#int loopback 0
NAT(config-if)#ip a
*Mar  1 00:13:38.847: %LINEPROTO-5-UPDOWN: Line
NAT(config-if)#ip add 10.10.1.1 255.255.255.0
NAT(config-if)#no sh
NAT(config-if)#
```

```
NAT(config-if)#do show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  19.19.12.1      YES manual up                    up
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
Loopback0                  10.10.1.1       YES manual up                    up
Loopback1                  10.10.2.2       YES manual up                    up
Loopback2                  unassigned      YES unset  up                    up
Loopback3                  10.10.3.3       YES manual up                    up
```

3. 문제 2번 – OSPF 프로토콜 구현하기

1) 각 라우터마다 표시된 부분에 OSPF 설정하기

```
NAT(config-if)#router ospf 1
NAT(config-router)#network 10.10.1.0 0.0.0.255 area 0
NAT(config-router)#network 10.10.2.0 0.0.0.255 area 0
NAT(config-router)#network 10.10.3.0 0.0.0.255 area 0
NAT(config-router)#network 19.19.12.1 0.0.0.255 area 0
```

```
R2(config-router)#router ospf 1
R2(config-router)#network 19.19.12.2 0.0.0.255 area 0
R2(config-router)#network 19.19.23.2 0.0.0.255 area 0
```

```
ISP(config)#router ospf 1
ISP(config-router)#network 19.19.23.3 0.0.0.255 area 0
```

2) OSPF 설정 후 라우터 간의 연결 확인하기

```
NAT(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     19.0.0.0/24 is subnetted, 2 subnets
C       19.19.12.0 is directly connected, Serial1/0
O       19.19.23.0 [110/128] via 19.19.12.2, 00:04:59, Serial1/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.10.1.0 is directly connected, Loopback0
C       10.10.2.0 is directly connected, Loopback1
C       10.10.3.0 is directly connected, Loopback3
```

```
R2(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     19.0.0.0/24 is subnetted, 2 subnets
C       19.19.12.0 is directly connected, Serial1/0
C       19.19.23.0 is directly connected, Serial1/1
     10.0.0.0/32 is subnetted, 3 subnets
O       10.10.3.3 [110/65] via 19.19.12.1, 00:09:44, Serial1/0
O       10.10.2.2 [110/65] via 19.19.12.1, 00:09:44, Serial1/0
O       10.10.1.1 [110/65] via 19.19.12.1, 00:09:44, Serial1/0
```

```
ISP(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     19.0.0.0/24 is subnetted, 2 subnets
O       19.19.12.0 [110/128] via 19.19.23.2, 00:06:12, Serial1/1
C       19.19.23.0 is directly connected, Serial1/1
     10.0.0.0/32 is subnetted, 3 subnets
O       10.10.3.3 [110/129] via 19.19.23.2, 00:06:02, Serial1/1
O       10.10.2.2 [110/129] via 19.19.23.2, 00:06:02, Serial1/1
O       10.10.1.1 [110/129] via 19.19.23.2, 00:06:02, Serial1/1
```

3) 결과 확인하기

- ping으로 서로 간의 통신 확인

NAT → R2

```
NAT(config)#do ping 19.19.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/40 ms
```

NAT → ISP

```
NAT(config)# do p 19.19.23.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/65/68 ms
```

R2 → NAT

```
R2(config)#do p 19.19.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/31/36 ms
```

R2 → ISP

```
R2(config)#do p 19.19.23.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/40 ms
```

ISP → R2

```
ISP(config)#do p 19.19.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/27/32 ms
ISP(config)#
```

ISP → R3

