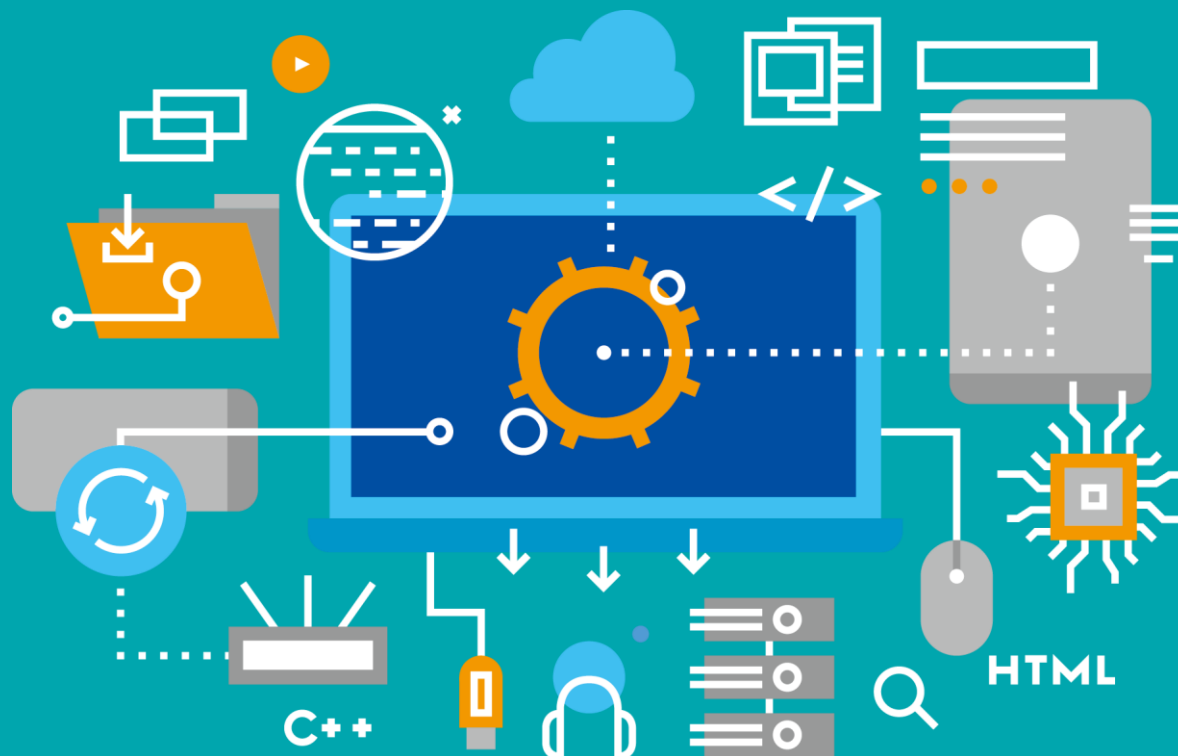


DMMU

# 동양미래대학교 전문기술 석사과정

클라우드와 네트워크 보안

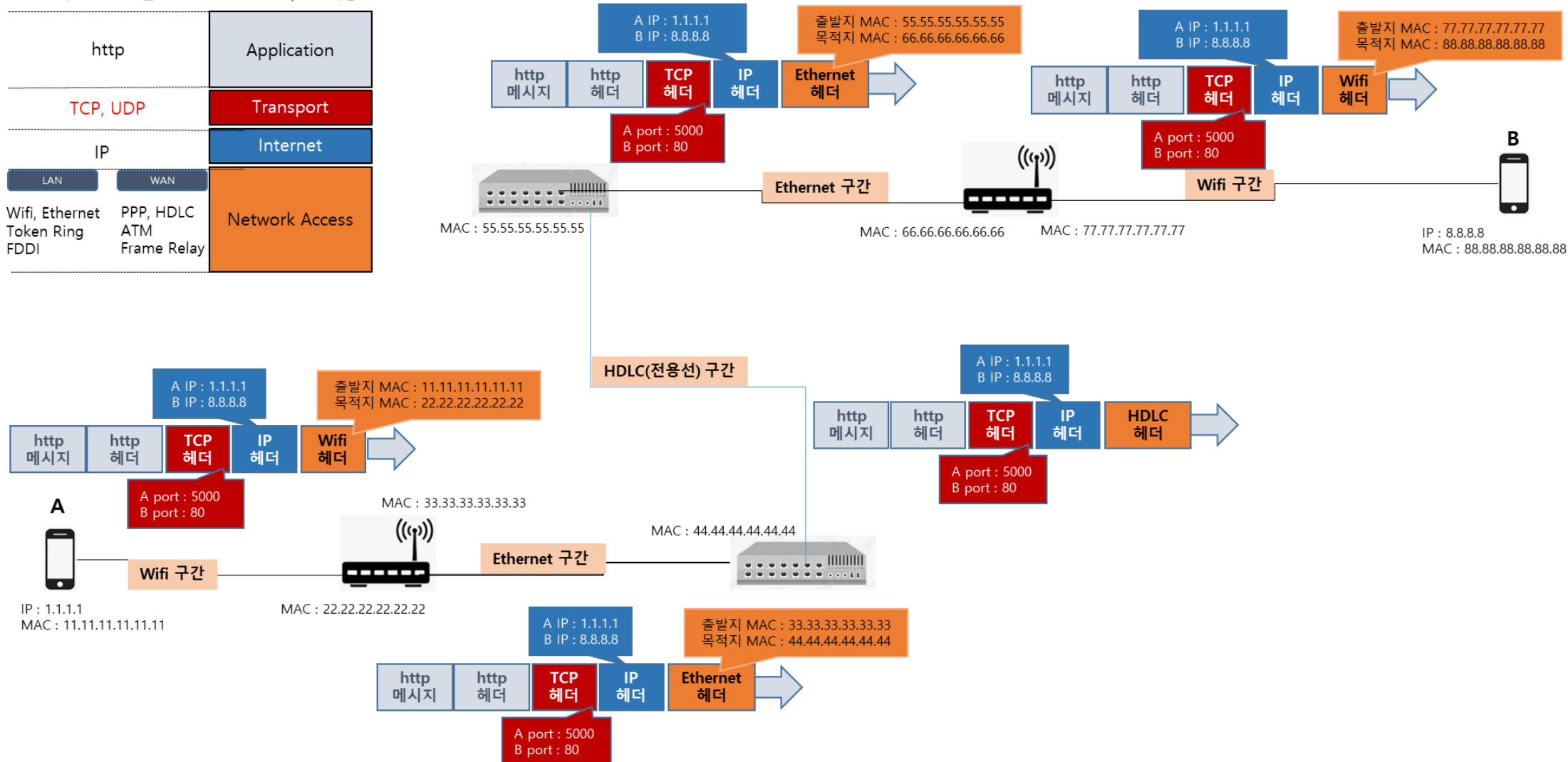
Dongyang Mirae University

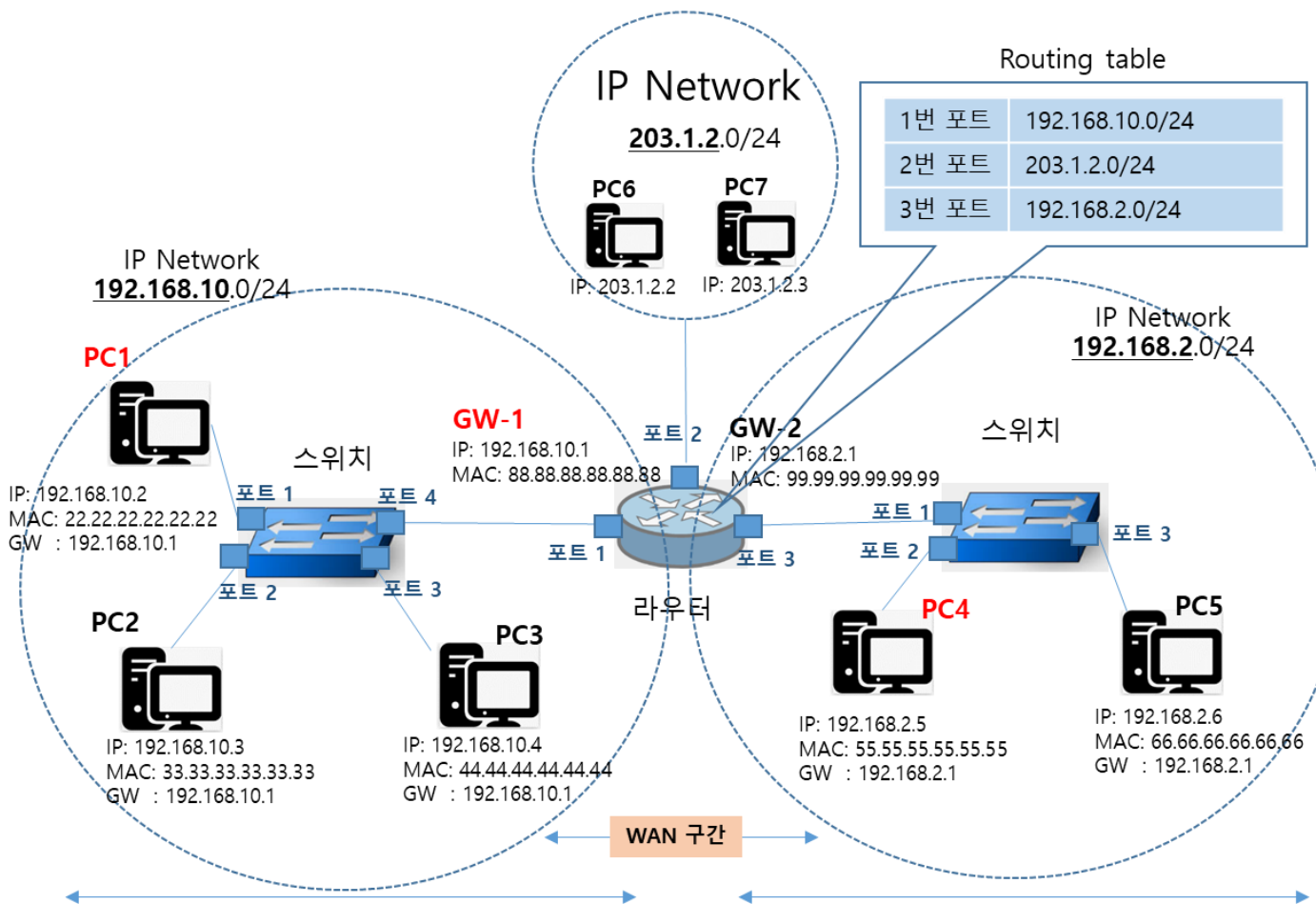


주요 프로토콜

TCP/IP 4 계층

http	Application
TCP, UDP	Transport
IP	Internet
LAN Wifi, Ethernet Token Ring FDDI	WAN PPP, HDLC ATM Frame Relay
Network Access	





PC1(192.168.10.2/24)이 PC4(192.168.2.5/24)로 데이터 전송

(PC1 -> GW-1/port1)

- PC4는 PC1과 다른 네트워크이므로 PC1은 데이터를 GW로 전송함



(GW-1/port1 -> GW-2/port3)

- Routing table에서 도착지(192.168.2.5/24)로 가기 위해서는 3번 포트  
로 전송

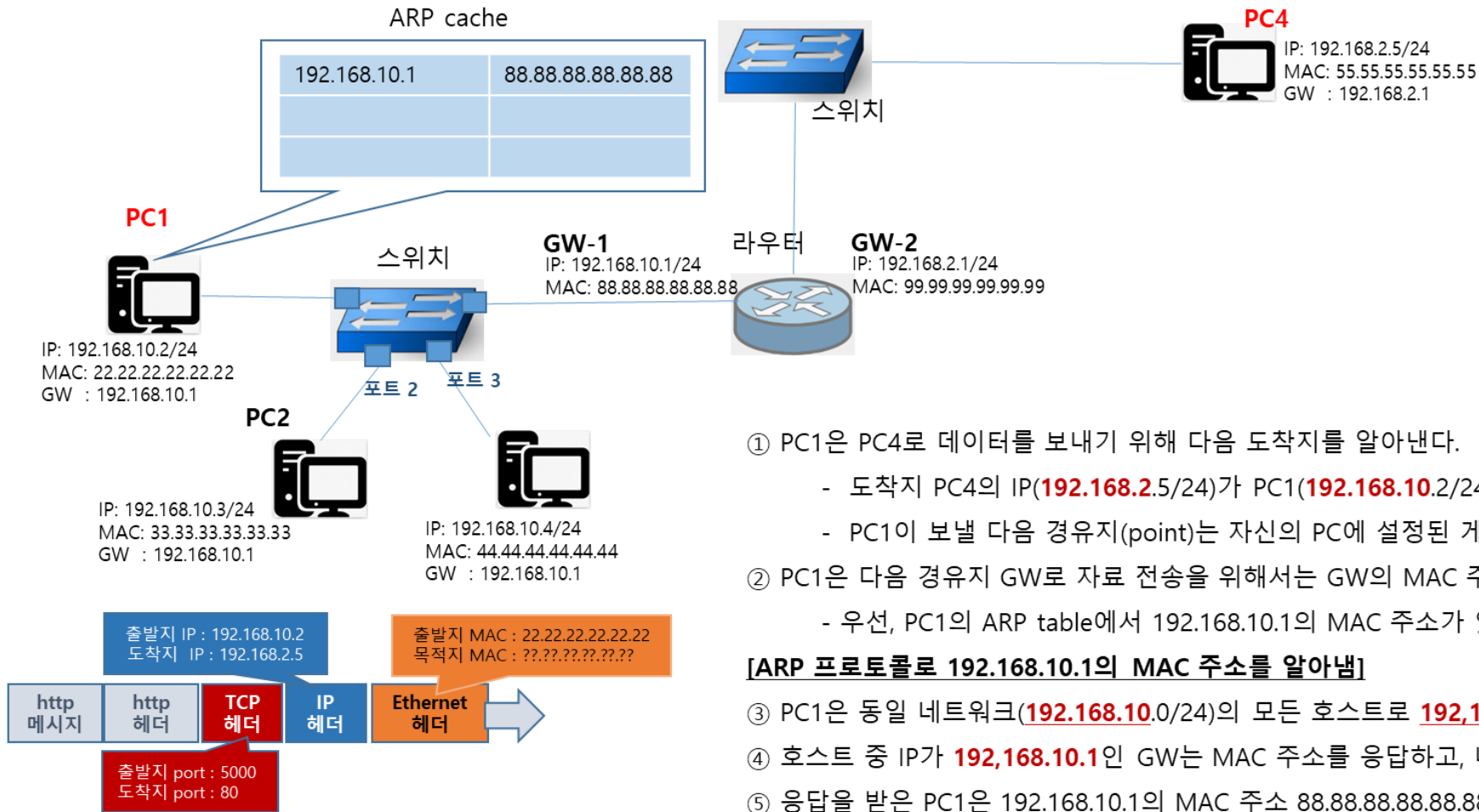


(GW-2/port3 -> PC4)

