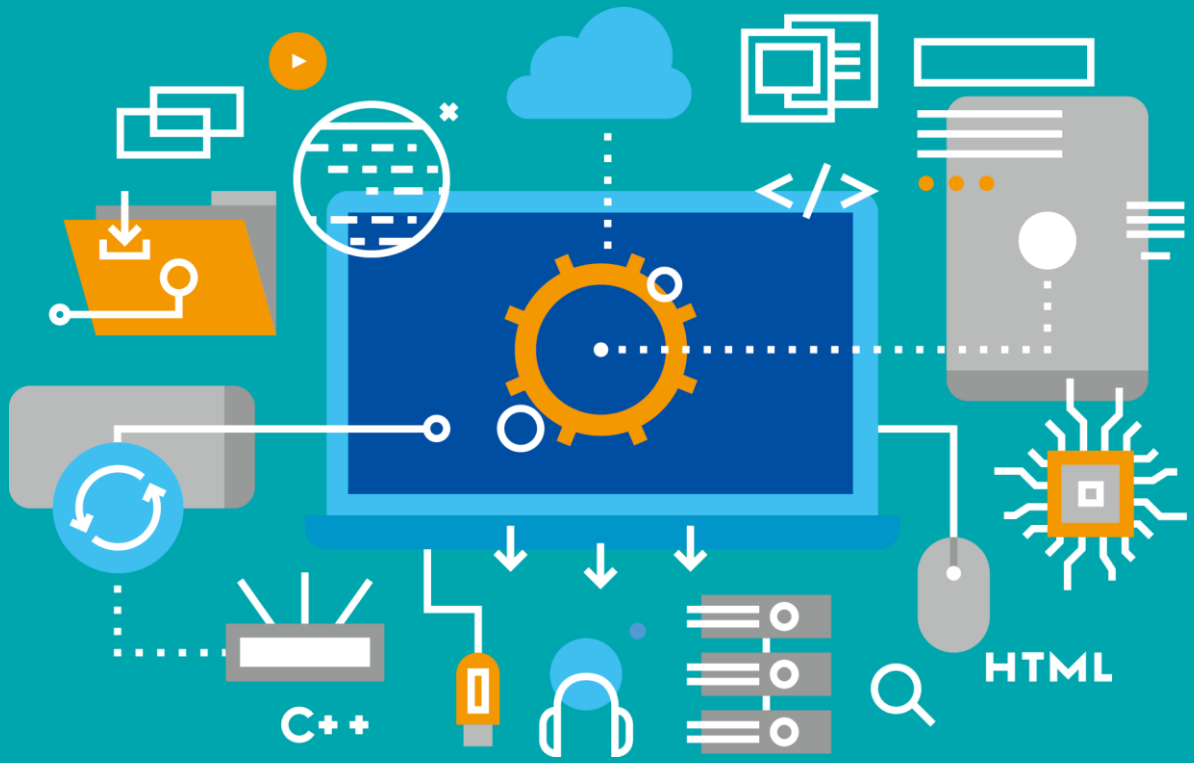
동양미래대학교

DMMU

동양미래대학교 전문기술 석사과정

클라우드와 네트워크 보안

Dongyang Mirae University



5장

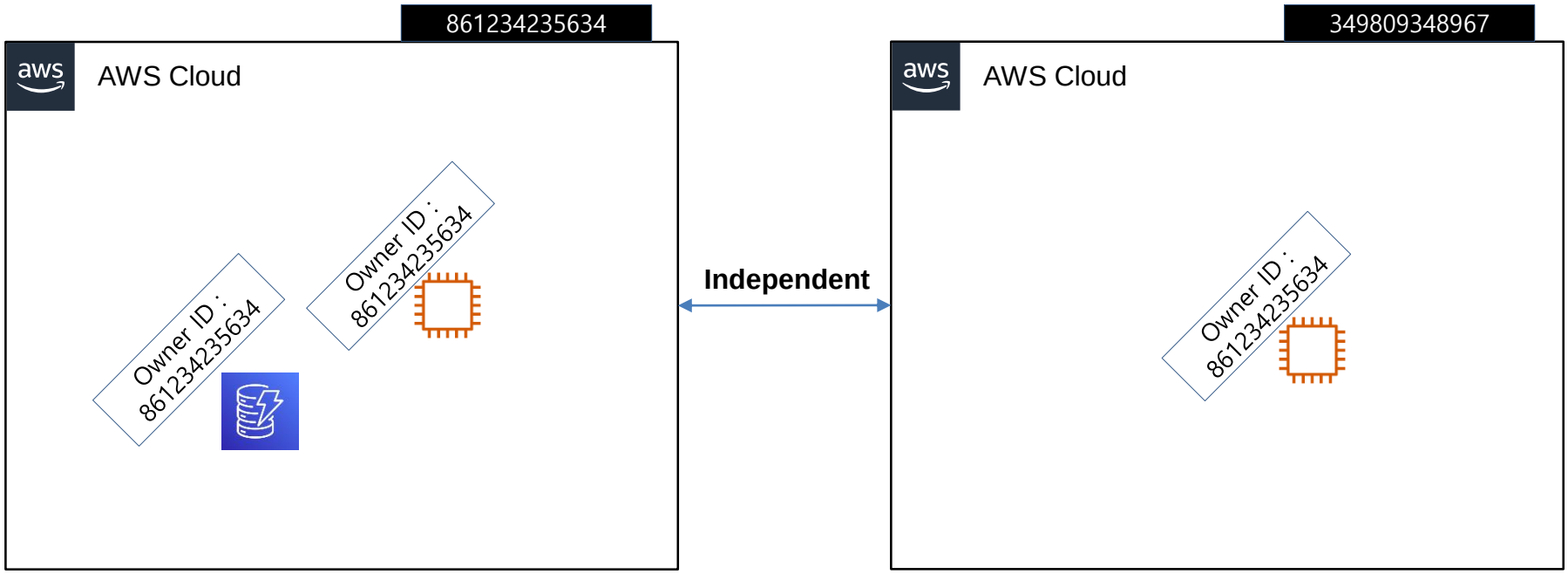
AWS VPC와 AWS 서비스

※ VPC (Virtual Private Cloud)

