

# NAT – Network Address Translation

## <NAT – Network Address Translation>

- 내부 네트워크에서는 사설 IP를 사용하고, 외부 네트워크 (Internet)로 나가는 경우 공인 IP주소로 변환돼서 나가게 하는 기술
- 공인 IP주소의 부족으로 많이 사용.
- 보안과 경제상의 이유로 NAT를 이용해서 사설 IP를 사용하기도 한다.

공인 IP : 유료, 외부와 통신 가능 (Internet 사용 가능)

사설 IP : 무료, 외부와 통신 불가능 (Internet 사용 X)

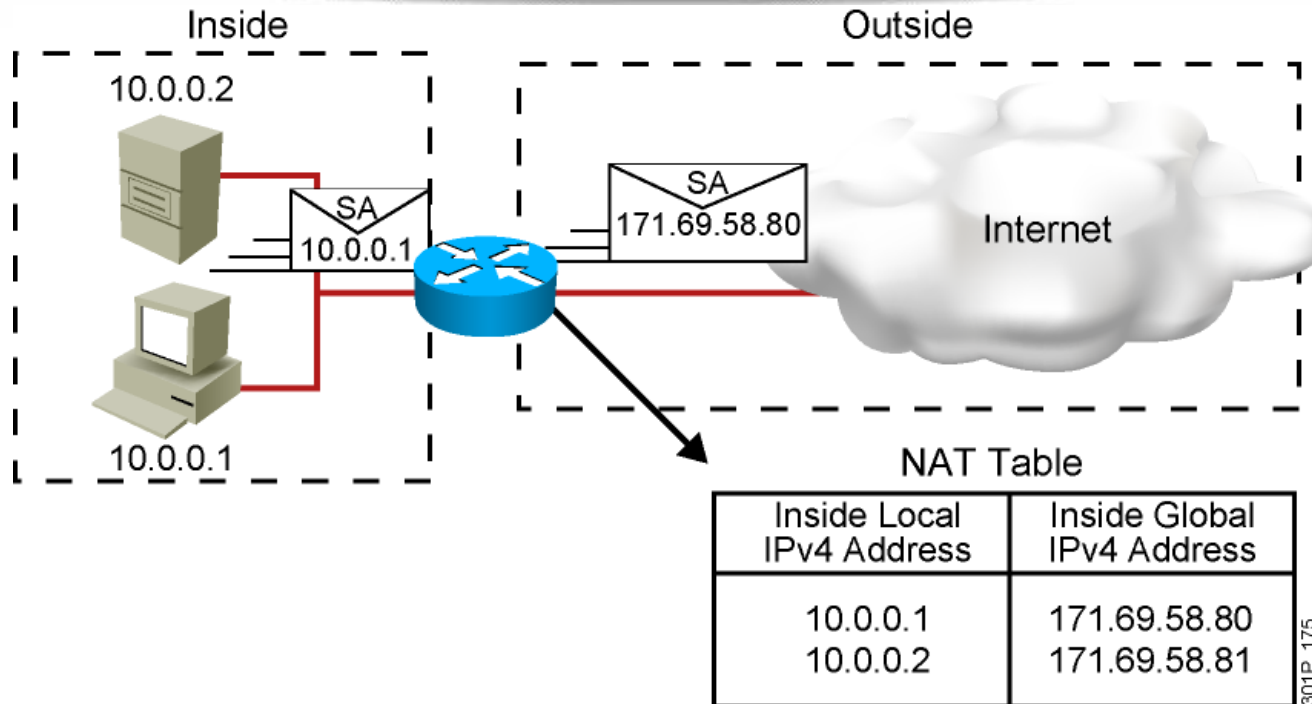
- NAT는 실제 출발지 주소가 아닌 다른 주소로 변환되어 외부 네트워크로 나가기 때문에 내부 네트워크 정보를 공개하지 않는다.
- ➔ 어느 정도 보안적인 역할도 수행.  
(즉, 외부에서 내부 사설망으로는 접근이 힘들다.)