- GW-2에서 PC4로 데이터를 전송함



ARP - IP 주소로 부터 MAC 주소를 알아내는 프로토콜

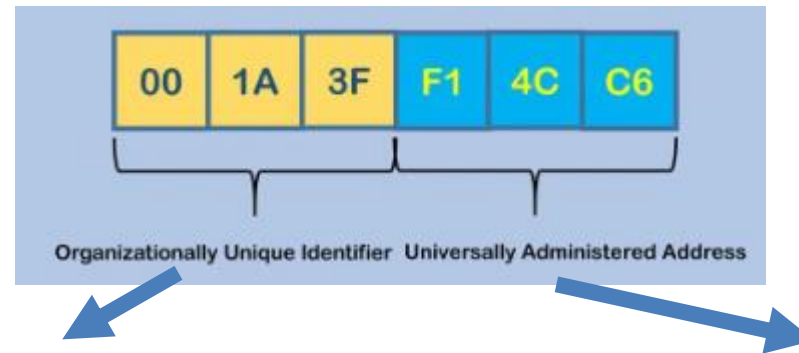


## 1.2 MAC (Media Access Control) 주소

- MAC 주소 : 2계층에서 통신을 위해 네트워크 인터페이스에 할당한 고유 식별자
- 네트워크에 접속하는 모든 장비는 MAC 주소가 있어야 하고, 이 주소로 통신
- 이더넷, 와이파이를 포함한 IEEE802 네트워크 기술에서 MAC을 2계층 주소로 사용

## 1.2 MAC (Media Access Control) 주소

### 1.2.1 MAC 주소 체계



OUI:

IEEE가 제조사에 할당하는 부분

UAA:

각 제조사에서 네트워크 구성 요소에 할당하는 부분

- **BIA(Burned-In-Address)** : 네트워크 카드나 장비 생산할 때 하드웨어적으로 정해져 나옴
- **유일하지 않은 MAC 주소** : 제조 업체에서 실수로 UAA를 중복할당 / 동일 네트워크에서만 중복되지 않으면 문제 없음
- **MAC 주소 변경** : NIC에 ROM에 고정되어 출하됨. 그러나 MAC 주소도 메모리에 적재하여 구동하므로 변경도 가능

MAC address

1C-1B-DD

77-90-4C

OUI(Organizational Unique Identifier)

네트워크카드 제작 회사 번호

회사별

네트워크카드 일련번호

```
Windows PowerShell
PS C:\Users\성석용> ipconfig /all

Windows IP 구성

호스트 이름 . . . . . : DESKTOP-0039KJQ
주요 DNS 접미사 . . . . . : 
IPv6 주소 . . . . . : 
IP 라우팅 사용 . . . . . : 아니요
WINS 프록시 사용 . . . . . : 아니요

이더넷 어댑터 이더넷:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . : 
물리적 주소 . . . . . : Realtek PCIe GbE Family Controller
E8-03-9A-00-8C-FC
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예

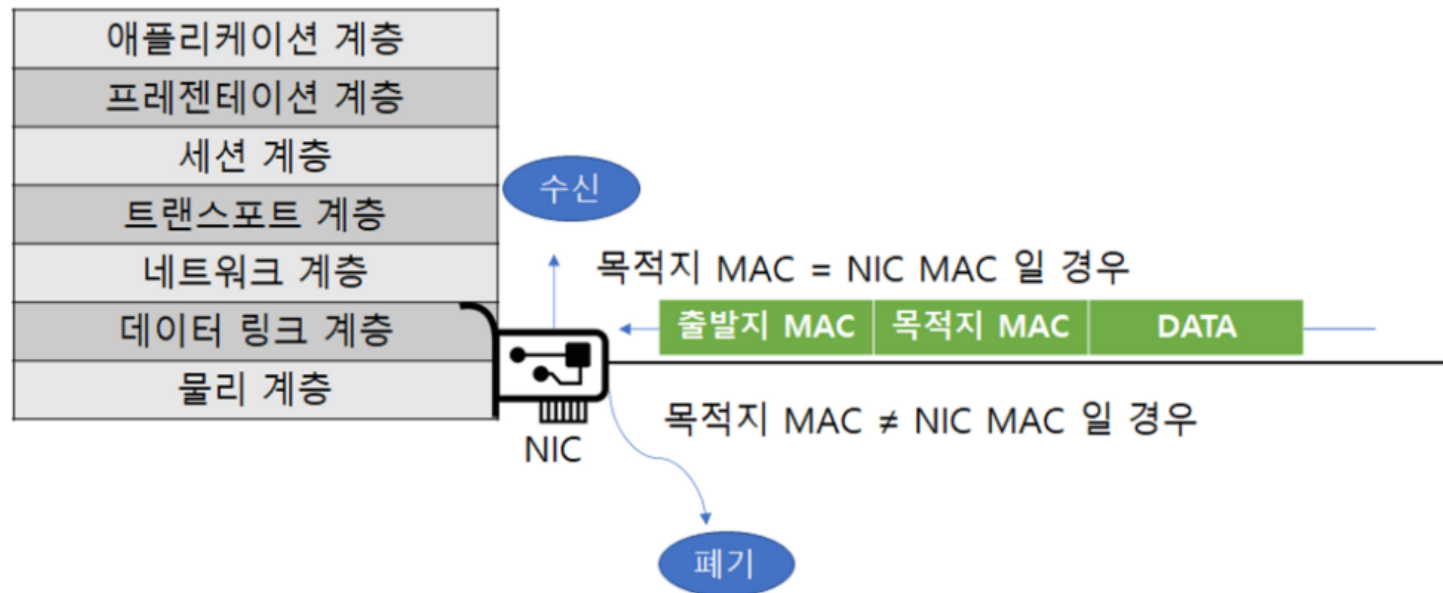
이더넷 어댑터 VirtualBox Host-Only Network:

연결별 DNS 접미사 . . . . . : 
물리적 주소 . . . . . : VirtualBox Host-Only Ethernet Adapter
0A-00-27-00-00-02
DHCP 사용 . . . . . : 아니요
자동 구성 사용 . . . . . : 예
링크-local IPv6 주소 . . . . . : fe80::182b:9454:4f0e:260a%2(기본 설정)
IPv4 주소 . . . . . : 192.168.56.1(기본 설정)
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . : 
DHCPv6 IAID . . . . . : 285868071
DHCPv6 클라이언트 DUID . . . . . : 00-01-00-01-22-5F-4F-54-E8-03-9A-00-8C-FC
DNS 서버 . . . . . : fec0::0:ffff::1%1
fec0::0:ffff::2%1
fec0::0:ffff::3%1
Tcpip를 통한 NetBIOS . . . . . : 사용
```

ipconfig /all

## 1.2 MAC (Media Access Control) 주소

### 1.2.2 MAC 주소 동작



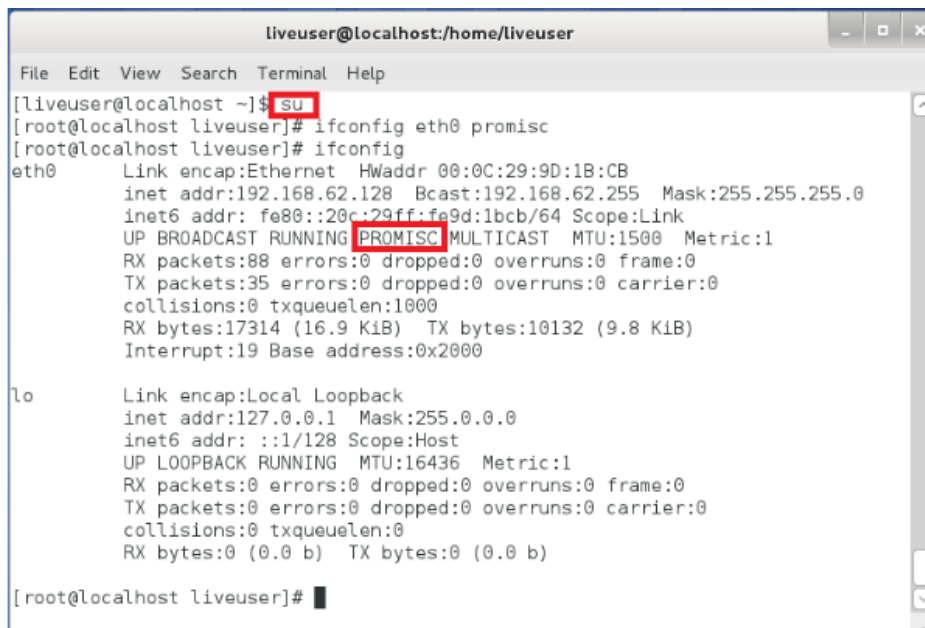
- NIC는 2계층에서 전기신호를 패킷으로 변화하고 도착지 MAC 주소를 확인
- 도착지 MAC 주소가 **자신의 MAC 주소**이거나 **그룹 주소(브로드캐스트, 멀티캐스트)**이면 패킷을 **상위 계층으로 전달**
- 그 밖에, 자신의 MAC 주소와 일치하지 않으면 수신 패킷을 자체 폐기 (폐기 하는데 시스템의 부하 발생)



## 1.2 MAC (Media Access Control) 주소

### 1.2.2 MAC 주소 동작 / 무차별 모드 (Promiscuous Mode)

- 자신의 MAC 주소와 무관하게 모든 패킷을 수신하여 상위 계층으로 전송
- 네트워크 상의 패킷을 수집하여 분석해야 하는 경우 사용
- 네트워크 패킷 분석 애플리케이션 Wireshark : 무차별 모드를 사용하는 대표적 프로그램



```
liveuser@localhost:/home/liveuser
File Edit View Search Terminal Help
[liveuser@localhost ~]$ su
[root@localhost liveuser]# ifconfig eth0 promisc
[root@localhost liveuser]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:9D:1B:CB
          inet addr:192.168.62.128  Bcast:192.168.62.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9d:1bcb/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:88 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17314 (16.9 KiB)  TX bytes:10132 (9.8 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@localhost liveuser]#
```

➤ Ifconfig eth0 promisc

➤ Ifconfig eth0 -promisc

윈도우에서는 별도의 드라이버 등을 설치해야 함

## 1.2 MAC (Media Access Control) 주소

### 1.2.2 MAC 주소 동작 / 여러 MAC 주소 갖는 경우, MAC 주소로 제조업체 찾기

- 단말이 여러 개의 NIC를 가지는 경우, 단말은 여러 개의 MAC 주소를 갖을 수 있음
  - MAC 주소는 단말에 종속되지 않고, NIC에 종속됨
- MAC 주소로 제조사 정보 확인 가능
  - <https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries>
  - [bit.ly/ieee\\_list](https://bit.ly/ieee_list)

The screenshot shows the IEEE Registration Authority website. The main heading is "IEEE Registration Authority: Assignments". Below this, there are links for "SIGN IN" and "CREATE ACCOUNT". A search bar is present with the text "Search the public listing to determine whether your organization has already been issued an assignment". The search results section is titled "ALL MAC (MA-L, MA-M, MA-S) SEARCH RESULTS" and shows a table of results. The table has columns for "Assignment", "Assignment Type", "Company Name", and "Company Address". The first row shows an assignment of "84-11-C2" to "MA-M" for "FUJIFILM Healthcare Corporation". The second row shows an assignment of "300000-3FFFF" to "MA-S" for "Fuzhou Tucsen Photonics Co., Ltd". The third row shows an assignment of "BC1F-64" to "MA-S" for "Fuzhou Tucsen Photonics Co., Ltd". The fourth row shows an assignment of "45D000-45DFFF" to "MA-S" for "Fuzhou Tucsen Photonics Co., Ltd". The table is paginated, showing "Showing 1 - 10 of 47551". On the right side, there is a "DOWNLOAD" section with a list of links for downloading the entire public listing for a registry, including "1. MAC Address Block Large (MA-L)", "2. MAC Address Block Medium (MA-M)", "3. MAC Address Block Small (MA-S)", "4. Company ID", "5. Ethernets", "6. Manufacturer ID", "7. IEEE 802.16 Operator ID", and "8. IAB".