AWS 서비스를 쉽게 관리할 수 있는 **네트워크 플랫폼**

※ 사용자 계정과 AWS cloud

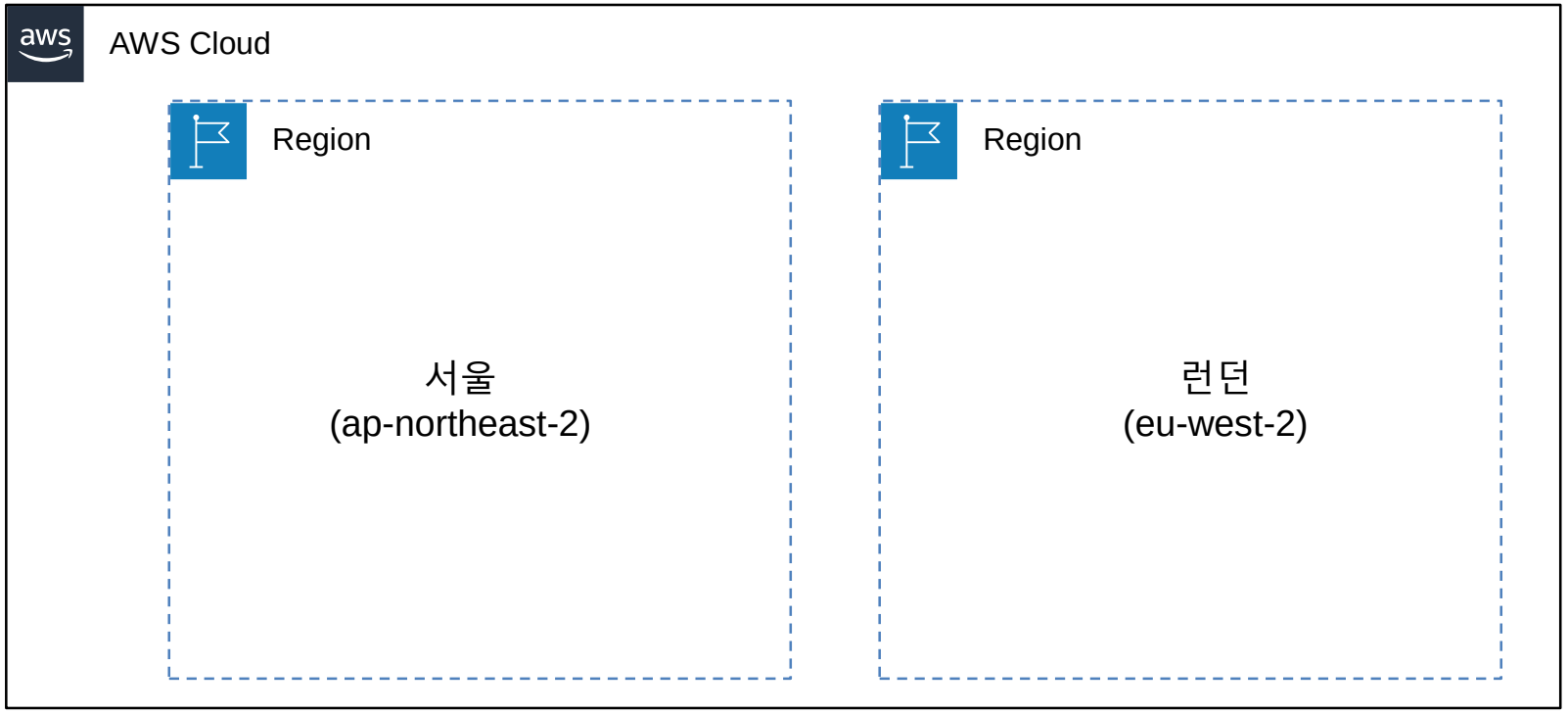
- AWS 계정 전용 doud 공간으로 , 서로 다른 AWS 계정 사이를 침범할 수 없음
- AWS 계정을 접속하여 클라우드 서비스를 구축하고 운영할 수 있는 나만의 공간



AWS 모든 서비스는 암묵적으로 계정 ID 식별자가 부착

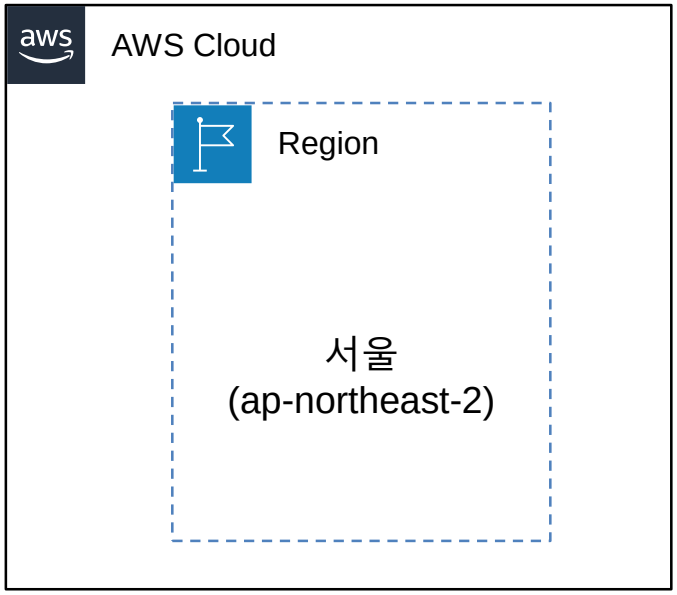
※ 사용자 계정과 Region

- Region은 지리적 개념으로 물리적으로 떨어진 공간 (Region간 교집합 없음)
- 사용자가 선택한 Region에 따라 서비스의 물리적 생성 위치가 달라짐