# NAT – Network Address Translation

## 사설 IP address

- Class A : 10.0.0.0 ~ 10.255.255.255 (10.0.0.0 /8)
- Class B : 172.16.0.0 ~ 172.31.255.255 (172.16.0.0 /12)
- Class C : 192.168.0.0 ~ 192.168.255.255 (192.168.0.0 /16)

# NAT – Network Address Translation



- An IP address is either local or global.
- Local IPv4 addresses are seen in the inside network.
- Global IPv4 addresses are seen in the outside network.

# NAT – Network Address Translation

- NAT에는 **Static NAT**, **Dynamic NAT**, **PAT**(Port address translation)가 있다.

## 1) Static NAT

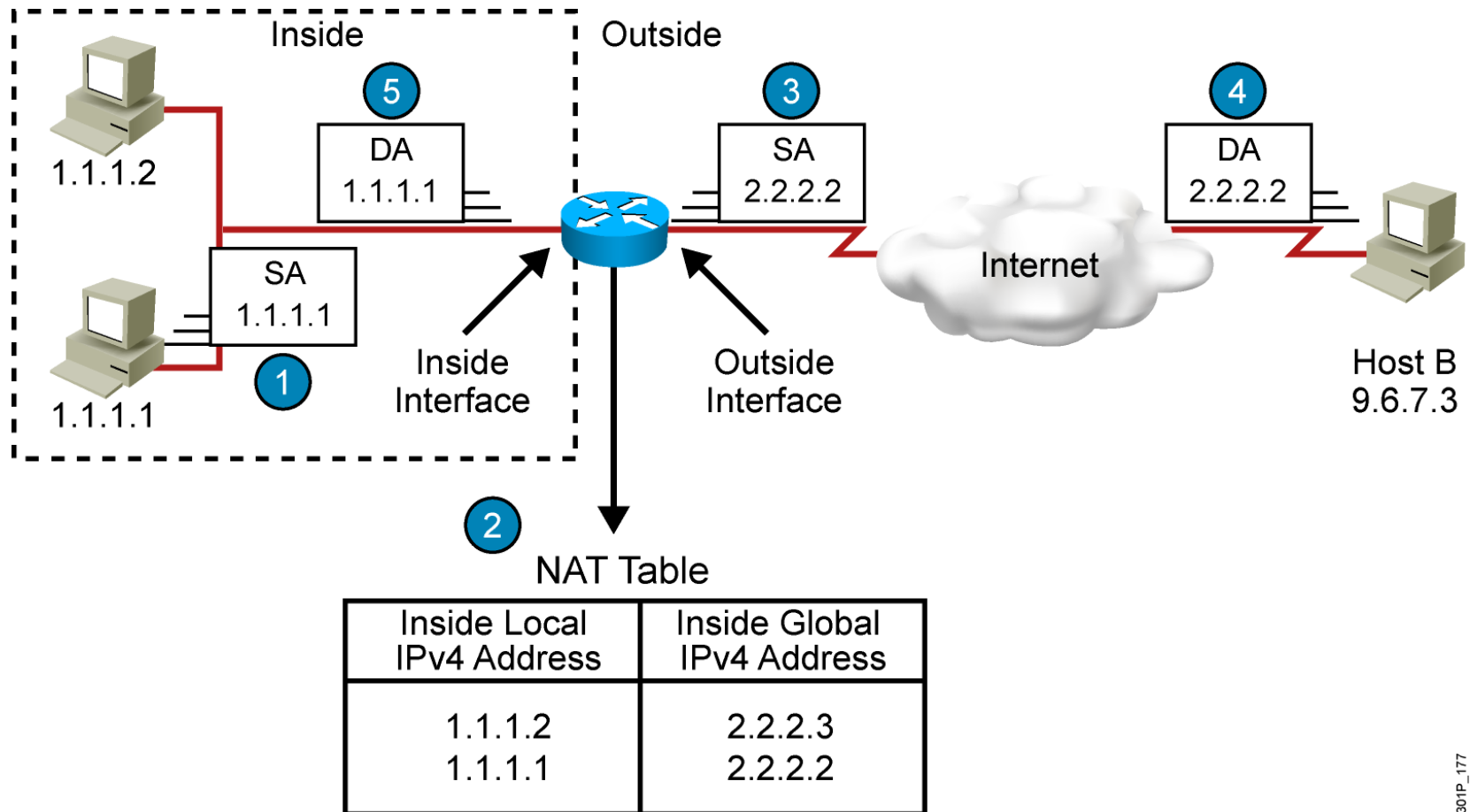
- **Inside Local IP** 주소와 **Inside Global IP** 주소간에 **일대일 Mapping** 하도록 설정
- **DNS** 서버나 이메일 서버 같이 외부 인터넷에서 접속해야 하는 내부 **IP** 호스트에 유용하다.
- 호스트가 꼭 변하지 않는 **global** 주소를 가져야 할 경우 **static NAT** 사용
- 외부에서 내부 사설망을 접속하고자 할 때 사용