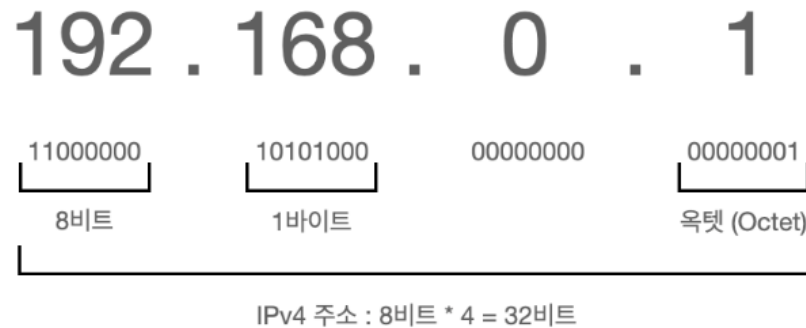
Assignment	Assignment Type	Company Name	Company Address
84-11-C2 (hex)	MA-M	FUJIFILM Healthcare Corporation	2-1, Shintoyofuta Kashiwa-shi Chiba 277-0804 JP
300000-3FFFF	MA-S	Fuzhou Tucsen Photonics Co., Ltd	5# Wanwushe Smart Industrial Park, No.2 Yangsi Branch Rd, Gaishan Town, Gangshan Area, Fuzhou, Fujian PRC
BC1F-64 (hex)	MA-S	Fuzhou Tucsen Photonics Co., Ltd	5# Wanwushe Smart Industrial Park, No.2 Yangsi Branch Rd, Gaishan Town, Gangshan Area, Fuzhou, Fujian PRC
45D000-45DFFF	MA-S	Fuzhou Tucsen Photonics Co., Ltd	5# Wanwushe Smart Industrial Park, No.2 Yangsi Branch Rd, Gaishan Town, Gangshan Area, Fuzhou, Fujian PRC

## 1.3 IP 주소

- 사용자가 변경이 가능한 논리 주소
- 주소에 레벨이 있음 (그룹을 의미하는 네트워크 주소 / 호스트 주소)

## 1.3 IP 주소

### 1.3.1 IP 주소 체계



- IP 주소는 두 부분으로 나뉨

- 네트워크 주소 :

- ❖ 호스트를 모은 네트워크를 지칭하는 주소
- ❖ 네트워크 주소가 동일한 네트워크를 **로컬 네트워크**라도 함

- 호스트 주소 :

- ❖ 하나의 네트워크에 존재하는 호스트를 구분하기 위한 주소

## 1.3 IP 주소

### 1.3.2 클래스풀(Classful) 과 클래스리스(Classless) – 클래스리스 네트워크의 등장

- 클래스풀(Classful) :
  - 클래스 기반의 IP 주소 체계
  - 서브넷마스크(네트워크 주소와 호스트 주소를 구분하는 구분자)가 필요 없음
  - 맨 앞자리로 클래스 구분 가능( A class : 0, B class : 10, C class : 110 )
  - 클래스를 기관에 할당하면, 비여있는 주소라도 다른 기관이 사용할 수 없음 (비효율성)
- IP 주소 부족과 낭비 문제 해결 방안
  - (단기 대책) **CIDR (Classless Inter-Domain Routing)** 기반 주소체계
  - (중기 대책) NAT와 사설 IP 주소
  - (장기 대책) IPv6 주소 체계

## 1.3 IP 주소

### 1.3.3 서브네팅 (Subnetting) - 네트워크 사용자 입장 (IP 범위 파악)

 cidr 계산기

 **IPv4 / IPv6 CIDR 계산기**  
IPv4, IPv6 CIDR 주소를 기반으로 IP 주소 범위 계산

검색

계산하다

첫 번째 IP 주소	103.9.32.128
마지막 IP 주소	103.9.32.191
IP 수	64
서브넷 범위	255.255.255.192
와일드 카드	0.0.0.63

네트워크 주소 : 103.9.32.128 / 첫번째 주소 : 103.9.32.129 / 마지막 주소 : 103.9.32.190 / 브로드캐스트 주소 : 103.9.32.191

## 1.3 IP 주소

### 1.3.3 서브네팅 (Subnetting) - 네트워크 설계자 입장 (네트워크에 수용 가능한 단말 수)

- 서브넛된 하나의 네트워크에 몇 개의 IP를 할당해야 하나 ?
- 서브넛된 네트워크가 몇 개나 필요한가 ?

- 회사에 12개의 지사가 있음
- 각 지사는 최대 12개의 IP가 필요한 단말이 있음 (PC, 복합기, IP 카메라 등)
- 현재 할당된(보유한) 네트워크는 103.9.32.0/24

- IP 주소 변환( 103.9.32.0/24 ) : 01100111.00001001.00100000.00000000/24

- 12개 네트워크로 쪼갬 : 01100111.00001001.00100000.00000000/28

1번 네트워크 : 01100111.00001001.00100000.00000000/28 103.9.32.0/28

2번 네트워크 : 01100111.00001001.00100000.00010000/28 103.9.32.16/28

3번 네트워크 : 01100111.00001001.00100000.00110000/28 103.9.32.32/28

....

16번 네트워크 : 01100111.00001001.00100000.11110000/28 103.9.32.240/28

## 1.3 IP 주소

### 1.3.3 서브네팅 (Subnetting) - 네트워크 설계자 입장 (네트워크에 수용 가능한 단말 수)

- 회사에 12개의 지사가 있음
- 각 지사는 최대 12개의 IP가 필요한 단말이 있음 (PC, 복합기, IP 카메라 등)
- 현재 할당된(보유한) 네트워크는 103.9.32.0/24



- IP 주소 2진수 변환( 103.9.32.0/24 ) : 01100111.00001001.00100000.00000000/24
- 12개 네트워크로 쪼갬(4비트 필요) : 01100111.00001001.00100000.**0000**0000/28

(16개 네트워크로 쪼개는 것이 가능)

1번 네트워크 :	01100111.00001001.00100000. <b>0000</b> 0000/28	103.9.32.0/28
2번 네트워크 :	01100111.00001001.00100000. <b>0001</b> 0000/28	103.9.32.16/28
3번 네트워크 :	01100111.00001001.00100000. <b>0011</b> 0000/28	103.9.32.32/28
....		
16번 네트워크 :	01100111.00001001.00100000. <b>1111</b> 0000/28	103.9.32.240/28



## 1.3 IP 주소

### 1.3.3 서브네팅 (Subnetting) - 네트워크 설계자 입장 (네트워크에 수용 가능한 단말 수)

1번 네트워크 : 01100111.00001001.00100000.00000000/28      103.9.32.0/28

IP 범위 : 103.9.32.0 ~ 103.9.32.15 / 네트워크 주소 : 103.9.32.0 / 브로드캐스트 103.9.32.15

2번 네트워크 : 01100111.00001001.00100000.00010000/28      103.9.32.16/28

IP 범위 : 103.9.32.16 ~ 103.9.32.31 / 네트워크 주소 : 103.9.32.16 / 브로드캐스트 103.9.32.31

3번 네트워크 : 01100111.00001001.00100000.00110000/28      103.9.32.32/28

....

16번 네트워크 : 01100111.00001001.00100000.11110000/28      103.9.32.240/28

IP 범위 : 103.9.32.240 ~ 103.9.32.255 / 네트워크 주소 : 103.9.32.240 / 브로드캐스트 103.9.32.255

IPv4 / IPv6 CIDR 계산기  
IPv4, IPv6 CIDR 주소를 기반으로 IP 주소 범위 계산

103.9.32.240 /28

계산하다

첫 번째 IP 주소	103.9.32.240
마지막 IP 주소	103.9.32.255
IP 수	16
서브넷 범위	255.255.255.240
와일드 카드	0.0.0.15

## 1.3 IP 주소

### 1.3.4 공인 IP와 사설 IP

- 공인 IP : 인터넷에 접속하기 위해 필요한 전세계에서 유일한 식별자
  - 통신사업자, IP 할당 기관(KISA 등)에서 독립 IP를 할당 받아 사용
- 사설 IP : 인터넷에 연결하지 않고 개인적으로 네트워크를 구성하는 경우 사용하는 IP 주소
  - 인터넷에 연결하지 않거나 NAT 기술(공유기나 방화벽 장비)을 사용하는 경우

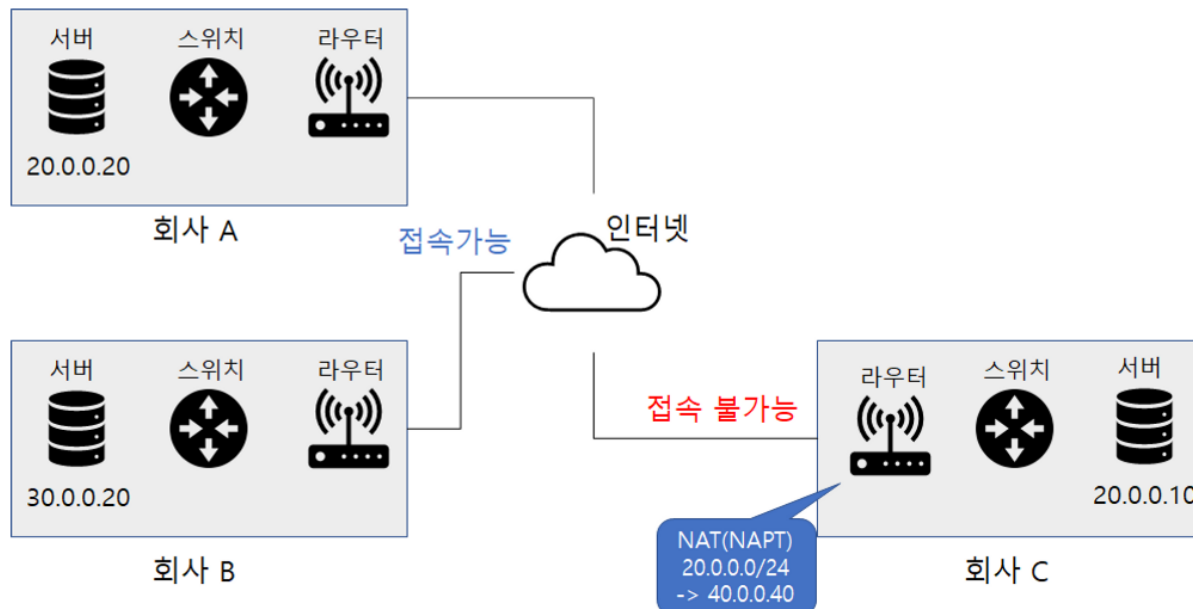
네트워크 주소	IP 범위	클래스 크기
10.0.0.0/8	10.0.0.0 ~ 10.255.255.255	A Class 1개
172.16.0.0/12	172.16.0.0~172.31.255.255	B Class 16개
192.168.0.0/16	192.168.0.0~192.168.255.255	C Class 256개

클래스별 사설 IP 주소

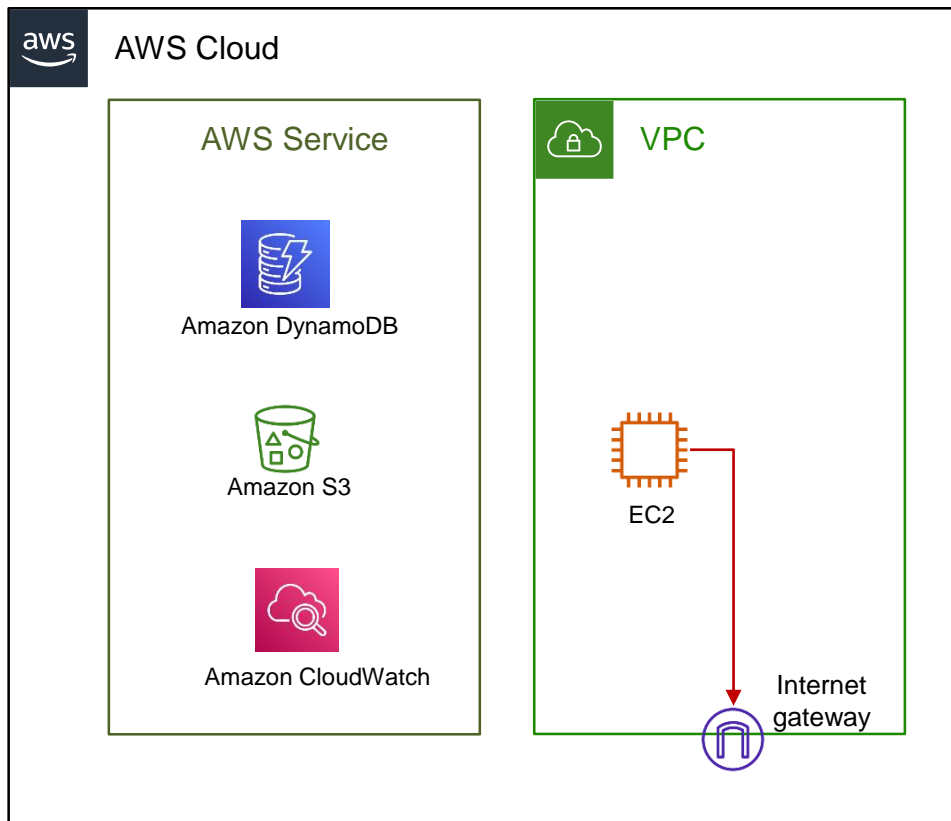
## 1.3 IP 주소

### 1.3.4 공인 IP와 사설 IP

- 다른 기관에서 사용하는 공인 IP를 회사 내부에서 사용하는 경우에도 접속이 불가능함
- 회사 C는 회사 A사 사용하는 공인 IP(20.0.0.0/24) 대역 IP를 사설 IP로 사용하고 있음
- **C사 서버(20.0.0.10)가 라우터(NAT 기능 보유)를 통해 A사 서버(20.0.0.20)에 접속하려고 하는 경우**
- C사 라우터는 발신지(**20.0.0.10/24**)와 목적지(**20.0.0.20/24**)가 동일한 네트워크로 인식
- C사 라우터는 패킷을 브로드 캐스트 한다. **통신 불가**



