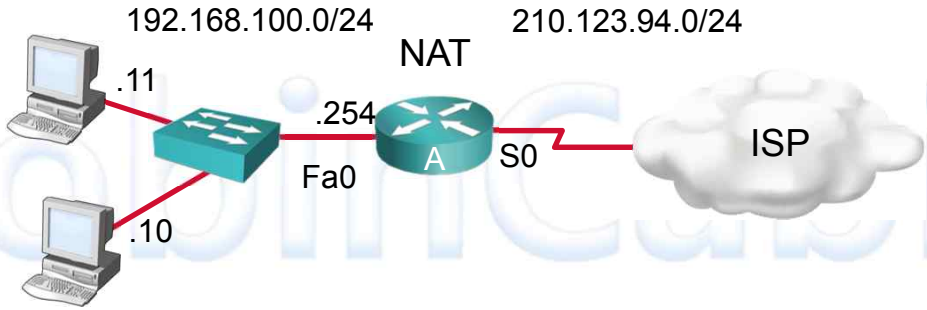
NAT(Network Address Translation)

NAT 개요

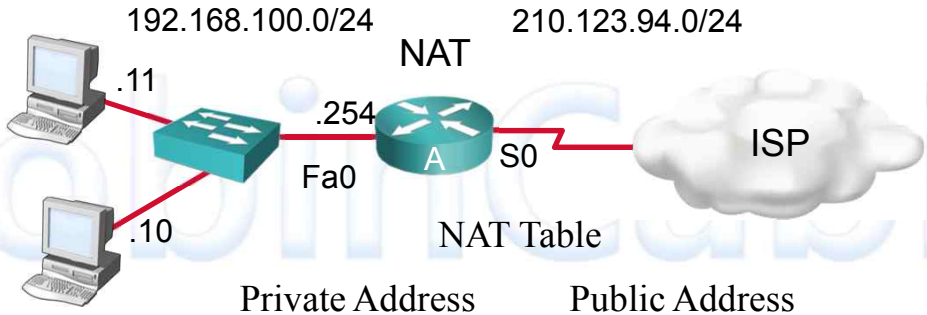


- RFC 1631에 정의된 것으로 IP Header의 주소를 다른 주소로 바꾸는 기술이다.
- 사설주소를 사용하는 호스트들이 인터넷에 서비스를 이용할 수 있도록 하기 위해 사용한다

NAT(Network Address Translation)

NAT 개요

Dynamic & Static NAT



NAT Table

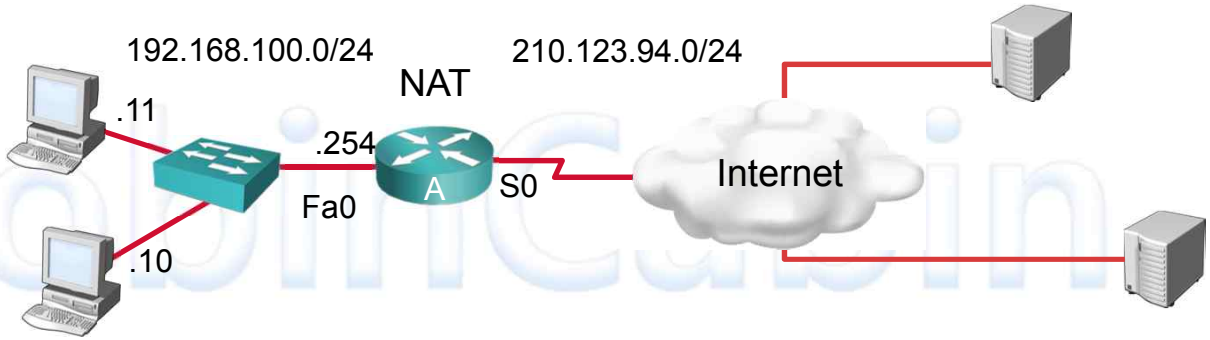
Private Address	Public Address
192.168.100.10	210.123.94.1
192.168.100.11	210.123.94.2