## 2) Dynamic NAT

- **Inside Global IP** 주소 그룹 (**pool**)에서 하나의 **Inside Global IP** 주소를 **IP** 주소와 동적으로 **Mapping**되도록 설정.  
(즉, 공인 **IP** 그룹과 사설 **IP** 그룹을 **그룹 대 그룹으로 Mapping**)
  - ➔ 사설망에서 인터넷에 접속할 때 주로 사용.



# NAT – Network Address Translation



# NAT – Network Address Translation

## 1) Static NAT 설정

```
RouterX(config)# ip nat inside source static <local-ip> <global-ip>
```

→ **inside Local IP** 주소와 **Inside Global IP** 주소간에 **일대일 Mapping**

```
RouterX(config)#interface fastethernet 0/0  
RouterX(config-if)# ip nat inside
```

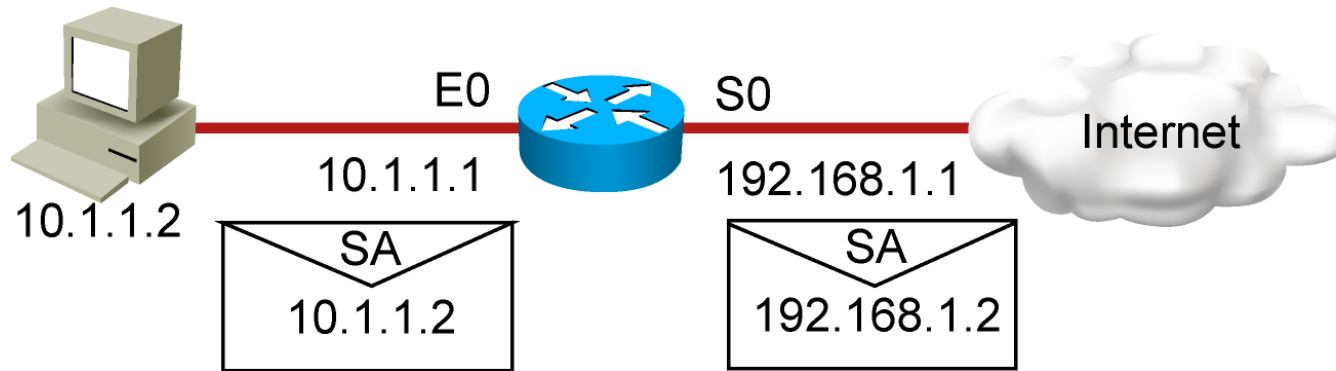
→ Fast ethernet 0/0을 NAT **내부 Interface**로 지정

```
RouterX(config)#interface serial 0/1  
RouterX(config-if)# ip nat outside
```

→ Serial 0/1을 NAT **외부 Interface**로 지정

# NAT – Network Address Translation

## 1) Static NAT 설정



```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

```
RouterX# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	192.168.1.2	10.1.1.2	---	---