## ※ VPC (Virtual Private Cloud)

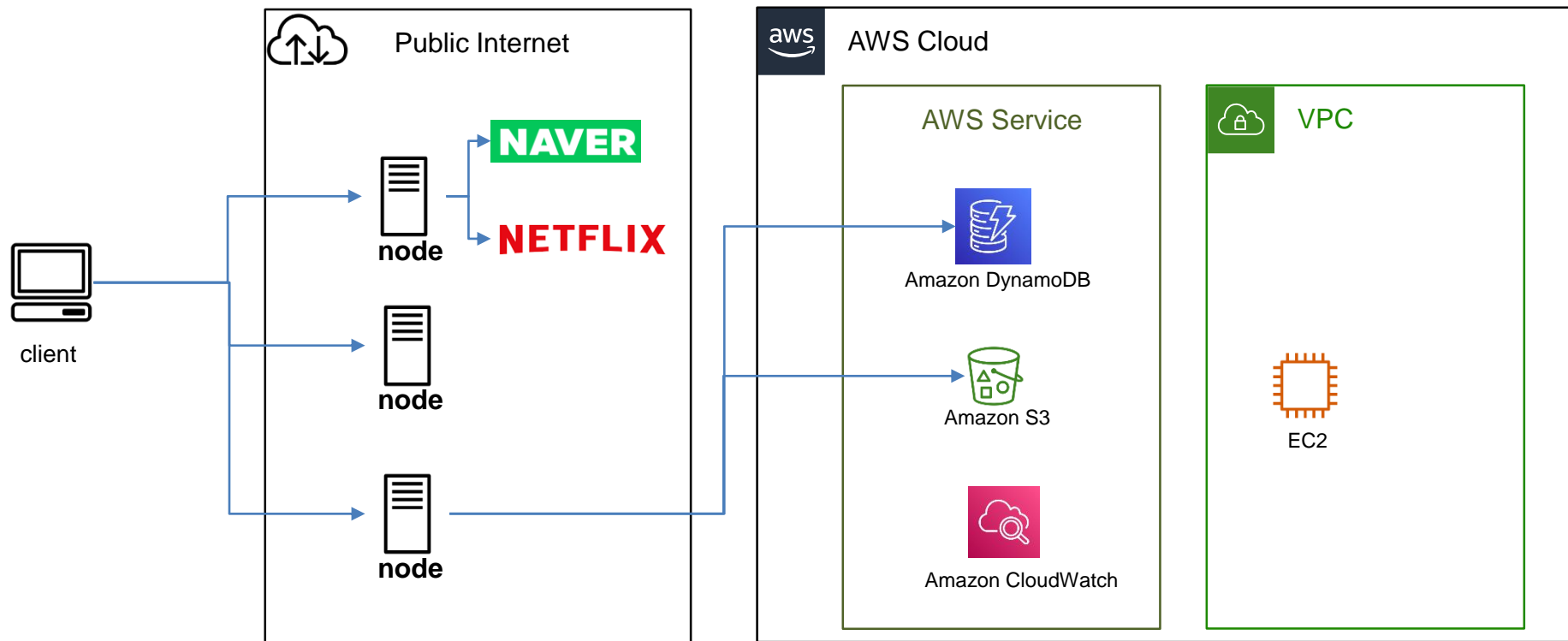


### VPC : 논리적으로 분리된 가상의 데이터 센터

- EC2, RDS, Lambda 등의 AWS 컴퓨팅 서비스 실행
- 다양한 서브넷 구성
- 보안 설정(NACL)

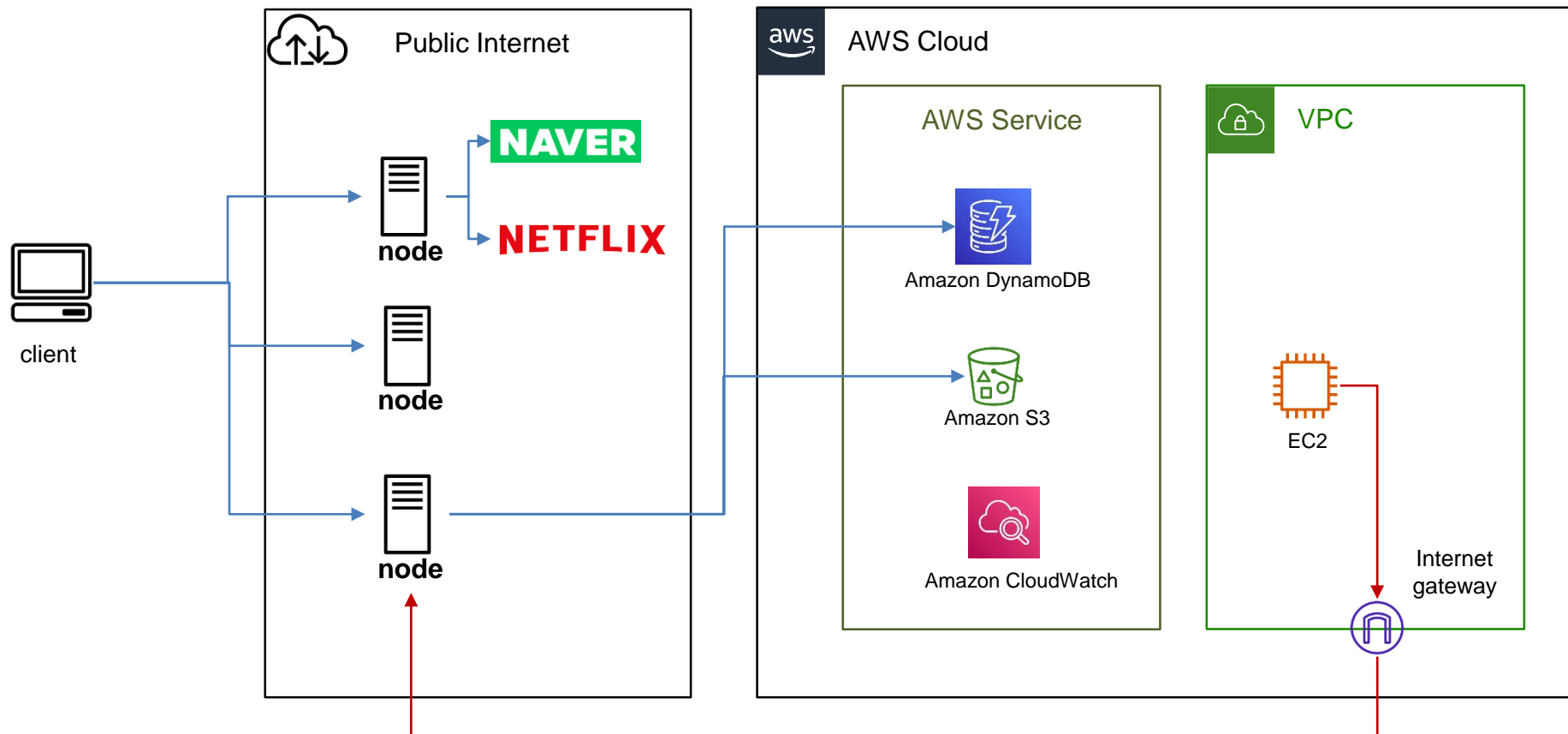
- 외부와 격리된 AWS 계정 전용 가상 네트워크
- 다른 가상 네트워크와 **논리적으로 분리되어** 있음
- AWS 리소스(EC2, RDS, Lambda 등)를 VPC에서 실행 가능
- 부여된 IP 대역을 분할한 **서브넷을** 구성하여 **사용 가능**
- **리전(Region) 단위** 구성

## ※ AWS 구조 – VPC (Virtual Private Cloud)



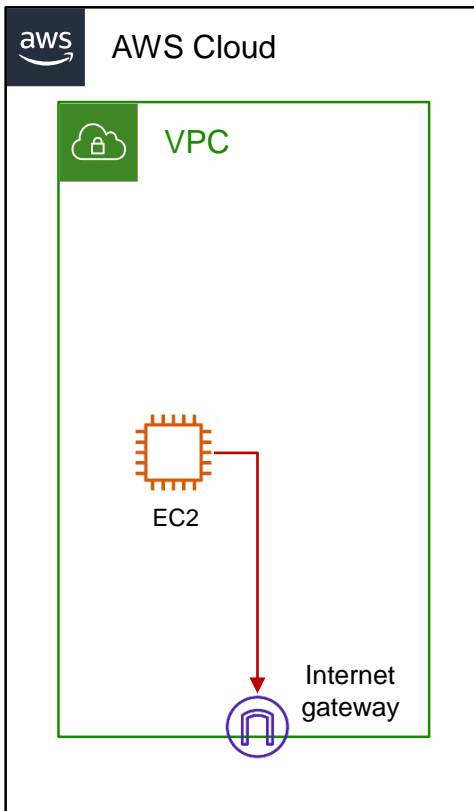
- Public Internet을 통해 회사 AWS Service에 접근하여 사용 가능
- VPC : 외부와 격리된 네트워크
  - AWS Cloud VPC는 (원칙적으로) 외부에서 접근 불가

## ※ AWS 구조 - VPC (Virtual Private Cloud)



- VPC내 EC2에서 AWS service를 사용하기 위해서는 (원칙적으로) Public Internet을 통해 접근

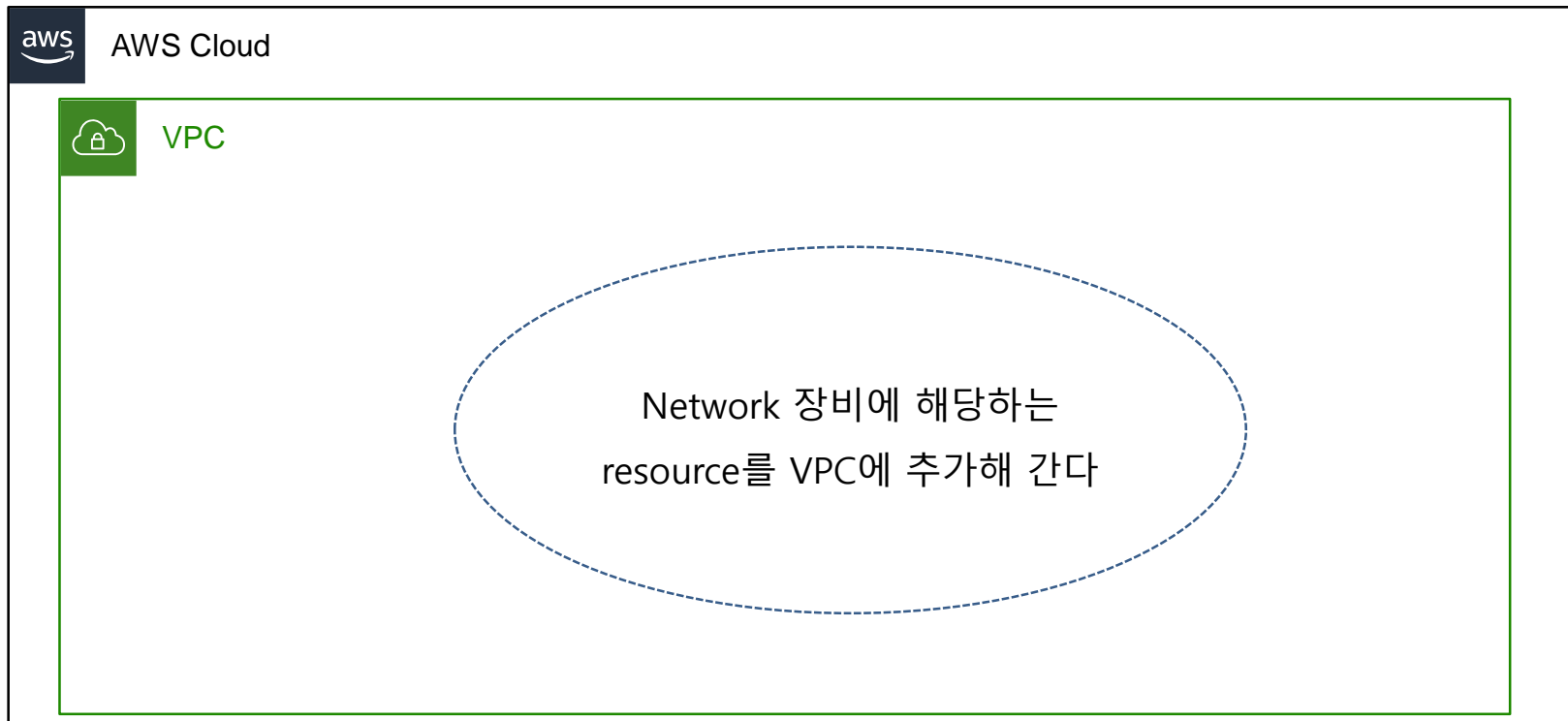
## ※ AWS 구조 - VPC (Virtual Private Cloud)