- 동적 NAT
  - 로컬 네트워크의 특정 호스트가 요구하는 Traffic을 받으면, 해당 호스트의 사설 IP를 NAT Router 에 설정된 주소 풀의 공인 IP로 변환한 후 외부로 전달한다.
  - 외부에서 응답 traffic이 라우터로 돌아오면, NAT Table에 기록된 정보를 이용하여 사설 IP로 변환해서 내부 망으로 전달한다
- 정적 NAT
  - 외부주소로 들어온 요청이 내부 서버로 전달 될 수 있도록 목적지 주소를 변환하는 기능이다.
  - 사설 망 서버를 구현하고 외부 주소로 들어오는 연결을 내부 서버로 전달할 수 있다

NAT(Network Address Translation)

NAT 개요

PAT(Port Address Translation)



NAT Table			
Inside Local IP	Inside Global IP	Outside Global IP	Outside Local IP
192.168.100.10:1555	210.123.94.1:1555	209.165.201.1:80	209.165.201.1:80
192.168.100.11:1331	210.123.94.1:1331	209.165.202.129:80	209.165.202.129:80

- PAT 또는 NAT Overloading
  - 다수의 사설 IP 주소들을 하나의 공인 IP주소 또는 복수 개의 주소들에 mapping시킨다

NAT(Network Address Translation)

NAT 개요

- Inside Local IP Address
  - 일반적으로 서비스 제공업자에 의해 할당된 IP가 아니라 RFC1918 사설 주소를 사용
- Inside Global IP Address
  - 내부 호스트가 NAT router를 빠져나갈 때 주어지는 공인 주소
- Outside Global IP Address
  - 인터넷의 호스트에 할당된 도달 가능한 IP 주소
- Outside Local IP Address
  - 외부 네트워크의 호스트에 할당된 로컬 IP 주소
- Port Address Translation
  - Port Number
    - 65,536개가 될 수 있지만, 약 4,000개의 내부 주소들이 하나의 IP주소에 할당될 수 있다.
    - 출발지 포트가 이미 사용되고 있으면, NAT Overload는 0-511, 512-1023, 또는 1024-65535의 처음부터 시작하는 이용 가능한 첫 번째 포트 번호를 할당.
    - 더 이상 이용할 수 있는 포트들이 없으면, 다음 IP주소로 이동
  - 첫 번째 packet는 항상 processing switching을 한다
  - Port Forwarding :
    - 한 네트워크의 node에서 다른 node로 포트를 전송
    - 외부 사용자가 NAT Router를 통해 내부 사설IP 주소의 포트에 도달하는 것을 허용한다.

NAT(Network Address Translation)

NAT 설정

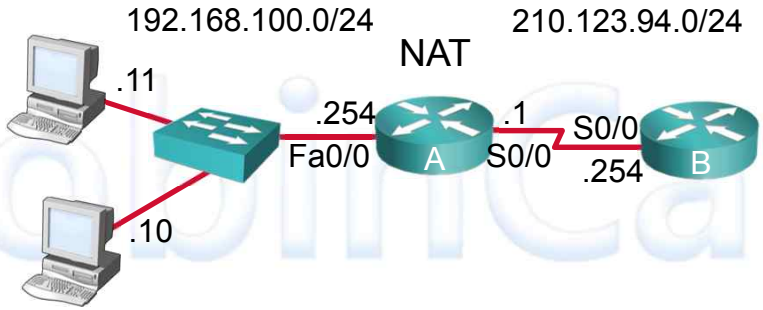
Dynamic NAT Configuration

- IP 변환에 사용할 전역 주소풀을 설정한다
  - Router(config)#ip nat pool name start-ip end-ip {netmask *Netmask* | prefix-length *Prefix-length*}
- 내부에서 IP변환을 허용할 주소를 Standard Access-list로 정의한다
  - Router(config)#Access-list number permit source-address [Wildcard-mask]
- 동적 변환을 수립하기 위한 NAT 설정을 한다
  - Router(config)#ip nat inside source list Access-list-number pool name [overload]
- 각 인터페이스로 이동 후 내부와 외부를 각각 설정한다
  - Router(config-if)#ip nat inside
  - Router(config-if)#ip nat outside

NAT(Network Address Translation)