런던 region(eu-west-2)을 선택하고 instance를 만들면,
런던에 위치한 데이터센터에 instance가 프로비전됨

※ 사용자 계정과 Region



Seoul region : ap-northeast-2

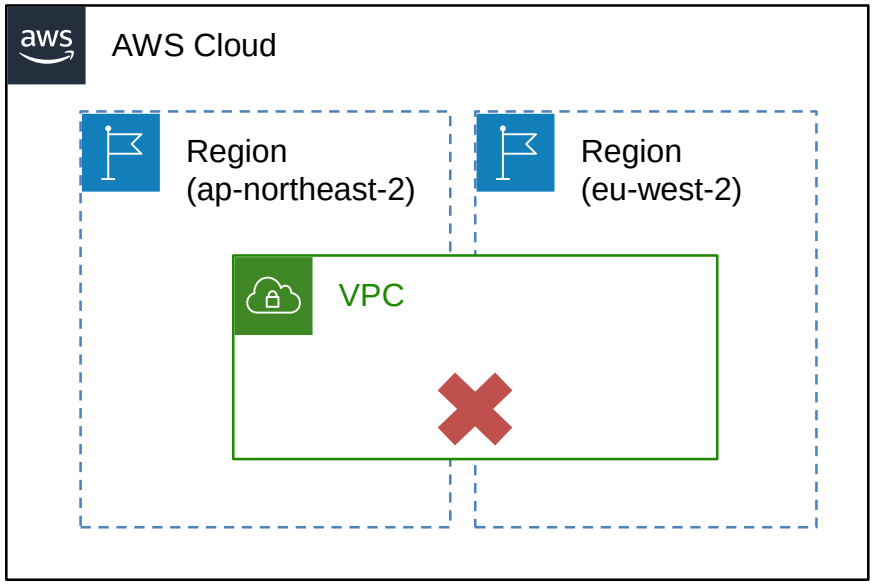
Tokyo region : ap-northeast-1

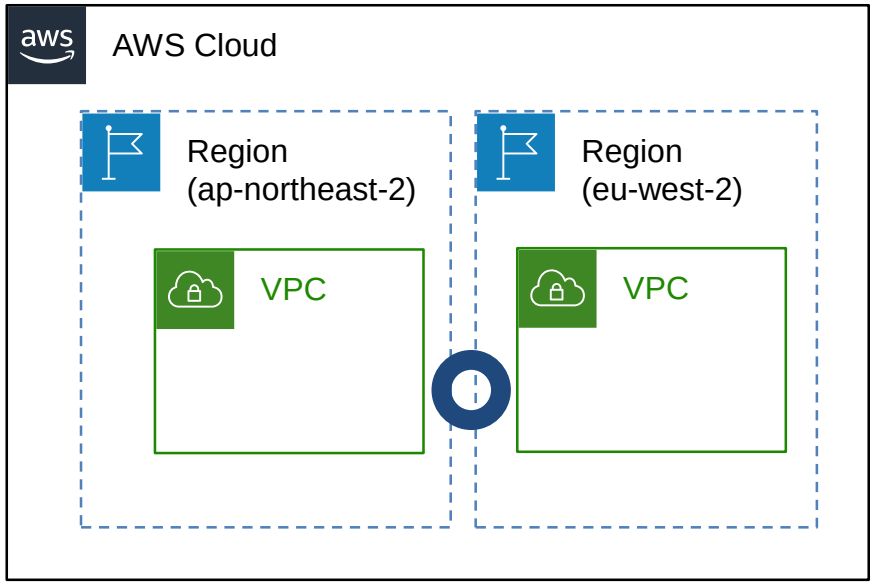
Osaka region : ap-northeast-3

- 세계 각지에 사용자가 이용하는 서비스를 구축하여 통신 시간 지연을 줄일 수 있음
- 특정 국가의 법적 요구사항을 만족하는 시스템을 구축해야 하는 경우 특정 리전을 사용하여 구축
- 재난 발생으로 특정 리전의 시스템 사용이 불가한 경우, 다른 리전에서 시스템 가동

※ Region과 VPC

- VPC 네트워킹의 시작 : 원하는 Region을 선택하고, VPC를 생성
- VPC는 오직 1개의 Region에만 포함

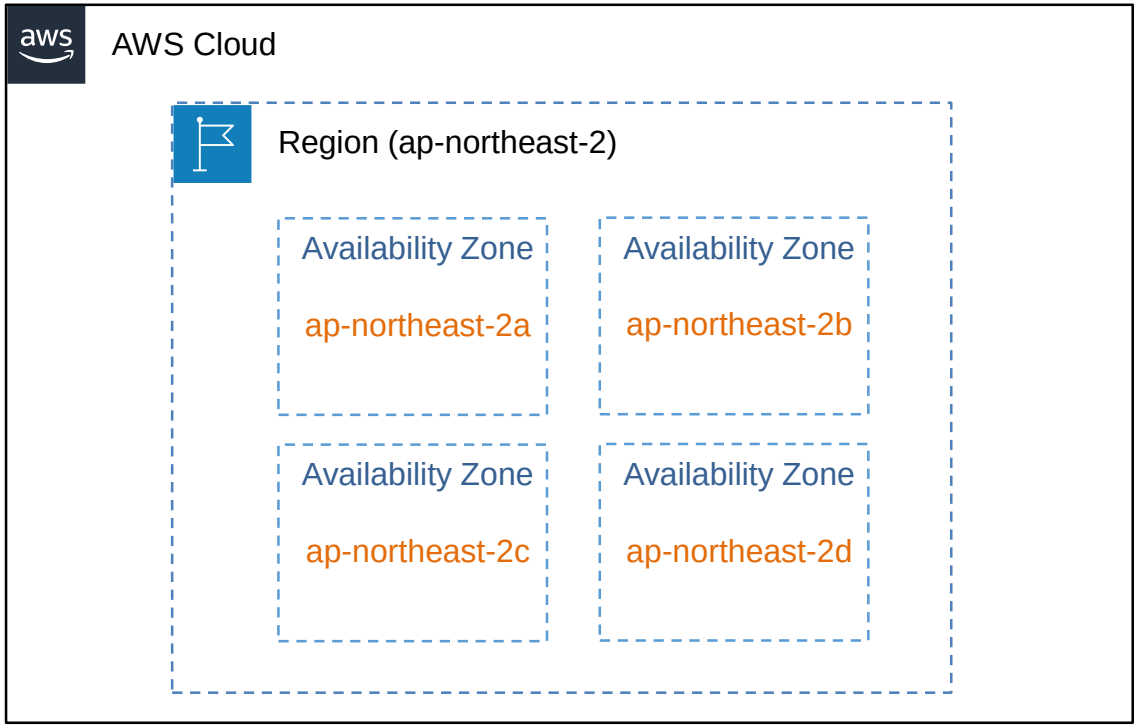




VPC는 하나의 특정 Region에서만 존재할 수 있다.