# NAT – Network Address Translation

## 1) Static NAT 예제

- 내부 네트워크에서 사용되는 사설 IP 주소 192.168.1.1~192.168.1.2를 공인 IP주소 102.19.10.1~102.19.10.2(/24)로 항상 변환되도록 NAT를 설정하시오. (192.168.1.1은 102.19.10.1, 192.168.1.2는 102.19.10.2로)

```
Router(config)#ip nat inside source static 192.168.1.1 102.19.10.1  
Router(config)#ip nat inside source static 192.168.1.2 102.19.10.2
```

```
Router(config)#interface fastethernet 0/1  
Router(config-if)#ip nat inside
```

```
Router(config)#interface serial 0/1  
Router(config-if)#ip nat outside
```



# NAT – Network Address Translation

## 2) Dynamic NAT 설정

```
RouterX(config)# ip nat pool <name> <start-ip> <end-ip> netmask <subnet mask>
```

→ 공인 IP 그룹을 생성. **start-ip**와 **end-ip** 사이의 IP가 공인 IP 그룹이 된다.

```
RouterX(config)# access-list <list-number> permit <source> <wildcard mask>
```

→ 사설 IP 그룹을 생성. **ACL**로 사설 IP 그룹을 지정.

```
RouterX(config)# ip nat inside source list <list-number> pool <name>
```

→ 공인 IP 그룹과 사설 IP 그룹을 그룹 대 그룹으로 Mapping.

```
RouterX(config)#interface fastethernet 0/0  
RouterX(config-if)# ip nat inside
```

→ Fast ethernet 0/0을 NAT 내부 Interface로 지정

```
RouterX(config)#interface serial 0/1  
RouterX(config-if)# ip nat outside
```

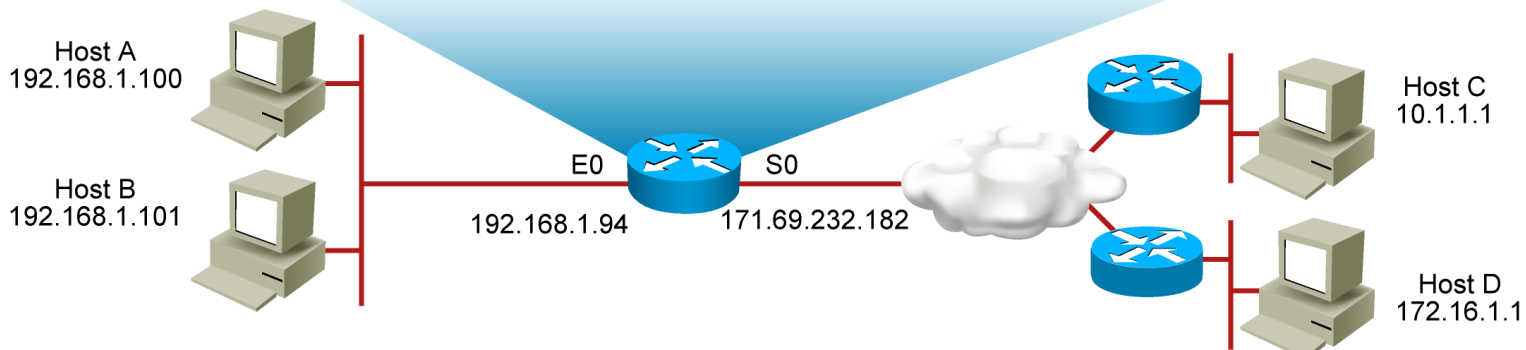
→ Serial 0/1을 NAT 외부 Interface로 지정

# NAT – Network Address Translation

## 2) Dynamic NAT 설정

```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

301P\_465



RouterX# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	171.69.233.209	192.168.1.100	---	---
---	171.69.233.210	192.168.1.101	---	---

# NAT – Network Address Translation

## 2) Dynamic NAT 설정

- 내부 네트워크는 사설 IP 192.168.1.0/24 주소를 사용하고 외부와 통신을 할 경우는 151.11.2.1~151.11.2.254(/24)사이의 공인 IP 주소로 변환돼서 정상적으로 외부와 통신이 가능하도록 NAT 설정을 하시오.