Dynamic NAT

Dynamic NAT Example

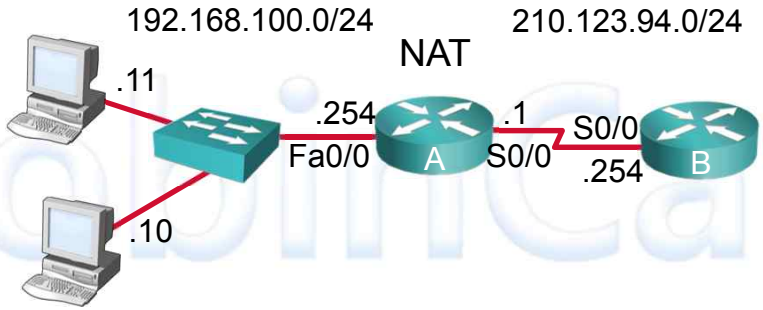


- NAT(config)#ip nat pool Pub_IP 10.1.0.1 10.1.0.99 netmask 255.255.255.0
- NAT(config)#access-list 10 permit 192.168.100.0 0.0.0.255
- NAT(config)#ip nat inside source list 10 pool Pub_IP
- NAT(config)#int Fa0/0
- NAT(config-if)#ip nat inside
- NAT(config-if)#int s0/0
- NAT(config-if)#ip nat outside

NAT(Network Address Translation)

Static NAT

Static NAT Configuration

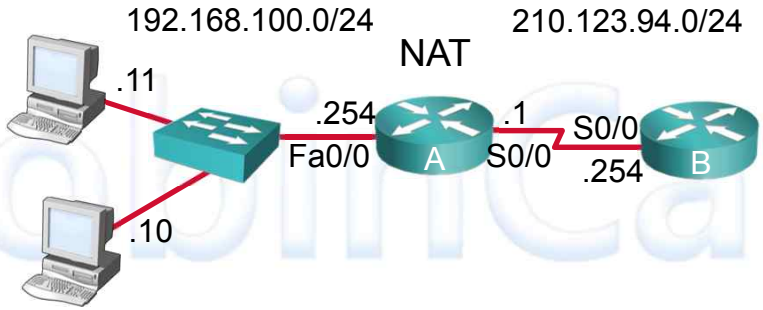


- 정적 변환을 수립하기 위한 NAT 설정을 한다
  - Router(config)#ip nat inside source Static *local-ip global-ip*
- 각 인터페이스로 이동 후 내부와 외부를 각각 설정한다
  - Router(config-if)#ip nat inside
  - Router(config-if)#ip nat outside

NAT(Network Address Translation)

Static NAT

Static NAT Example

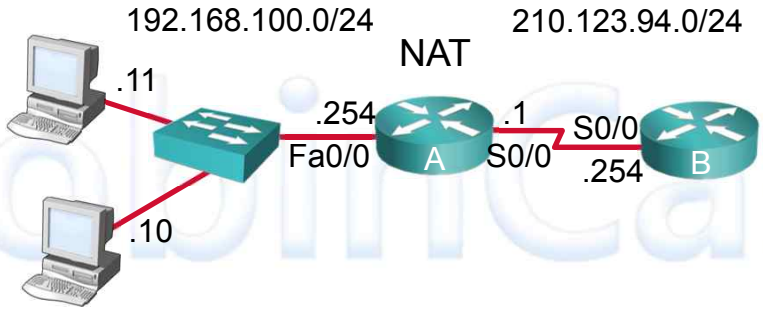


- NAT(config)#ip nat inside source static 192.168.100.10 10.1.0.100
- NAT(config)#int Fa0/0
- NAT(config-if)#ip nat inside
- NAT(config-if)#int s0/0
- NAT(config-if)#ip nat outside

NAT(Network Address Translation)

Dynamic NAT

NAT-PAT Example



- NAT(config)#ip nat pool Pub_IP 10.1.0.1 10.1.0.99 netmask 255.255.255.0
- NAT(config)#access-list 10 permit 192.168.100.0 0.0.0.255
- NAT(config)#ip nat inside source list 10 pool Pub_IP overload
- NAT(config)#int Fa0/0
- NAT(config-if)#ip nat inside
- NAT(config-if)#int s0/0
- NAT(config-if)#ip nat outside

NAT(Network Address Translation)