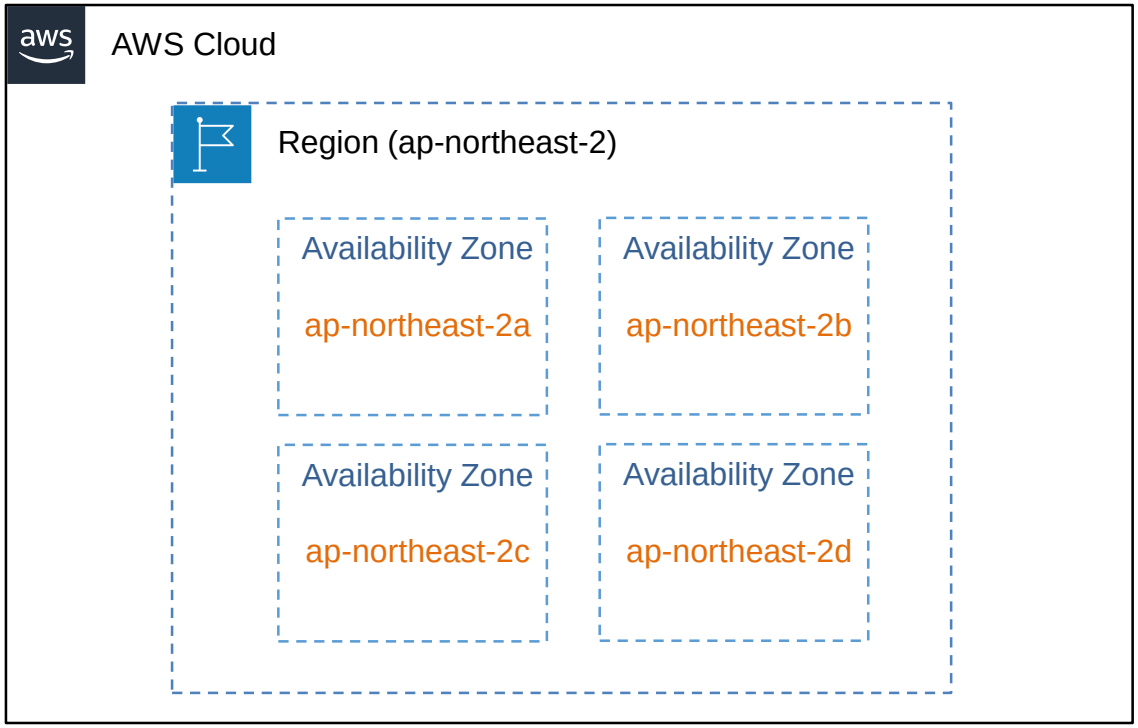
※ Region과 가용영역(AZ : Availability Zone)

- 서비스의 **가용성 보장**을 위해 **Region을 세분화해서 격리시킨 공간**
- Region에는 1개에서 6개 이상의 가용영역을 포함하며,
- AZ 이름은 **region 이름 뒤에 a, b, c 순으로 알파벳** 붙임



서울 region(ap-northeast-2)은 4개의 가용영역으로 구성됨

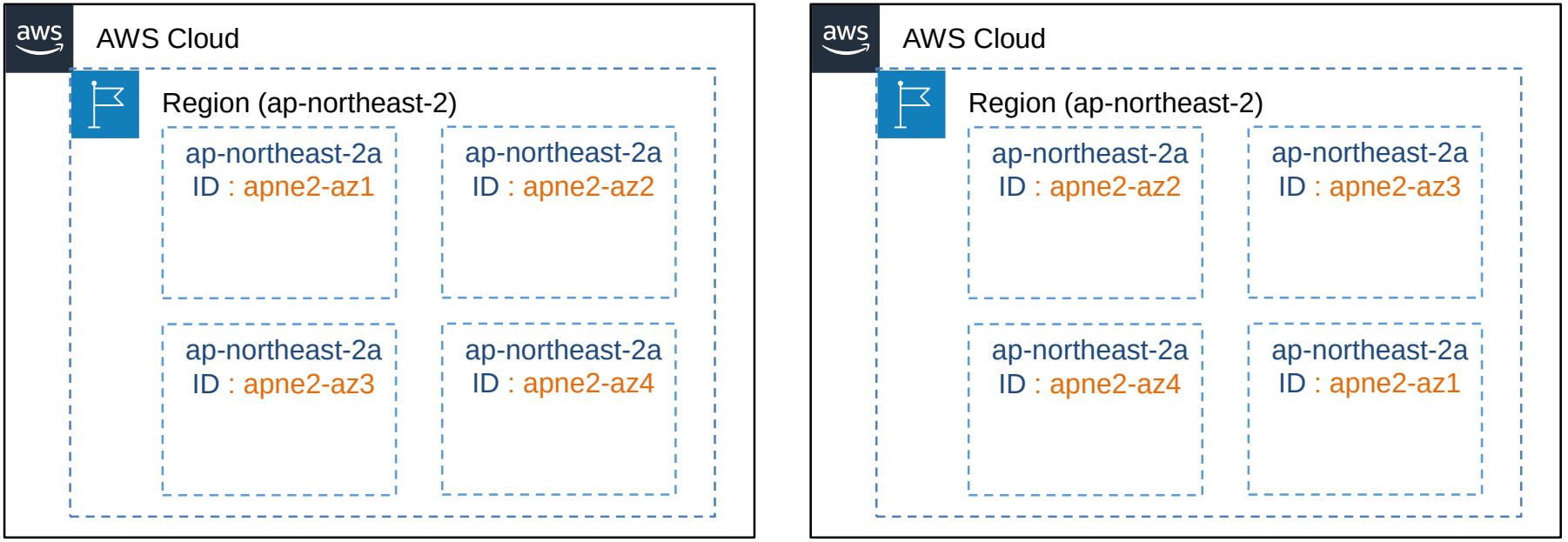
※ VPC와 가용영역(AZ : Availability Zone)