```
Router(config)#ip nat pool AA 151.11.2.1 151.11.2.254 netmask 255.255.255.0
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 10 pool AA
```

```
Router(config)#interface fastethernet 0/1
Router(config-if)#ip nat inside
```

```
Router(config)#interface serial 0/1
Router(config-if)#ip nat outside
```

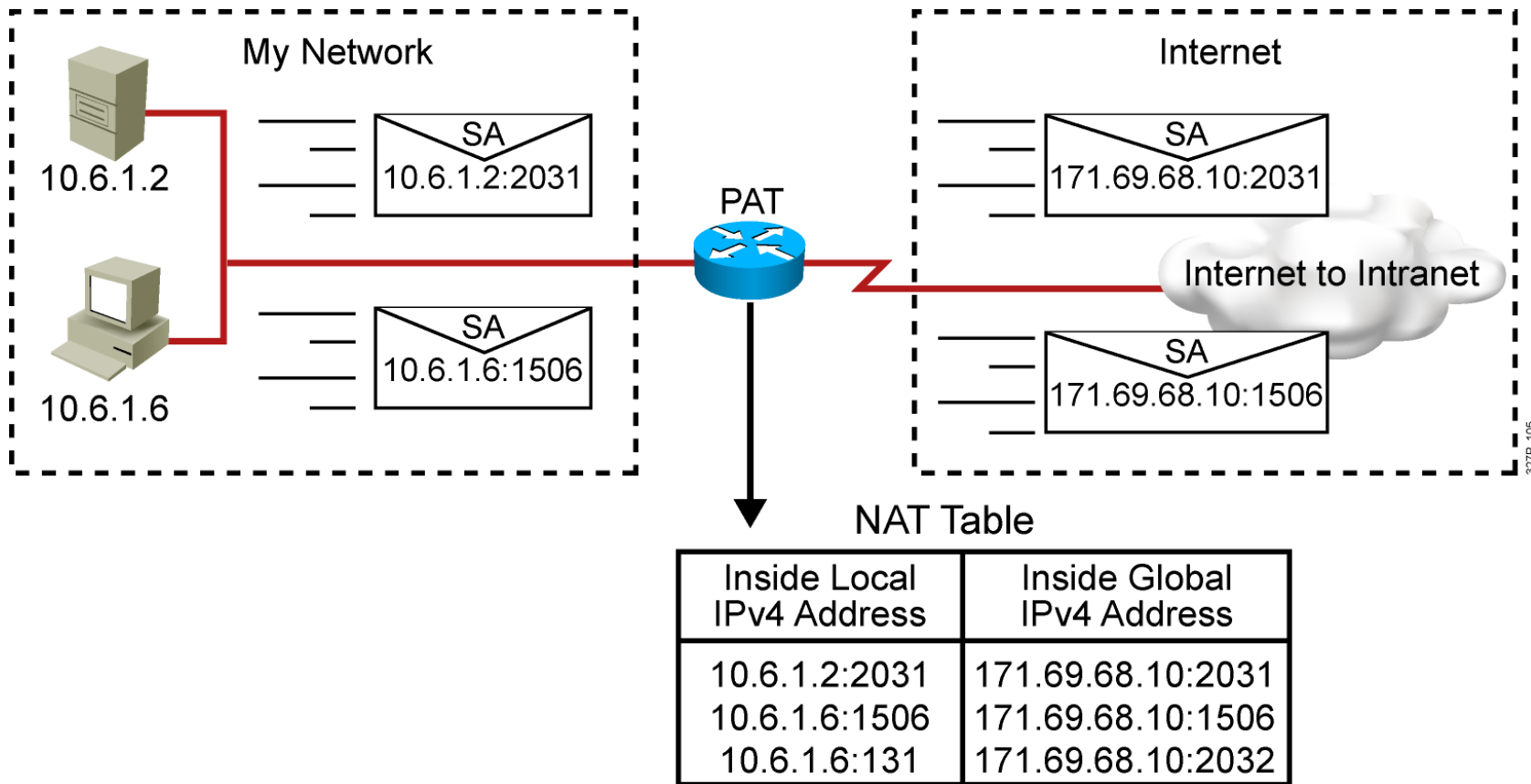
# PAT – Port Address Translation

## 3) PAT(Port address translation)

- 다수의 사설 IP를 1개의 공인 IP로 변환시켜서 외부와 통신이 가능하게 하는 기술.  
(이론적으로는 64000개의 사설 IP를 하나의 공인 IP로 사용 가능)
- host마다 Port 번호를 다르게 설정해서 하나의 공인 IP 주소로 외부와 통신가능  
(포트 번호로 각각의 host 들을 구분할 수 있기 때문에 외부와의 통신에 문제가 없다.)
- PAT는 Cisco IOS 설정에서는 Overload라고 한다.
- PAT는 여러개의 inside local ip address를 단지 하나 또는 몇 개의 inside global ip address에 포트 번호를 다르게해서 외부 네트워크와 통신을 한다.
- Router는 외부 IP 주소에 유일한 송신지 port 번호를 할당하기 때문에 내부 호스트 별 packet을 구분할 수 있다.



# PAT – Port Address Translation



# PAT – Port Address Translation

## 3) PAT(Port address translation) 설정