### VPC 기능

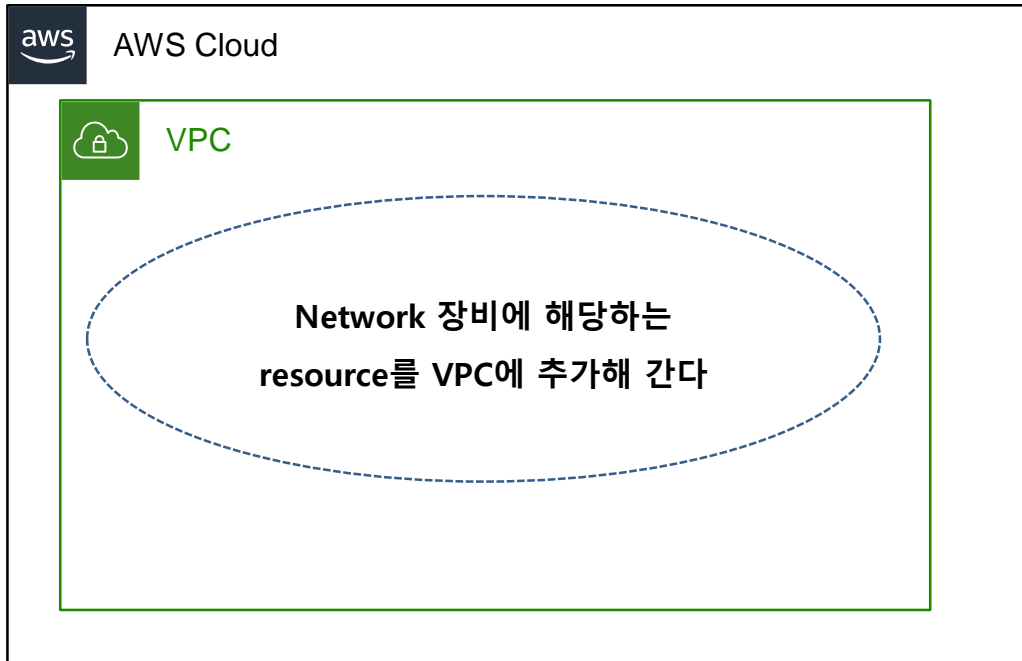
- **VPC** : VPC를 생성한 후 서브넷을 추가할 수 있음
- **Subnet** : VPC를 IP 주소 범위로 분할. subnet 추가 후 AWS 리소스 배포
- **IP 주소 지정** : CIDR 방식으로 VPC와 subnet에 IP 주소 할당
- **라우팅** : 라우팅 테이블을 사용하여 네트워크 트래픽이 전달되는 위치를 결정
- **인터넷 게이트웨이** : VPC를 인터넷에 연결
- **엔드포인트** : 인터넷 게이트웨이 또는 NAT 장치를 사용하지 않고 AWS 서비스에 비공개로 연결
- **피어링 연결** : 두 VPC의 리소스 간 트래픽을 라우팅

## ※ AWS 구조 - VPC (Virtual Private Cloud)





## ※ AWS 구조 - VPC에 할당되는 IP 주소 범위



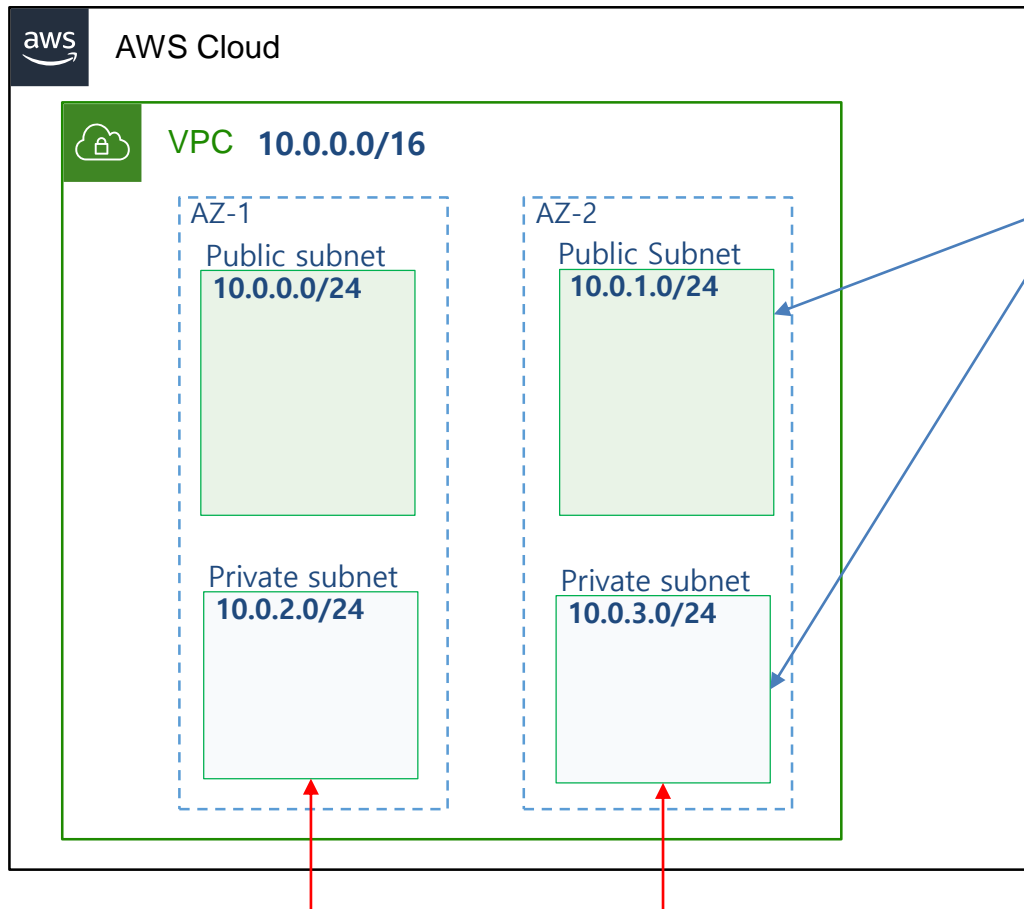
### VPC에 할당되는 IP 주소 범위

- 24bit 블록 : 10.0.0.0 ~ 10.255.255.255
- 20bit 블록 : 172.16.0.0 ~ 172.31.255.255
- 16bit 블록 : 192.168.0.0 ~ 192.168.255.255

※ 실제 VPC로 지정하여 사용할 수 있는 IP 주소 범위는 최대 16bit 블록까지 사용 가능

VPC CIDR 허용된 블록 크기 : /16 ~ /28

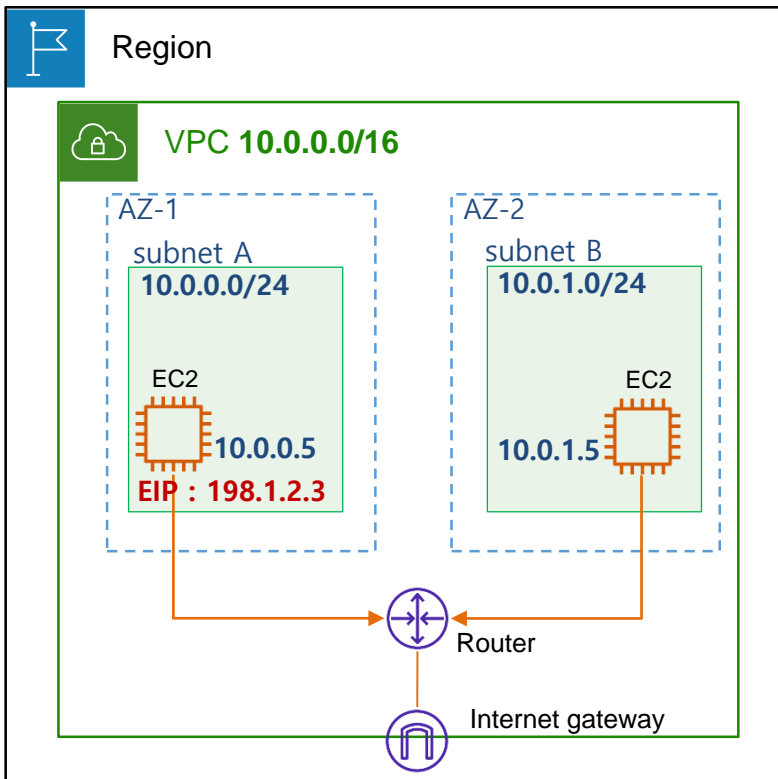
## ※ AWS 구조 - VPC에 Subnet 생성



### VPC에 Subnet을 만들어 사용하는 이유

- 역할 분리 : 외부에 공개하는 리소스 여부 구별  
(예) Private Subnet / Public Subnet
- 기기분리 : 2개 이상의 가용영역에 다중화(내결함성)  
(예) Private Subnet을 AZ1과 AZ2에 위치시킴

## ※ AWS 구조 - VPC (Virtual Private Cloud)

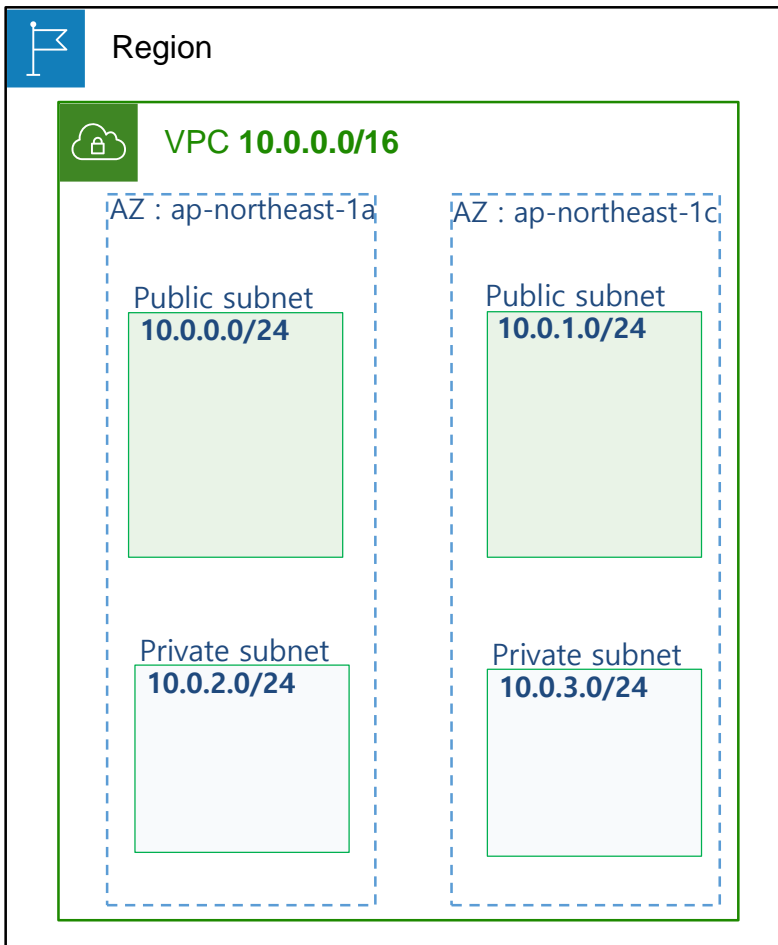


### VPC - Subnet

- VPC의 하위 단위로 VPC에 할당된 IP를 더 작은 단위로 분할
- 하나의 서브넷은 **하나의 가용영역(AZ)에 위치**
- **CIDR block range로 IP 주소 지정**

※ subnet 생성시 퍼블릭 IPv4 주소 자동 할당(Enable auto-assign public IPv4 address) 을 활성화 하면, 선택된 서브넷에서 시작된 모든 인스턴스에 **공인 IPv4 주소도 함께 할당** (인스턴스 재 시작시 새로운 공인 IP 할당)  
※ 변경되지 않는 공인 IP를 위해서는 EIP(Elastic IP)를 할당받아 사용해야 함

## ※ AWS 구조 - VPC (Virtual Private Cloud)



### VPC - Subnet

VPC 10.0.0.0/16

#### Subnet CIDR 설계 방법의 예

Subnet의 CIDR 블록	Subnet 수	리소스 수	비고
00001010.00000000.XXXXXXXXXX.YYYYYYYY	256	251	24bit subnet mask
00001010.00000000.XXXXYYYY.YYYYYYYY	16	4091	20bit subnet mask
00001010.00000000.XXYYYYYY.YYYYYYYY	4	16379	18bit subnet mask

※ AAA : VPC / XXXX : subnet / YYYY : 리소스

※ 서브넷에서 리소스 수는 이론적 최댓값에서 AWS가 예약한 5개를 뺀 값

※ 서브넷을 한 번 만들면 서브넷이 사용하는 CIDR 블록을 변경할 수 없음

## ※ AWS에서 서브넷의 IP 대역 마다 예약된 주소



172.16.0.0 / 16

- |                         |                               |
|-------------------------|-------------------------------|
| • 첫번째 주소 (네트워크 주소)      | : 172.16.0.0                  |
| • 마지막 주소 (Broadcast 주소) | : 172.16.255.255              |
| • 유효 IP 주소              | : 172.16.0.1 ~ 172.16.255.254 |