서울 region(ap-northeast-2)은
4개의 가용영역으로 구성됨

- Region내 가용영역은 서로 지리적으로 떨어져 있음(100km 이내 위치)
- 각 AZ은 전력원이나 네트워크 설비가 독립적이고,
- 가용영역 사이에는 다중 광 네트워크로 연결되고(최소지연시간내 통신), 데이터 암호화 통신

※ VPC와 가용영역(AZ : Availability Zone)

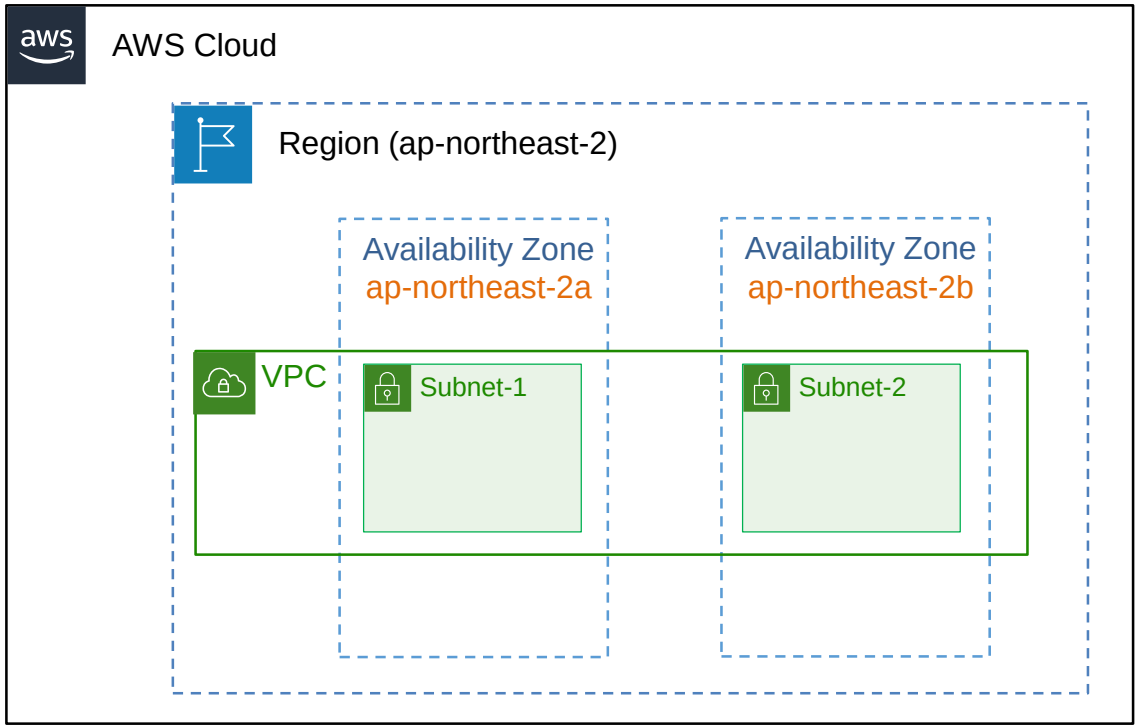


- AWS 계정마다 AZ 이름에 연결되는 ID는 다르다.
- 리소스를 생성하는 등 이용할 때는 AZ 이름을 사용하여 지정
- 장애가 발생하면 AZ ID를 확인