NAT 검증

NAT Monitoring

- 변환 테이블 내의 모든 항목 삭제
  - Router#clear ip nat translation *
- 내부 및 외부변환을 모두 포함하는 단순 동적 변환 주소 엔트리를 제거하기
  - Router#clear ip nat translation inside *global-ip local-ip* outside *global-ip local-ip*
- 활성화된 변환 정보 보기
  - Router#show ip nat translation [verbose]
- 변환된 통계 정보 보기
  - Router#show ip nat statistics
- 변환된 IP정보는 24시간 이후에 삭제
  - ip nat translation timeout timeout_seconds

NAT(Network Address Translation)

NAT Table

NAT Table 보기

```
NAT#show ip nat translations
Pro   Inside global     Inside local       Outside local      Outside global
udp   10.1.0.1:1438     172.16.1.10:1438   200.200.200.254:69   200.200.200.254:69
udp   10.1.0.1:1439     172.16.1.11:1438   200.200.200.254:69   200.200.200.254:69
```

```
NAT#show ip nat statistics
```

NAT(Network Address Translation)

NAT 검증

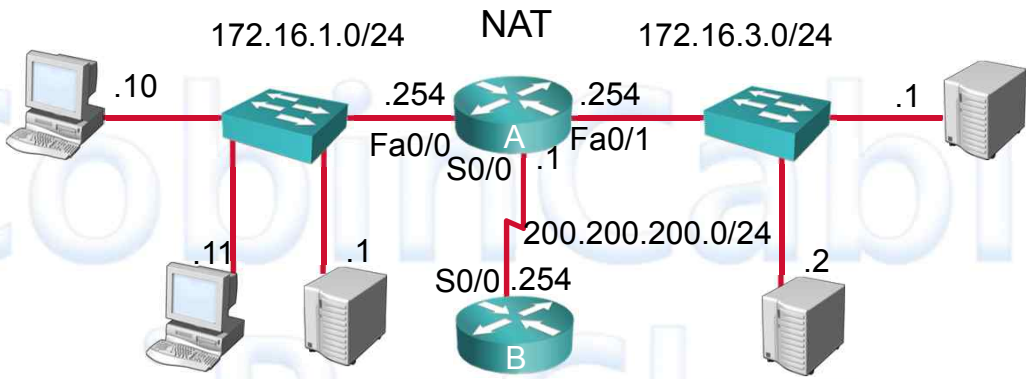
NAT 변환 상태 모니터링

- Router#debug ip nat
  - *IP NAT debugging is on*
    **OCT 6 19:55:31.579: NAT* : s=172.16.1.10->10.1.0.1, d=200.200.200.254 [14434]*
- NAT*
  - Fast switched 경로 변환이 일어나고 있다는 것을 가리킨다
- s=
  - 출발지 IP address
- a.b.c.d->w.x.y.z
  - 출발지 주소 a.b.c.d가 w.x.y.z로 변환
- d=
  - 목적지 IP address
- [xxxx]
  - IP 식별 번호로써, 다른 패킷과의 상관 관계를 추적 할 수 있다.

NAT(Network Address Translation)

Dynamic NAT

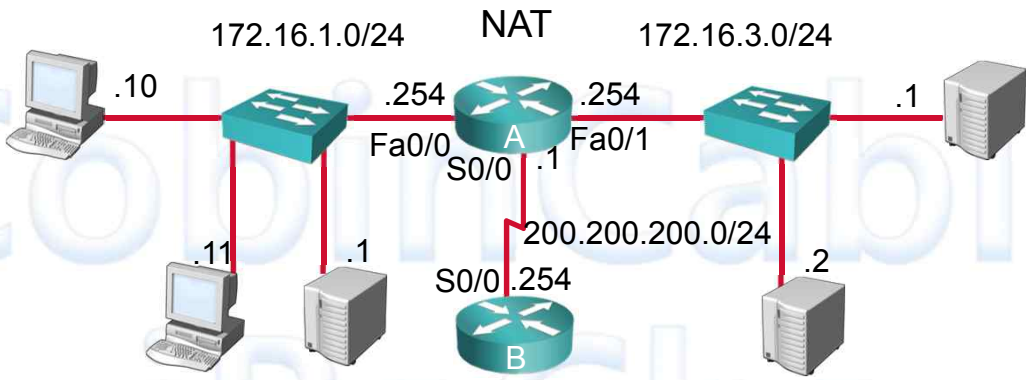
NAT LAB



NAT(Network Address Translation)