```
RouterX(config)# ip nat pool <name> <start-ip> <end-ip> netmask <subnet mask>
```

→ 공인 IP 그룹을 생성. **start-ip**와 **end-ip** 사이의 IP가 공인 IP 그룹이 된다.

```
RouterX(config)# access-list <list-number> permit <source> <wildcard mask>
```

→ 사설 IP 그룹을 생성. **ACL**로 사설 IP 그룹을 지정.

```
RouterX(config)# ip nat inside source list <list-number> pool <name> overload
```

→ 공인 IP 그룹과 사설 IP 그룹을 그룹 대 그룹으로 Mapping.

```
RouterX(config)#interface fastethernet 0/0  
RouterX(config-if)# ip nat inside
```

→ Fast ethernet 0/0을 NAT 내부 Interface로 지정

```
RouterX(config)#interface serial 0/1  
RouterX(config-if)# ip nat outside
```

→ Serial 0/1을 NAT 외부 Interface로 지정

# NAT – Network Address Translation

## 3) PAT 설정

- 내부 네트워크는 사설 IP 192.168.1.0/24 주소를 사용하고 외부와 통신을 할 경우는 191.15.100.1~191.15.100.10 사이의 공인 IP 주소로 변환돼서 정상적으로 통신이 가능하도록 NAT-PAT 설정을 하시오.

```
Router(config)#ip nat pool AA 191.15.100.1 191.15.100.10 netmask 255.255.255.0
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 10 pool AA overload
```

```
Router(config)#interface fastethernet 0/1
Router(config-if)#ip nat inside
```