❖ AWS 자원이 각 AZ에 분산시키기 위해 AWS 계정마다 AZ 이름에 연결되는 ID가 다르게 운영

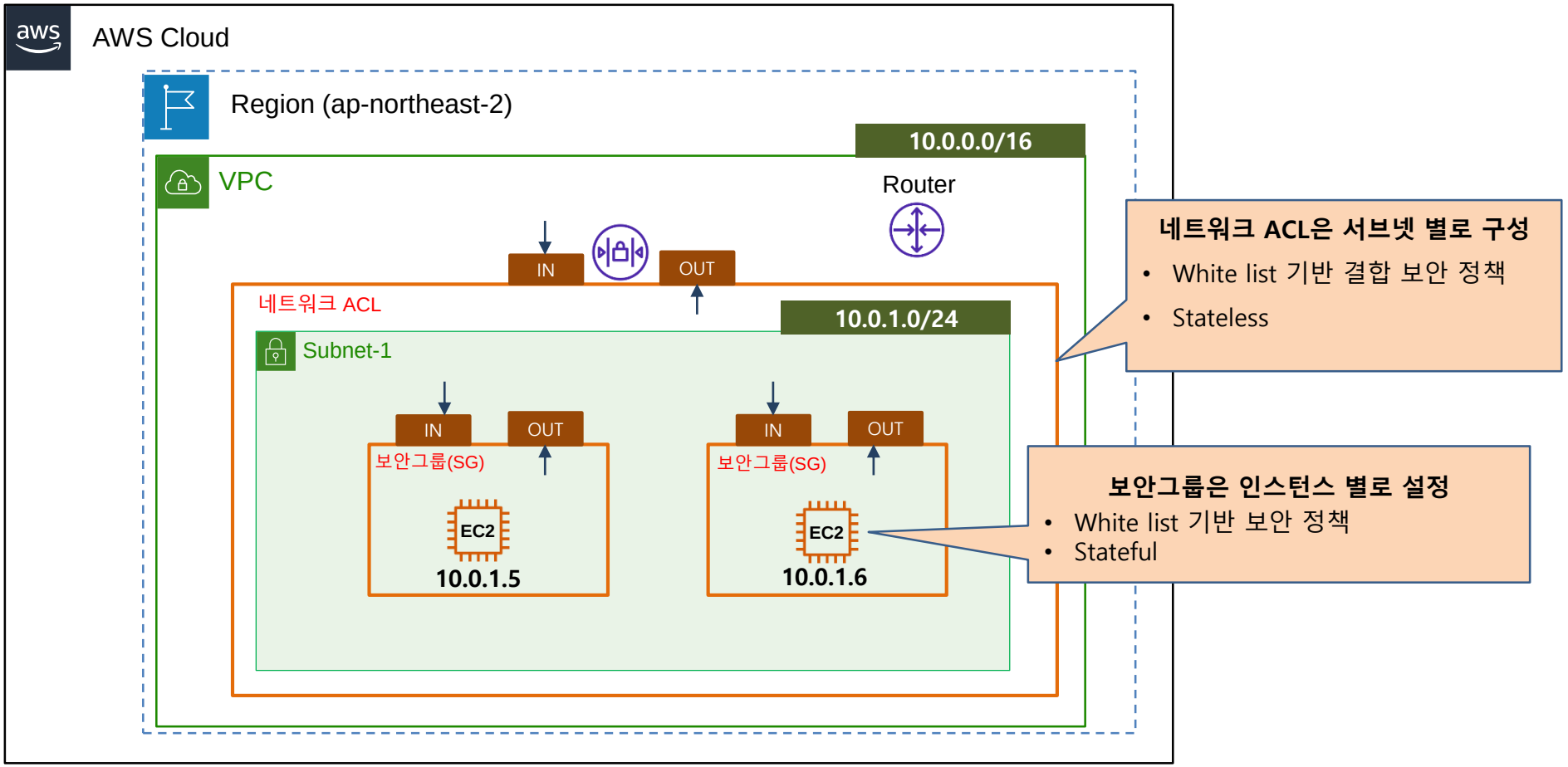
※ VPC와 서브넷

- 서브넷은 특정 VPC내, 특정 AZ에 구성됨
- VPC 내부에 생성하는 논리적 네트워크 공간 (네트워크 인터페이스를 서브넷에 배분하고 보안 통제요소 관리)
- 서브넷에 위치하는 서비스(네트워크 인터페이스)는 자동으로 보안그룹, NACL, 라우팅 테이블의 통제를 받음
- VPC는 서브넷의 모음