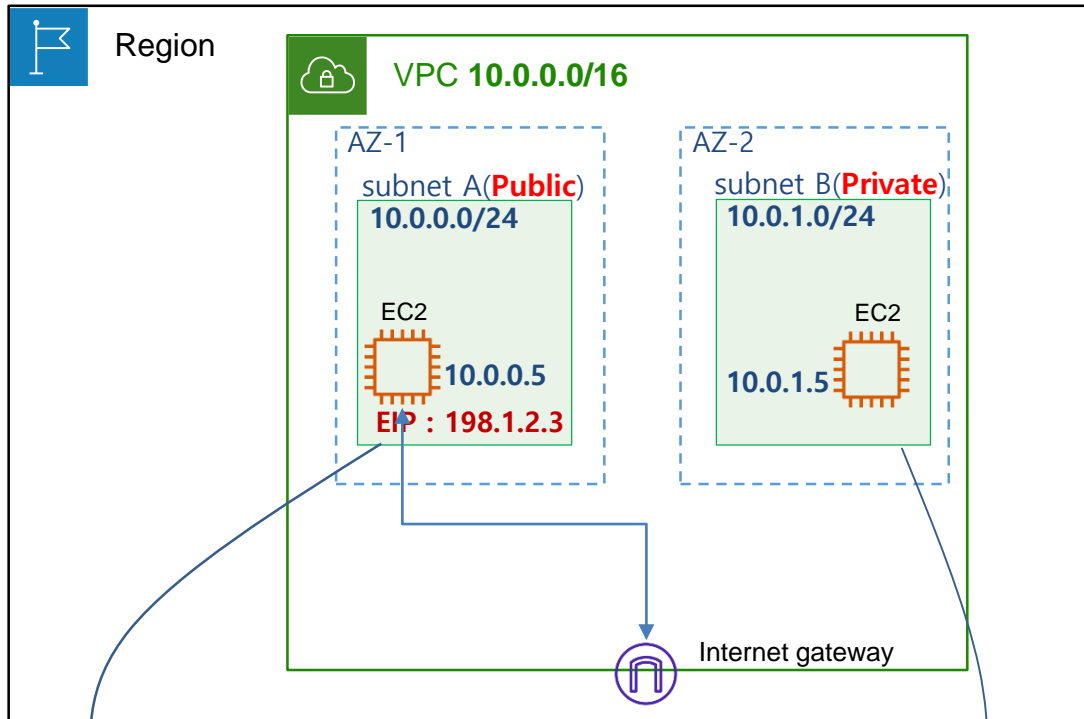


172.16.0.0 / 16

AWS의 사용 가능 IP 숫자는 5개를 제외하고 계산

- |                              |                                    |
|------------------------------|------------------------------------|
| • 첫번째 주소 (네트워크 주소)           | : 172.16.0.0                       |
| • 두번째 주소 (AWS VPC 가상 라우터 주소) | : 172.16.0.1                       |
| • 세번째 주소 (AWS DNS 주소)        | : 172.16.0.2                       |
| • 네번째 주소 (향후 새로운 기능에 사용할 주소) | : 172.16.0.3                       |
| • 마지막 주소 (브로드캐스트 주소)         | : 172.16.255.255 (단 브로드캐스트는 지원 안함) |
| • 유효 IP 주소                   | : 172.16.0.4 ~ 172.16.255.254      |

## ※ AWS 구조 - VPC (Virtual Private Cloud)



Routing Table

Destination	Target
10.0.0.0/16	local
<b>0.0.0.0/0</b>	<b>Igw-id</b>

- 목적지가 10.0.\*.\*이면 VPC안의 리소스
- 기타 모든 목적지는 Igw-id를 경유

Routing Table

Destination	Target
10.0.0.0/16	local

- 목적지가 10.0.\*.\*이면 VPC안의 리소스

### VPC – Subnet 유형

#### • 퍼블릭 서브넷(Public Subnet)

인터넷 게이트웨이로 향하는 라우팅이 있는 라우팅 테이블과 연결

- 인터넷 게이트웨이를 통해 인터넷으로 라우팅

인터넷 통신 가능 하려면, 각 인스턴스는 **공인 IP**를 가지고 있어야 함

- 공인 IP 자동할당 또는 EIP 명시 할당

웹서버, 애플리케이션 서버 등 사용자에게 노출하는 인프라

#### • 프라이빗 서브넷(Private Subnet)

인터넷 게이트웨이로 향하는 라우팅이 없는 라우팅 테이블과 연결

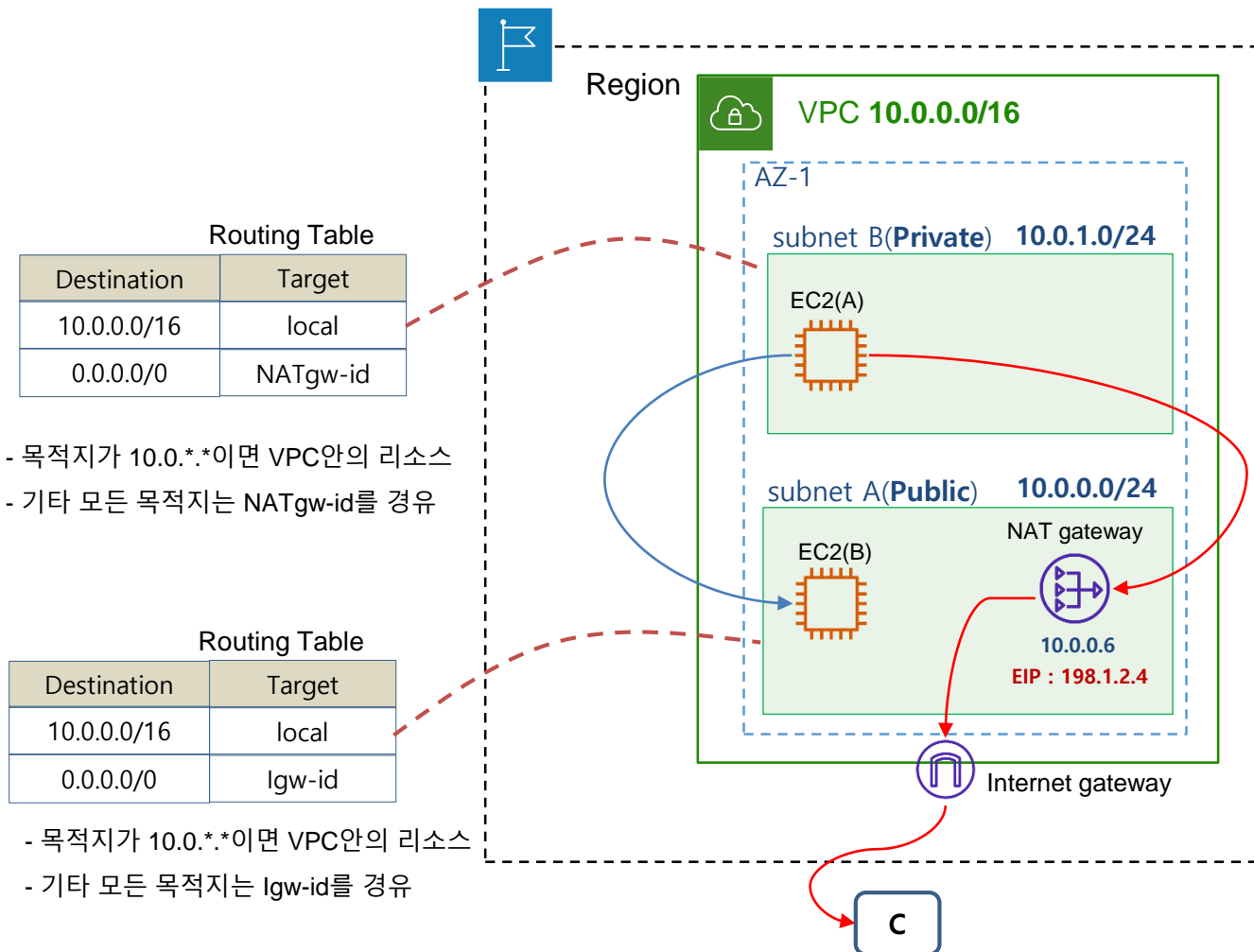
- 외부 인터넷 경로가 없음

인터넷에 액세스하려면 **NAT 장치**가 필요

데이터베이스, 로직 서버 등 외부 노출이 불필요한 인프라



## ※ AWS 구조 - VPC (Virtual Private Cloud)



### 프라이빗 서브넷에서 인터넷 연결

- NAT gateway를 통해 외부 인터넷 접속
- 외부 인터넷 통신을 위해 NAT gateway는 Public subnet에 위치해야 하고, 공인 IP를 부여 받아야 함

※ IGW는 공인 IP가 할당된 VPC내 인스턴스에 대해 NAT 수행

## NAT / PAT

- NAT (Network Address Translation) : IP 주소를 다른 IP 주소로 변화해 주는 기술
- NAPT (Network Address Port Translation) : 여러 IP 주소를 하나의 IP로 변환하는 기술
  - 통산, NAT로 불리기도 하고, PAT(Port Address Translation)라고 부르기도 함
- AFT (Address Family Translation) : IPv4 주소와 IPv6 주소의 상호 변환 기술

**NAT가 가장 많이 사용되는 경우는  
사설 IP 주소와 공인 IP 주소 간의 변환**



# 1 NAT / PAT

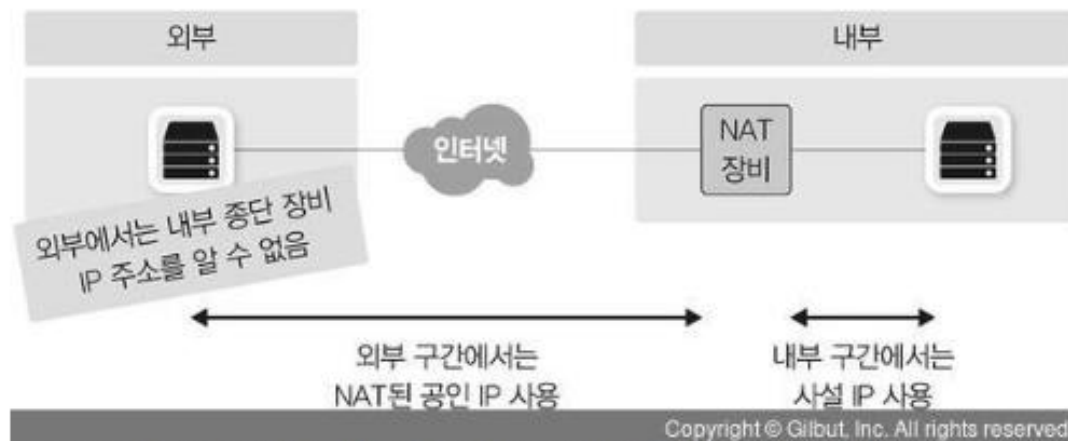
## 1.1 NAT / PAT의 필요성

### (1) IPv4 주소의 고갈 문제 해결 방안

- (단기 전략) subnetting / (중기 전략) NAT와 사설 IP 체계 / (장기 전략) IPv6
- 외부에 공개할 필요가 없는 사용자 PC나 종단 장비는 사설 IP 사용

### (2) 보안 강화

- 외부 통신시 내부 IP를 다른 IP로 변환해 통신하면 외부에 사내 IP 주소체계 숨기 가능

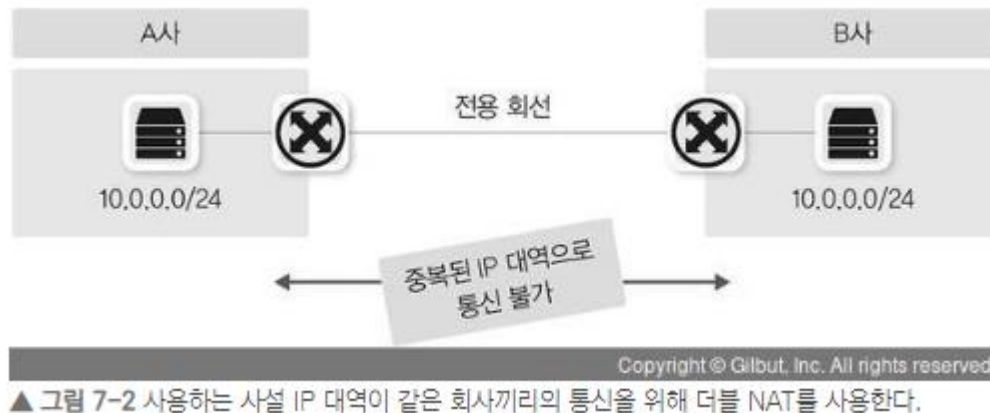


▲ 그림 7-1 외부 구간에서는 내부 장비의 IP가 보이지 않도록 NAT를 사용한다.