```
ISP(config)#do p 19.19.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/72 ms
```

4. 문제 3번 – ACL 이용해 내부→외부 접근 차단하기

1) ACL 정책 생성 후 R2 라우터의 Inbound로 적용하기

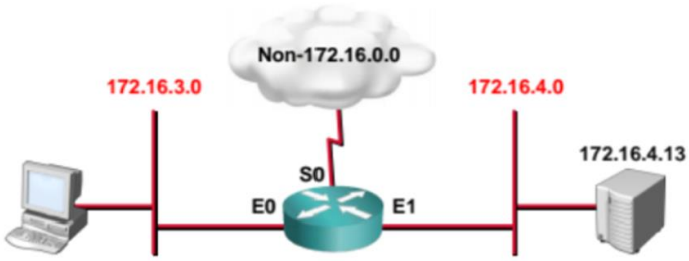
```
R2(config)#access-list 1 deny 10.10.0.0 0.0.255.255
R2(config)#acc
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#int s1/0
R2(config-if)#ip access-group 1 in
```

- NAT 라우터의 outbound로 설정하면 X

  ⇒ 루프백을 가지고 있어서 자신이 만든 정책은 필터링하지 않고 내보내기 때문

- deny할 때 자동으로 deny 설정이 들어가기 때문에 마지막에 permit any로

  다른 출발지는 허용해줘야 함




```
Router(config)#access-list 1 deny 172.16.4.0 0.0.0.255
Router(config)#access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

Router(config)#interface ethernet 0
Router(config-if)#ip access-group 1 out
```

2) 결과 확인하기

- 각 PC → ISP

  명령어) do ping 19.19.23.3 source 10.10.1.1

  - 10.10.1.1 →19.19.23.3으로 ping을 보낼 것이라는 뜻

```
NAT#ping 19.19.23.3 source 10.10.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.1.1
UUUUU
Success rate is 0 percent (0/5)
NAT#
NAT#ping 19.19.23.3 source 10.10.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.2.2
UUUUU
Success rate is 0 percent (0/5)
NAT#
NAT#ping 19.19.23.3 source 10.10.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.3.3
UUUUU
Success rate is 0 percent (0/5)
```

5. 문제 4번 – NAT를 이용해 다시 내부→외부 접근 허용하기

1) Dynamic Nat 설정으로 10.0.0.0/22 → 1.1.1.1/24로 변환하기

① pubic 주소 풀 설정

```
NAT(config)#ip nat pool change 1.1.1.1 1.1.1.254 netmask 255.255.255.0
```

명령어)

ip nat pool {이름} {public_시작 주소} {public_마지막 주소} {netmask 서브넷_마스크}

② 변환할 사설 ip 지정

```
NAT(config)#access-list 1 permit 10.10.0.0 0.0.3.255
```

명령어)

access-list {access-list 번호} permit {Source ip} { Source ip 와일드마스크 카드}

③ Dynamic NAT로 설정

```
NAT(config)#ip nat inside source list 1 pool change overload
```

명령어)

ip nat inside source list {access-list 번호} pool {이름} {overload}

④ NAT를 해당 인터페이스에 적용하기

```
NAT(config-if)#int lo 0
NAT(config-if)#ip nat inside
NAT(config-if)#
NAT(config-if)#int lo 1
NAT(config-if)#ip nat inside
NAT(config-if)#
NAT(config-if)#int lo 3
NAT(config-if)#ip nat inside
```

```
NAT(config-if)#int s1/0
NAT(config-if)#ip nat outside
```

명령어)

int {인터페이스}

ip nat inside

int {인터페이스}

ip nat outside

2) 결과 확인하기

- ping 통신 실패

```
NAT(config-if)#do ping 19.19.23.3 source 10.10.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.1.1
.....
Success rate is 0 percent (0/5)
```

- 디버그를 통해 살펴보기

```
NAT(config-if)#do debug ip nat
IP NAT debugging is on
NAT(config-if)#do ping 19.19.23.3 source 10.10.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.1.1

*Mar  1 01:16:35.495: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [75].
*Mar  1 01:16:37.495: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [76].
*Mar  1 01:16:39.495: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [77].
*Mar  1 01:16:41.495: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [78].
*Mar  1 01:16:43.495: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [79].
Success rate is 0 percent (0/5)
NAT(config-if)#
```

- 사설 ip → 공인 ip로 변환은 됨

- 1.1.1.1/24가 어디로 가는지 알려줘야 함 (static route로)

3) static route 설정하기