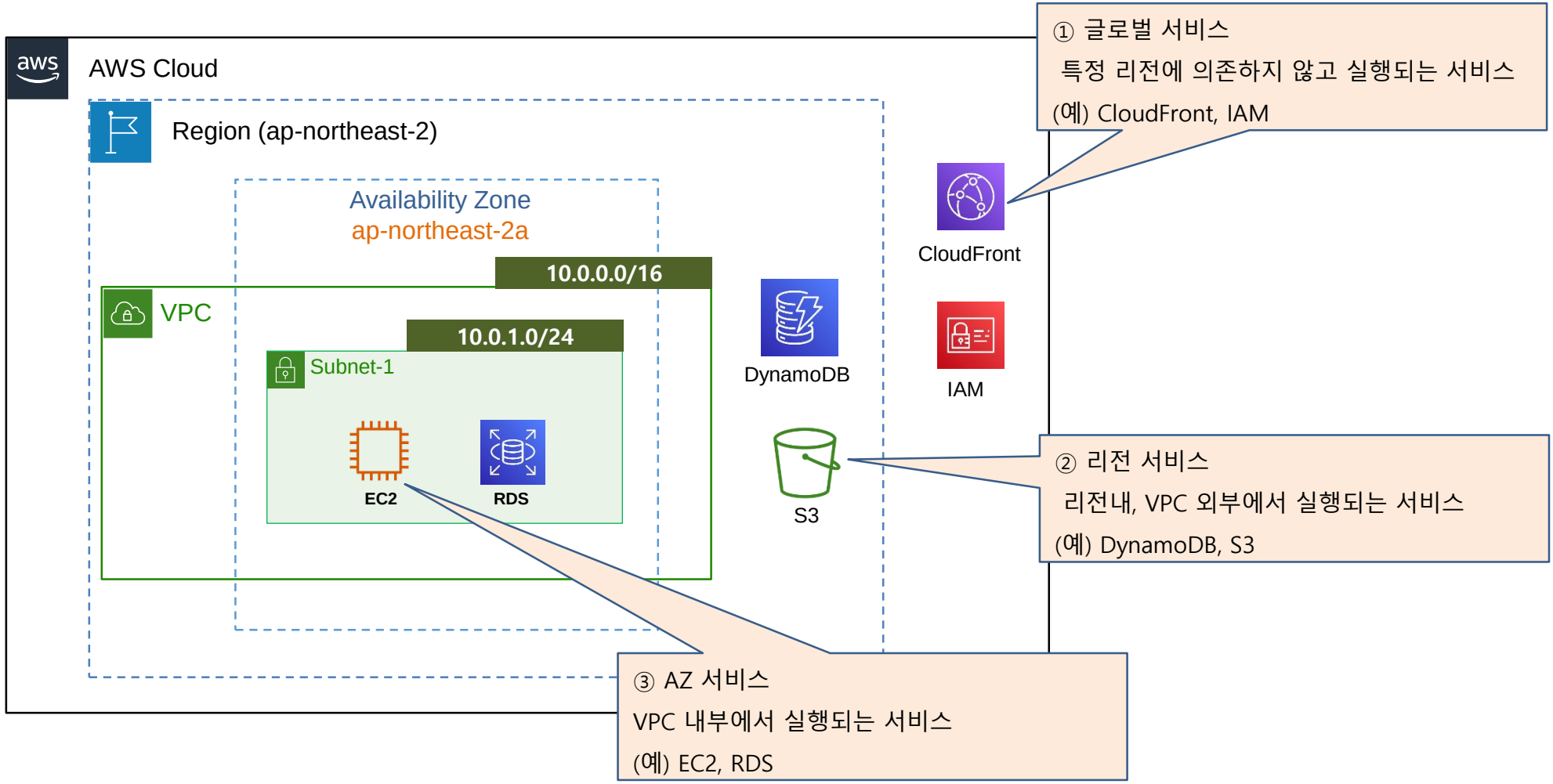
※ VPC와 서브넷

- 서브넷에 위치하는 서비스(네트워크 인터페이스)는 자동으로 보안그룹, NACL, 라우팅 테이블의 통제를 받음



※ VPC와 AWS 서비스

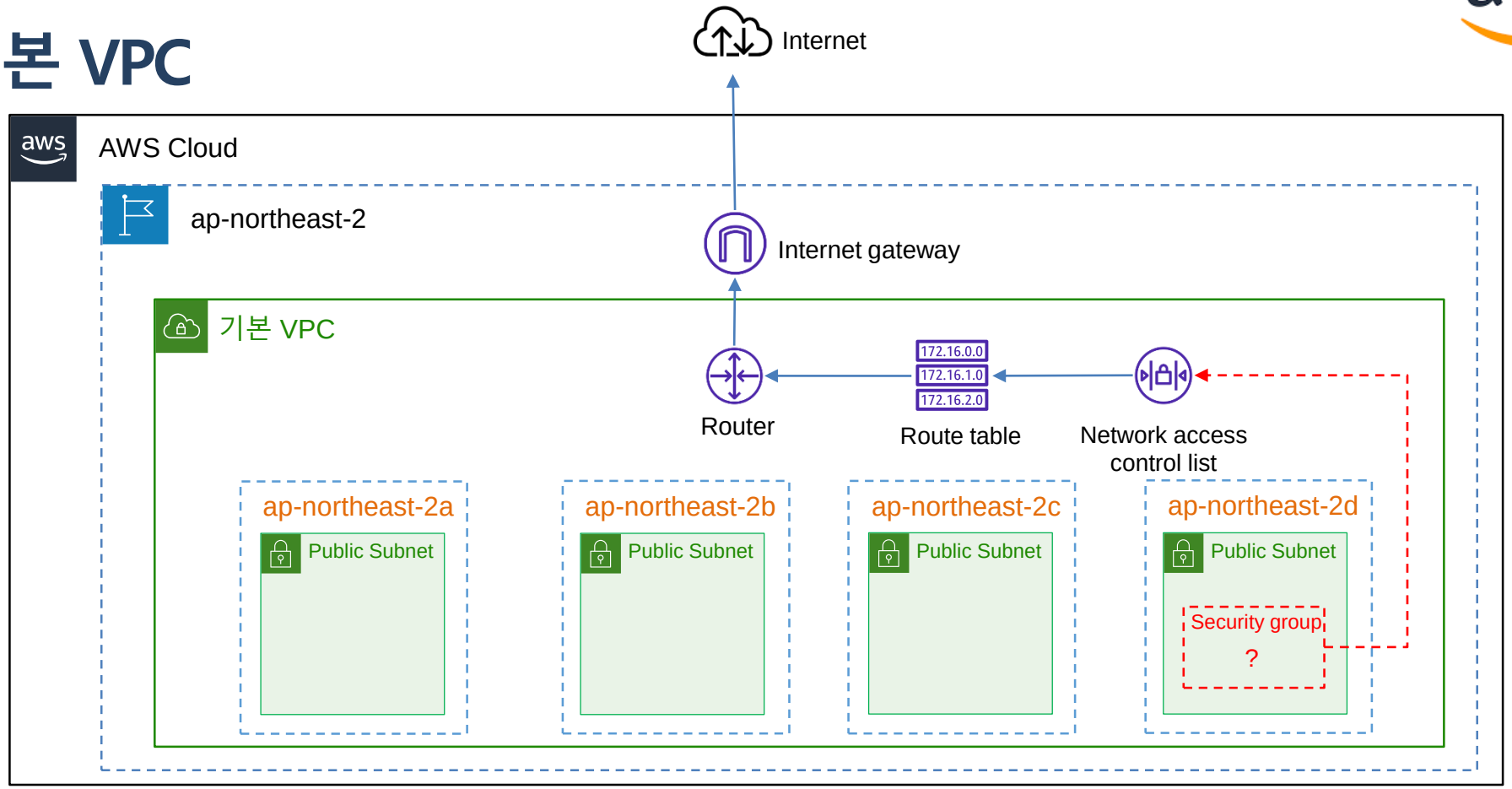
- AWS 서비스는 실행 위치에 따라 3가지 유형으로 구분 가능



※ VPC와 서브넷


AWS Cloud
Region (ap-northeast-2)
Availability Zone
ap-northeast-2a
Availability Zone
ap-northeast-2b
VPC
Subnet-1
AWS Cloud
Region (ap-northeast-2)
Availability Zone
ap-northeast-2a
Availability Zone
ap-northeast-2b
VPC
Subnet-1
Subnet-1
VPC