# 1 NAT / PAT

## 1.1 NAT / PAT의 필요성

(3) IP 주소 체계가 같은 두 개의 네트워크 간 통신을 가능하게 해 줌



- 대외계 : 카드사, 은행 간 통신 등은 개인 정보 보호와 각종 법규 등으로 인터넷을 사용하지 않고 별도 네트워크 사용
- 대외계의 경우, IP 대역이 같은 네트워크와 통신할 가능성이 많음
- 더블 나트(Double NAT) : 출발지와 도착지 IP를 동시에 변경하는 기술

# 1 NAT / PAT

## 1.1 NAT / PAT의 필요성

(4) 불필요한 설정 변경을 줄일 수 있음

- 회선 사업자나 IDC를 이전하면, 그동안 사용하던 공인 IP 주소 사용이 안됨
- 신규 사업자가 부여한 새로운 IP 주소로 변경해야 함
- NAT/PAT 사용시 내부 서버 PC의 IP 주소 변경 없이 IDC 사업자 이전이 가능
- NAT 장비나 DNS 등의 설정은 해주어야 함

NAT 사용으로 장애 발생시 문제 해결의 어려움 발생 (IP 변환으로 추적이 어려움)

# 1 NAT / PAT

## 1.2 NAT 동작 방식



▲ 그림 7-3 NAT 동작 순서

1. 사용자는 웹 서버에 접근하기 위해 출발지 IP를 10.10.10.10으로, 목적지 IP와 서비스 포트는 20.20.20.20과 80으로 패킷을 전송합니다. 출발지 서비스 포트는 임의의 포트로 할당됩니다. 여기서는 2000번 포트로 가정했습니다.
2. NAT 역할을 수행하는 장비에서는 사용자가 보낸 패킷을 수신한 후 NAT 정책에 따라 외부 네트워크와 통신이 가능한 공인 IP인 11.11.11.11로 IP 주소를 변경합니다. NAT 장비에서 변경 전후의 IP 주소는 NAT 테이블에 저장됩니다.
3. NAT 장비에서는 출발지 주소를 11.11.11.11로 변경해 목적지 웹 서버로 전송합니다.
4. 패킷을 수신한 웹 서버는 사용자에게 응답을 보냅니다. 응답이므로 수신한 내용과 반대로 출발지는 웹 서버(20.20.20.20)가 되고 목적지는 NAT 장비에 의해 변환된 공인 IP 11.11.11.11로 사용자에게 전송합니다.
5. 웹 서버로부터 응답 패킷을 수신한 NAT 장비는 자신의 NAT 테이블에서 목적지 IP에 대한 원래 패킷을 발생시킨 출발지 IP 주소가 10.10.10.10인 것을 확인합니다.
6. NAT 변환 테이블에서 확인된 원래 패킷 출발지 IP(10.10.10.10)로 변경해 사용자에게 전송하면 사용자는 최종적으로 패킷을 수신합니다.

# 1 NAT / PAT

## 1.3 PAT 동작 방식



▲ 그림 7-4 PAT 동작 순서

1. 사용자가 웹 서버로 접근하기 위해 패킷에 출발지 10.10.10.10, 목적지 20.20.20.20, 목적지 서비스 포트는 웹 서비스 포트인 80으로 채워 패킷을 전송합니다. 출발지 서비스 포트는 NAT와 마찬가지로 임의의 서비스 포트가 할당되며 이 예제에서는 2000번 포트에 할당되었다고 가정합니다.
2. NAT 장비는 사용자가 보낸 패킷을 받아 외부 네트워크와 통신이 가능한 공인 IP인 11.11.11.11로 변경합니다. 다만 출발지에 있는 다수의 사용자가 동일한 공인 IP로 변환되어야 하므로 패킷의 주소 변경 시 출발지 IP뿐만 아니라 출발지의 서비스 포트도 변경됩니다. 출발지 IP와 출발지 서비스 포트는 NAT 장비에 의해 모두 변경되고 NAT 장비가 이 변경 정보를 NAT 테이블에 기록합니다.
3. NAT 장비에서 변경된 출발지 IP 주소인 11.11.11.11과 서비스 포트 3000으로 패킷을 재작성해 웹 서버로 다시 전송합니다.
4. 사용자가 보낸 패킷을 수신한 웹 서버는 사용자에게 패킷을 응답하는데 출발지 IP는 웹 서버의 IP 주소인 20.20.20.20으로 채워지고 목적지 IP는 NAT 장비에 의해 변환된 공인 IP 11.11.11.11과 서비스 포트에 채워져 전송합니다.
5. 웹 서버로부터 응답 패킷을 수신한 NAT 장비는 NAT 테이블을 확인해 웹 서버로부터 받은 패킷의 목적지 IP 주소인 11.11.11.11이 원래 10.10.10.10이며 서비스 포트 3000이 원래 2000인 것을 확인합니다.
6. NAT 장비는 NAT 테이블에서 확인한 목적지 IP 주소와 서비스 포트에 패킷을 재작성한 후 사용자에게 전달합니다. 사용자는 NAT 장비에서 역변환된 패킷을 받아 웹 페이지를 표시합니다.

# 1 NAT / PAT

## 1.3 PAT 동작 방식



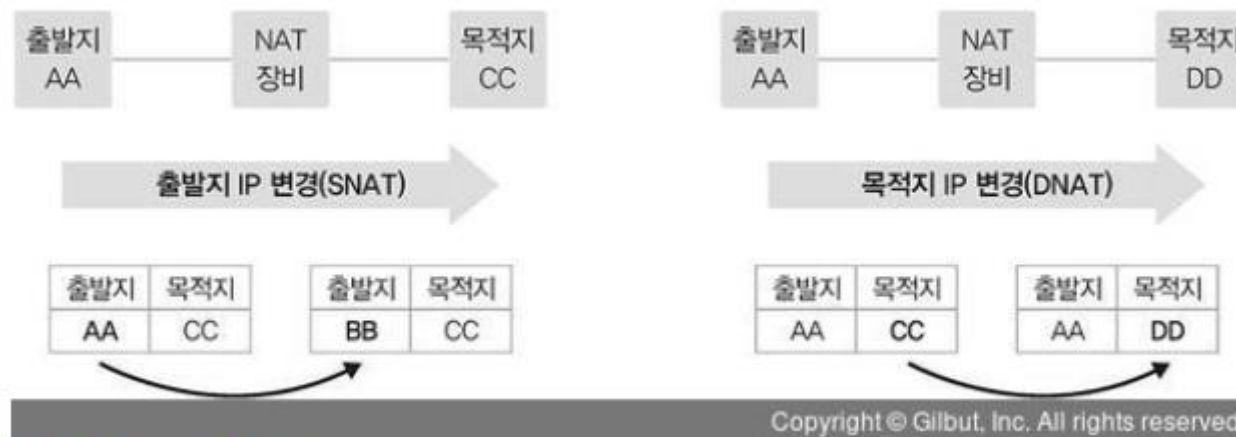
▲ 그림 7-5 PAT는 내부에서 외부로 출발하는 경우에만 가능하다.

- **NAT/PAT 내부에서** 시작된 요청은 NAT 장비에 NAT 테이블이 생성되어 응답에 대해서도 NAT 테이블을 참조하여 서비스 제공이 가능
- **NAT/PAT 외부에서** 시작된 요청은 NAT 장비에 NAT 테이블이 없기 때문에 서비스 불가

# 1 NAT / PAT

## 1.4 SNAT와 DNAT

- SNAT(Source NAT, 출발지 NAT) : 출발지 주소를 변경하는 NAT
- DNAT(Destination NAT, 도착지 NAT) : 도착지 주소를 변경하는 NAT



▲ 그림 7-6 SNAT와 DNAT

- SNAT, DNAT은 NAT가 수행되기 이전 트래픽이 출발하는 시작 지점을 기준으로 구분
- ※ 역 NAT(응답 패킷에 대한 주소변환)는 별도 NAT 설정 없이 자동으로 함께 수행됨

# 1 NAT / PAT

## 1.4 SNAT와 DNAT - SNAT의 사용 예

- 사설 IP에서 공인 IP로 통신할 때 (공유기)
- (보안) 회사에서 다른 대외사와 통신시 내부 IP를 숨기 필요가 있는 경우



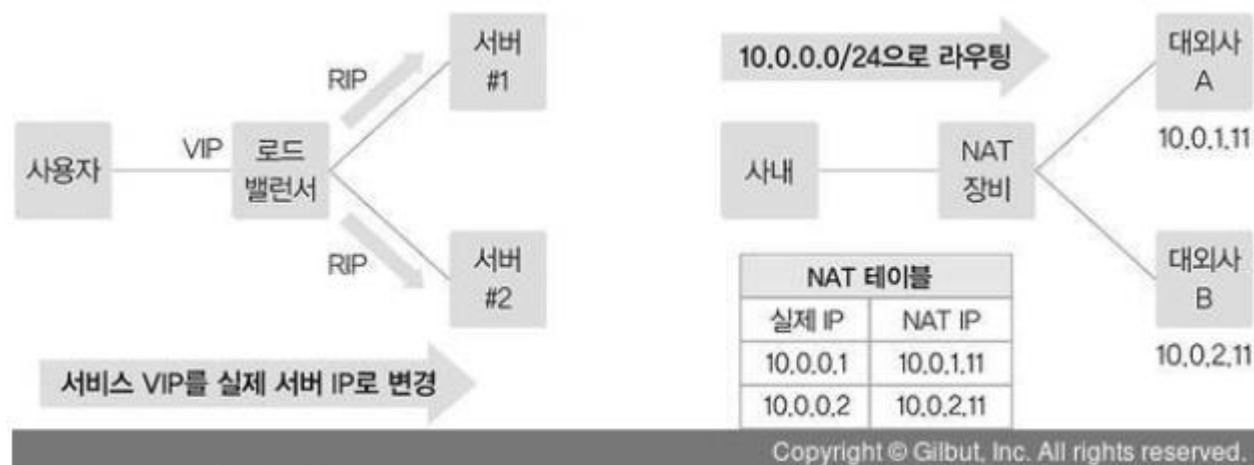
▲ 그림 7-7 SNAT를 하는 경우



# 1 NAT / PAT

## 1.4 SNAT와 DNAT - DNAT의 사용 예

- Load Balancer에서 VIP(Virtual IP)를 RIP(Real IP)로 변경할 때 사용
- 대외사의 IP 대역이 제각각 이라서 신규 대외사와 연동할 때마다 라우팅 설정이 필요
  - 내부적으로 대외망 전용 NAT 대역으로 NAT 테이블 구성
  - 10.0.0.1은 대외사 A, 10.0.0.2는 대외사 B 등으로 정하고, 실제 IP는 NAT 테이블로 조정

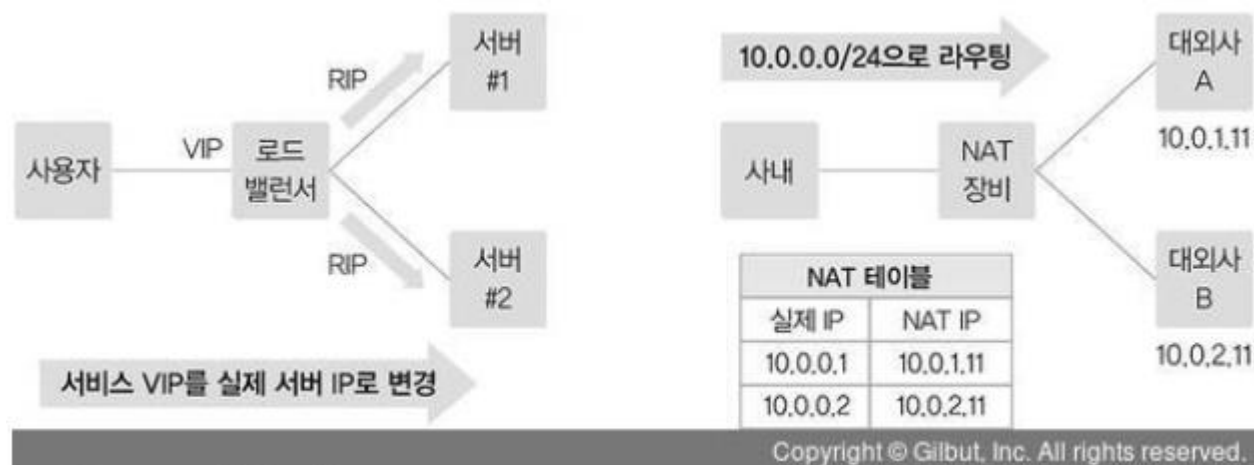


▲ 그림 7-8 DNAT를 하는 경우

# 1 NAT / PAT

## 1.4 SNAT와 DNAT - DNAT의 사용 예

- Load Balancer에서 VIP(Virtual IP)를 RIP(Real IP)로 변경할 때 사용
- 대외사의 IP 대역이 제각각 이라서 신규 대외사와 연동할 때마다 라우팅 설정이 필요
  - 내부적으로 대외망 전용 NAT 대역으로 NAT 테이블 구성
  - 10.0.0.1은 대외사 A, 10.0.0.2는 대외사 B 등으로 정하고, 실제 IP는 NAT 테이블로 조정



▲ 그림 7-8 DNAT를 하는 경우

# 1 NAT / PAT

## 1.5 동적 NAT와 정적 NAT

- 정적 NAT : 출발지와 목적지 IP를 미리 매핑해 고정해 놓은 NAT
  - 출발지, 목적지 IP가 사전에 정의 됨. 1:1 NAT라고도 부름
- 동적 NAT : 출발지, 목적지 IP를 미리 정해 놓지 않고, NAT를 수행할 때 IP를 동적으로 변경
  - 출발지나 목적지 IP 중 하나는 다수의 IP pool 또는 IP Range로 설정됨
  - NAT를 수행하는 시점에서, IP Pool에서 어떤 IP로 매핑할지 판단해 NAT 테이블 구성
  - NAT table Timeout : 설정된 시간 동안 유지되고 일정시간 통신이 없으면 사라짐