```
Router(config)#interface serial 0/1
Router(config-if)#ip nat outside
```

# DHCP - Dynamic Host Configuration Protocol

## <DHCP - Dynamic Host Configuration Protocol>

- PC나 Host가 지정된 IP address를 갖는 것이 아니라 PC가 부팅되면 **DHCP Server**에게 **dynamic** 한 방식으로 IP 주소를 하나씩 받아오는 방식. (**동적 IP address 할당**)
- PC들은 부팅되면, **TCP/IP** 네트워크에 참여하기 위해서 자신이 사용해야 할 IP 주소 정보 (IP 주소, **Subnet mask**, 기본 **Gateway**, **DNS** 서버)를 찾는다.
- IP 주소 배정을 자동으로 하고 IP 주소 관리를 편하게 해준다.
- **DHCP**는 임대(**Lease**) 서비스이기 때문에 사용 기간을 설정할 수도 있다.
- **DHCP** 서버의 역할은 주로 전문 서버 장비들이 하지만 **Cisco**의 경우 **Router**도 이 기능을 지원.
- **UDP** 포트 **67**, **68** 사용 (**67**은 서버, **68**은 클라이언트)



# DHCP - Dynamic Host Configuration Protocol

## <DHCP 동작>

- 4단계 과정을 거쳐서 **Client**에게 **IP address**를 할당한다.

### 1) DHCP Discover

- **Client** → **Server**에게 '**Discover**' message 전송 (**IP 임대 요청 시작**)

출발지 포트 번호 : 68

목적지 포트 번호 : 67

출발지 IP 주소 : 0.0.0.0

목적지 IP 주소 : 255.255.255.255

- '**Discover**' message 를 수신한 서버는 IP 주소 중복을 방지하기 위해서 **ICMP Echo** 전송

### 2) DHCP Offer

- **Server** → **Client**에게 '**Offer**' message 전송 (**IP 임대 응답**)

출발지 포트 번호 : 67

목적지 포트 번호 : 68

출발지 IP 주소 : **DHCP** 서버

목적지 IP 주소 : 255.255.255.255

# DHCP - Dynamic Host Configuration Protocol

## <DHCP 동작>

### 3) DHCP Request

- Client → Server에게 'Request' message 전송 (IP 임대 최종 요청)

출발지 포트 번호 : 68

목적지 포트 번호 : 67

출발지 IP 주소 : 0.0.0.0

목적지 IP 주소 : 255.255.255.255

### 4) DHCP Ack

- Server → Client에게 'Ack' message 전송 (IP 임대)

출발지 포트 번호 : 67

목적지 포트 번호 : 68

출발지 IP 주소 : DHCP 서버1

목적지 IP 주소 : 255.255.255.255

# DHCP - Dynamic Host Configuration Protocol

## <DHCP 설정>

**Router(config)#service dhcp**

→ DHCP 서버로 사용 가능하게 하겠다는 선언 (default)

**Router(config)#ip dhcp pool cisco**

→ DHCP로 사용된 주소의 pool(영역) 지정.

**Router(dhcp-config)#network 192.168.0.0 255.255.255.0**

→ DHCP로 할당할 IP address 대역을 지정

**Router(dhcp-config)#default-router 192.168.0.254**

→ 호스트가 내부에서 목적지를 찾지 못했을 때 갈 수 있는 Router의 Ethernet 인터페이스의 IP 주소

**Router(dhcp-config)#exit**

**Router(config)#ip dhcp excluded-address 192.168.0.254**

→ DHCP로 할당할 IP address 중 할당하지 말아야 할 IP address 지정.

즉, DHCP pool에서 제외시켜줄 IP를 지정한다.

(지금은 192.168.0.254가 Router의 Ethernet 인터페이스 IP로 사용되기 때문에 제외.)

# DHCP - Dynamic Host Configuration Protocol

## <DHCP 설정>

### - 추가 설정 -

**Router(config)#ip dhcp pool cisco**

→ DHCP로 사용된 주소의 pool(영역) 지정.

**Router(dhcp-config)#dns-server x.x.x.x**

→ DNS 서버를 지정한다. (x.x.x.x는 DNS서버의 IP주소)

**Router(dhcp-config)#domain-name cisco.com**

→ domain-name을 설정 (cisco.com은 임의로 사용했음)

**Router(dhcp-config)#lease infinite**

→ 배정시간(lease time) 지정, 즉 IP를 얼마 동안 할당하겠다는 의미.

(infinite는 무한정으로 할당하겠다는 의미. infinite 대신 <0 - 365> 입력 가능 (단위는 Days))

- ‘show ip dhcp binding’와 ‘show ip dhcp server statistics’ 명령어로 확인 가능.