```
R2(config)#ip route 1.1.1.0 255.255.255.0 19.19.12.1
```

```
ISP(config)#ip route 1.1.1.0 255.255.255.0 19.19.23.2
```

4) 결과 다시 확인하기

- NAT router의 loopback 0→ ISP

```
NAT(config)#do ping 19.19.23.3 source 10.10.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/64/76 ms
NAT(config)#
NAT(config)#
NAT(config)#
*Mar  1 01:27:17.107: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [80]
*Mar  1 01:27:17.159: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.1.1 [80]
*Mar  1 01:27:17.163: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [81]
*Mar  1 01:27:17.235: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.1.1 [81]
*Mar  1 01:27:17.235: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [82]
*Mar  1 01:27:17.299: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.1.1 [82]
*Mar  1 01:27:17.299: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [83]
*Mar  1 01:27:17.363: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.1.1 [83]
*Mar  1 01:27:17.367: NAT: s=10.10.1.1->1.1.1.1, d=19.19.23.3 [84]
*Mar  1 01:27:17.427: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.1.1 [84]
```

- NAT router의 loopback 1→ ISP

```
NAT(config)#do ping 19.19.23.3 source 10.10.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/68 ms
NAT(config)#
*Mar  1 01:28:16.275: NAT: s=10.10.2.2->1.1.1.1, d=19.19.23.3 [85]
*Mar  1 01:28:16.335: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.2.2 [85]
*Mar  1 01:28:16.339: NAT: s=10.10.2.2->1.1.1.1, d=19.19.23.3 [86]
*Mar  1 01:28:16.403: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.2.2 [86]
*Mar  1 01:28:16.407: NAT: s=10.10.2.2->1.1.1.1, d=19.19.23.3 [87]
*Mar  1 01:28:16.471: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.2.2 [87]
*Mar  1 01:28:16.475: NAT: s=10.10.2.2->1.1.1.1, d=19.19.23.3 [88]
*Mar  1 01:28:16.535: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.2.2 [88]
*Mar  1 01:28:16.535: NAT: s=10.10.2.2->1.1.1.1, d=19.19.23.3 [89]
*Mar  1 01:28:16.599: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.2.2 [89]
NAT(config)#
*Mar  1 01:28:17.659: NAT: expiring 1.1.1.1 (10.10.1.1) icmp 16 (16)
```

- NAT router의 loopback 3→ ISP

```
NAT(config)#do ping 19.19.23.3 source 10.10.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.23.3, timeout is 2 seconds:
Packet sent with a source address of 10.10.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/60/68 ms
NAT(config)#
*Mar  1 01:29:00.987: NAT: s=10.10.3.3->1.1.1.1, d=19.19.23.3 [90]
*Mar  1 01:29:01.047: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.3.3 [90]
*Mar  1 01:29:01.047: NAT: s=10.10.3.3->1.1.1.1, d=19.19.23.3 [91]
*Mar  1 01:29:01.099: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.3.3 [91]
*Mar  1 01:29:01.103: NAT: s=10.10.3.3->1.1.1.1, d=19.19.23.3 [92]
*Mar  1 01:29:01.159: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.3.3 [92]
*Mar  1 01:29:01.163: NAT: s=10.10.3.3->1.1.1.1, d=19.19.23.3 [93]
*Mar  1 01:29:01.227: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.3.3 [93]
*Mar  1 01:29:01.231: NAT: s=10.10.3.3->1.1.1.1, d=19.19.23.3 [94]
*Mar  1 01:29:01.299: NAT*: s=19.19.23.3, d=1.1.1.1->10.10.3.3 [94]
NAT(config)#
*Mar  1 01:29:17.051: NAT: expiring 1.1.1.1 (10.10.2.2) icmp 17 (17)
```