# 1 NAT / PAT

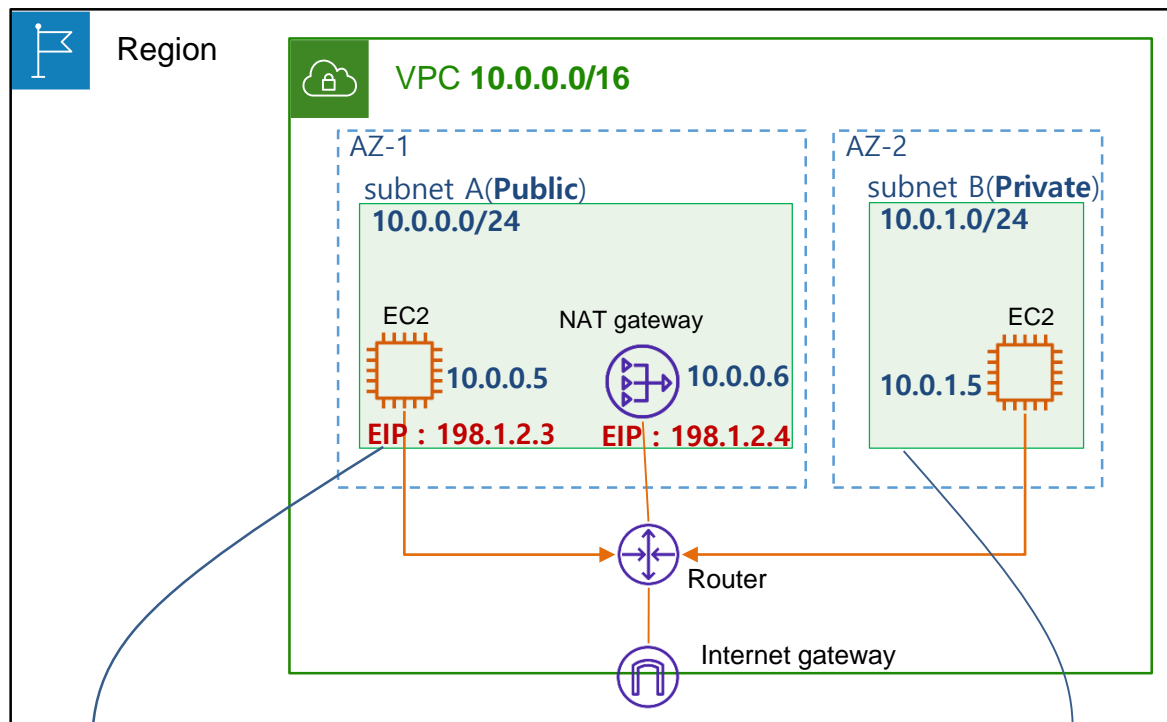
## 1.5 동적 NAT와 정적 NAT

▼ 표 7-1 동적 NAT와 정적 NAT 비교

	동적 NAT	정적 NAT
NAT 설정	1:N, N:1, N:M	1:1
NAT 테이블	NAT 수행 시 생성	사전 생성
NAT 테이블 타임아웃	동작	없음
NAT 수행 정보	실시간으로만 확인하거나 별도 변경 로그 저장 필요	별도 필요 없음 (설정 = NAT 내역)



## ※ AWS 구조 - VPC (Virtual Private Cloud)



### 프라이빗 서브넷에서 인터넷 연결

- NAT gateway를 통해 외부 인터넷 접속

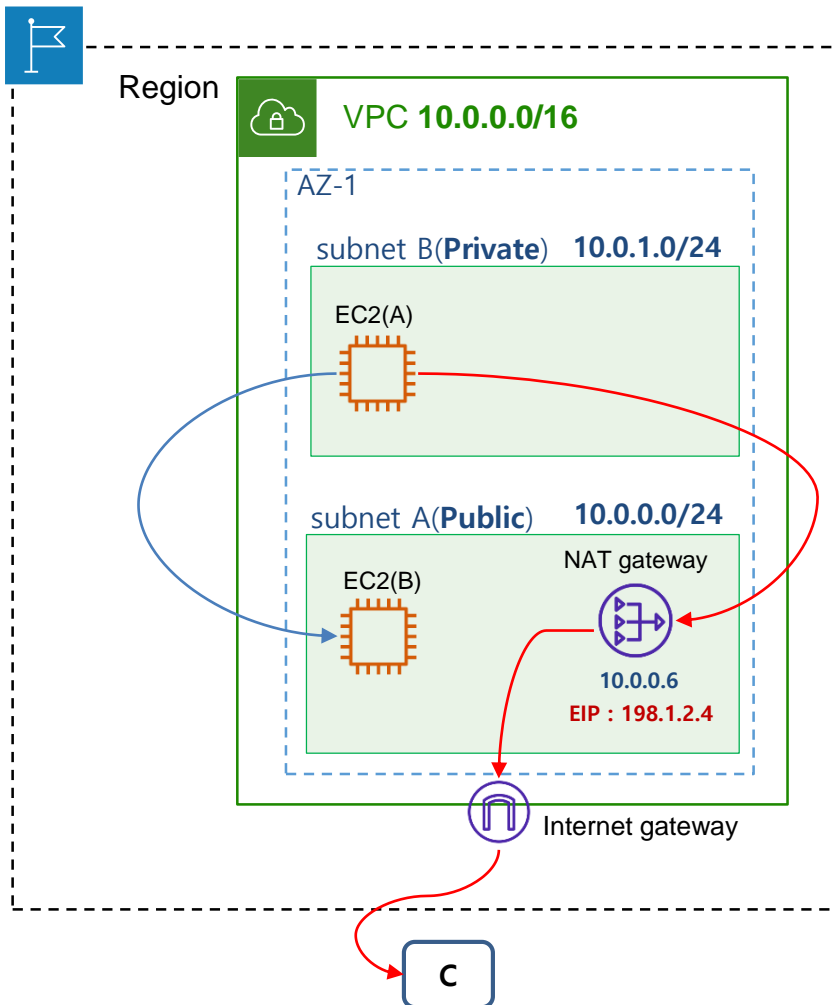
Routing Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	lgw-id

Routing Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<b>NAT-GW-id</b>

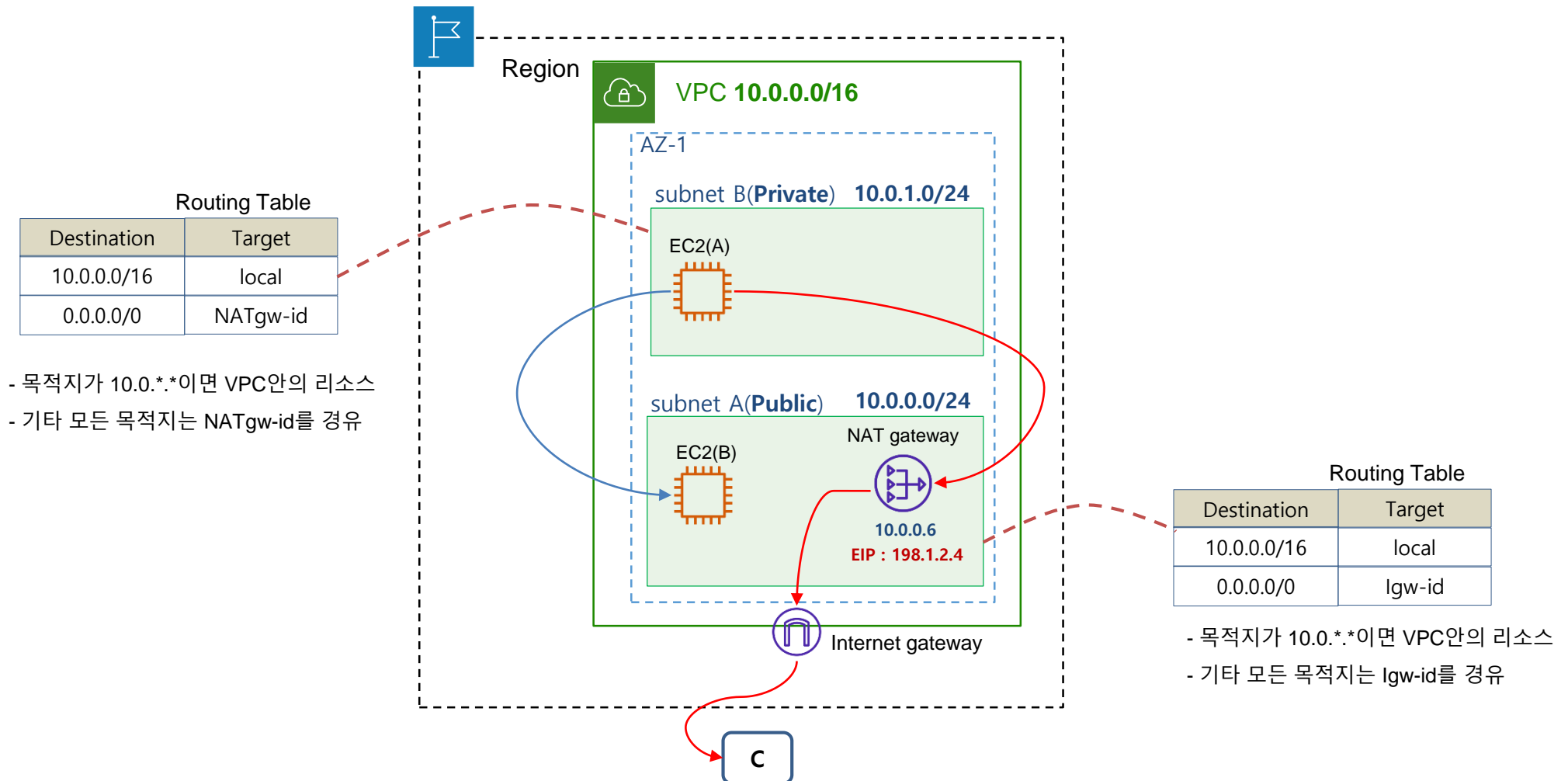
## ※ AWS 구조 - VPC (Virtual Private Cloud)



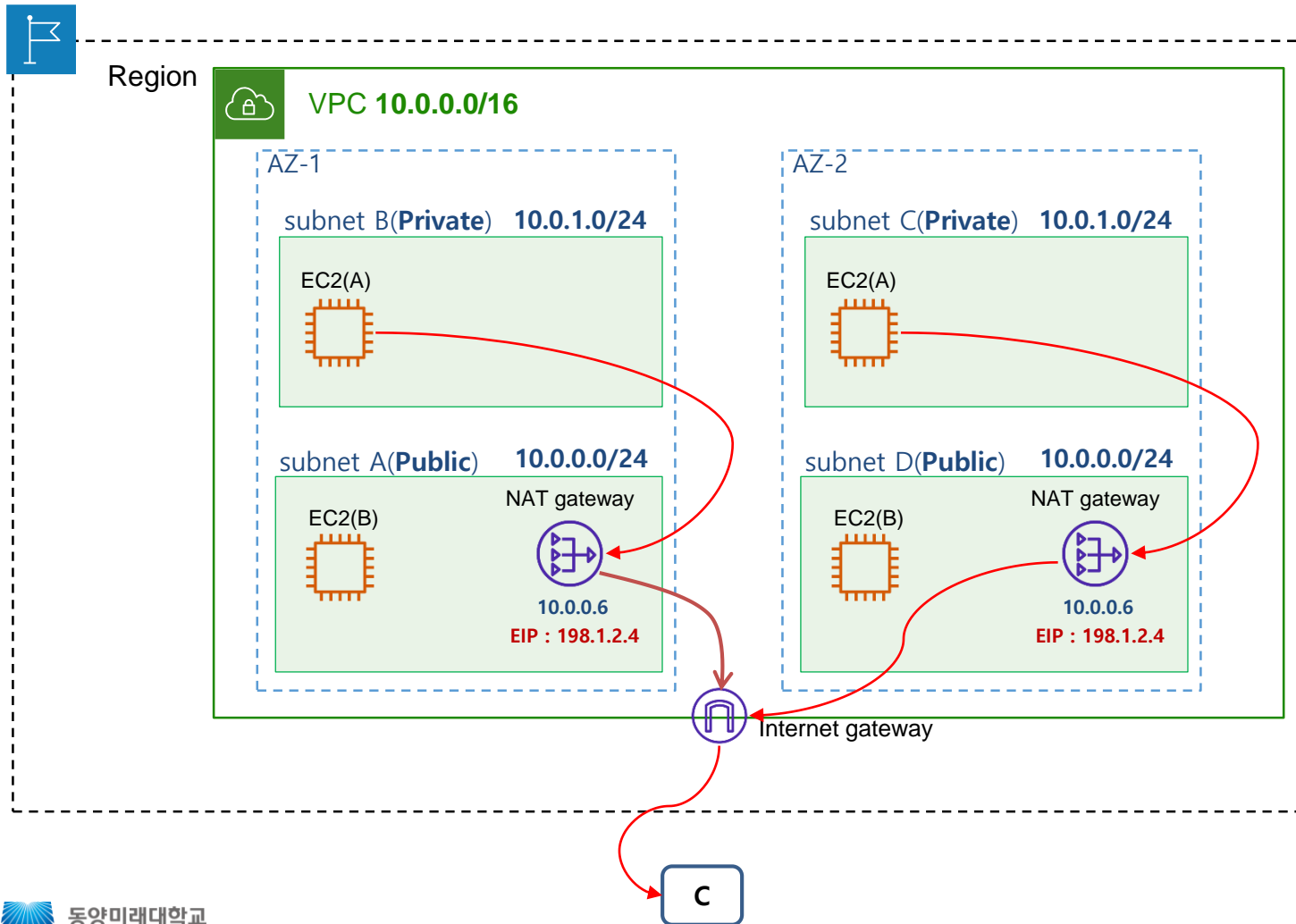
## 프라이빗 서브넷에서 인터넷 연결

- NAT gateway를 통해 외부 인터넷 접속
  - NAT gateway는 Public subnet에 위치해야 함
  - NAT는 공인 IP(EIP)를 할당해야 함(외부 인터넷 통신)
  - Subnet 사이의 통신 경로를 설정하기 위해 라우팅테이블 설정
- ❖ NAT 장비에 EIP를 할당하여 사용하다가, NAT를 삭제하여도 EIP는 그대로 남아있고 이용료가 부가됨

## ※ AWS 구조 - VPC (Virtual Private Cloud)



## ※ AWS 구조 - VPC (Virtual Private Cloud)



- 사용 영역별 NAT GW를 구성하여 장애 대비