Dynamic NAT

Dynamic NAT LAB

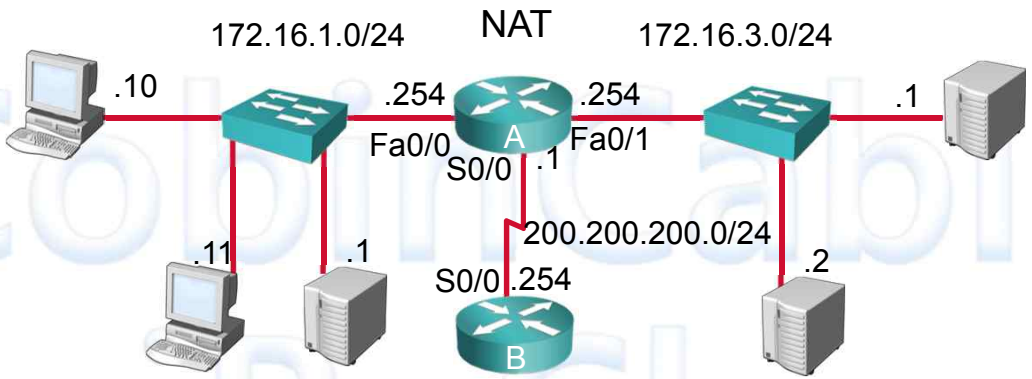


- NAT(config)#ip nat pool LocalSite 10.1.0.10 10.1.0.99 netmask 255.255.255.0
- NAT(config)#access-list 10 permit 172.16.1.0 0.0.0.255
- NAT(config)#ip nat inside source list 10 pool LocalSite
- NAT(config)#int Fa0/0
- NAT(config-if)#ip nat inside
- NAT(config-if)#int s0/0
- NAT(config-if)#ip nat outside

NAT(Network Address Translation)

Static NAT

Static NAT LAB

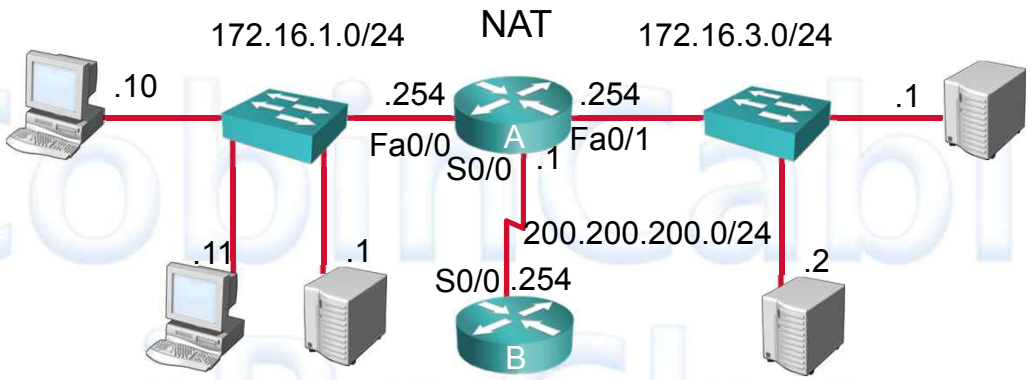


- NAT(config)#ip nat inside source static 172.16.1.1 10.1.0.9
- NAT(config)#int Fa0/0
- NAT(config-if)#ip nat inside
- NAT(config-if)#exit
- NAT(config)#int s0/0
- NAT(config-if)ip nat outside

NAT(Network Address Translation)

Dynamic NAT

NAT-PAT LAB



- NAT(config)#ip nat pool ServerFarm 10.1.0.1 10.1.0.8 netmask 255.255.255.0
- NAT(config)#access-list 20 permit 172.16.3.0 0.0.0.255
- NAT(config)#ip nat inside source list 20 pool ServerFarm overload
- NAT(config)#int Fa0/1
- NAT(config-if)#ip nat inside
- NAT(config-if)#int s0/0
- NAT(config-if)#ip nat outside