※ 기본 VPC

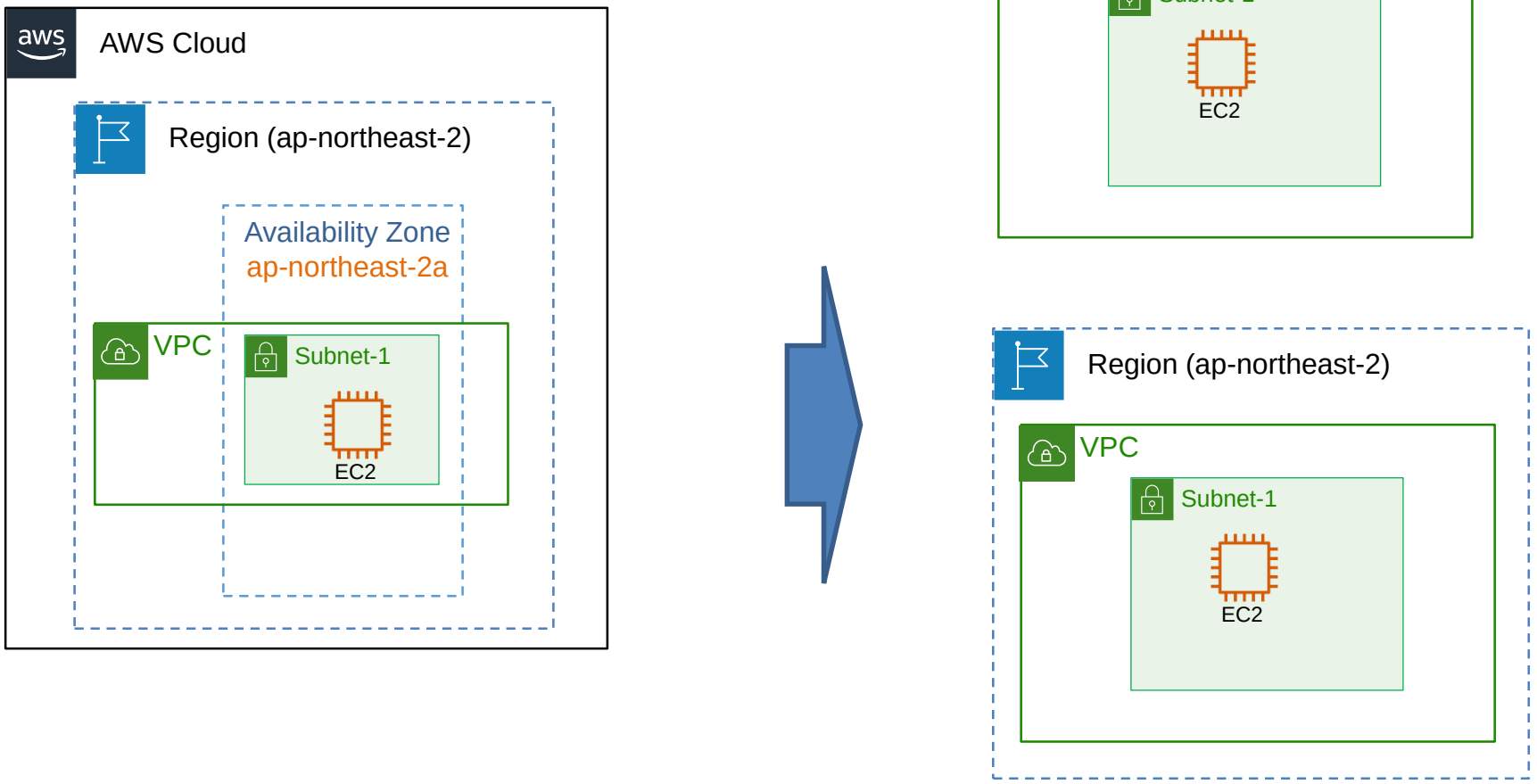


- 서울 region(ap-northeast-2)에 계정을 생성하면, 별도의 작업을 하지 않아도 기본 VPC 네트워크 플랫폼이 구성됨
- 가령, 사용자가 가용영역 (ap-northeast-2d)에 instance 레벨의 서비스(예: EC2)를 생성하면 네트워크 인터페이스가 자동 생성
- 네트워크 인터페이스에 보안 그룹을 연결하고, NACL과 라우팅 테이블을 설정하면 통신 가능

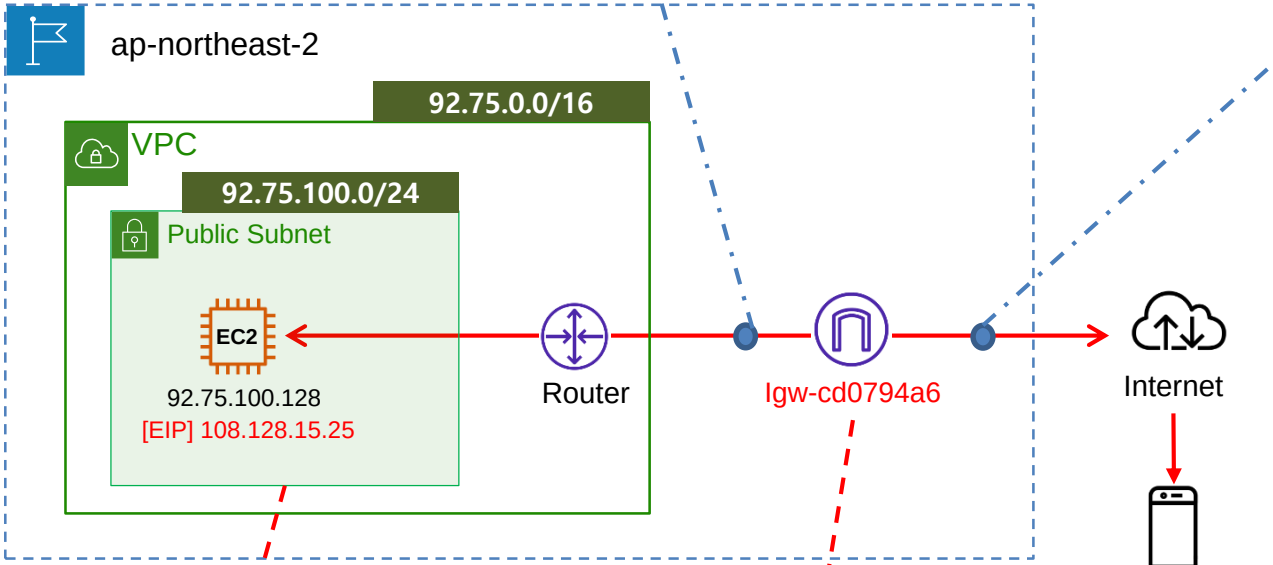
※ AWS 계정을 만들면 global 모든 region에 기본 VPC가 생성되고 불필요한 VPC 리소스가 무분별하게 생성됨

※ 보안 강화 측면에서 AWS 기본 VPC는 삭제하고 별도 VPC를 생성해 작업할 것을 권고

Internet Gateway



Internet Gateway의 NAT 기능



Source	Destination	Data
92.75.100.128	122.248.2.9	

Source	Destination	Data
108.128.15.25	122.248.2.9	

Destination	Target
92.75.0.0/16	Local
0.0.0.0/0	Igw-cd0794a6

Routing Table

IGW NAT Table

Original IP	Translated IP
92.75.100.128	108.128.15.25

IGW 동작 순서

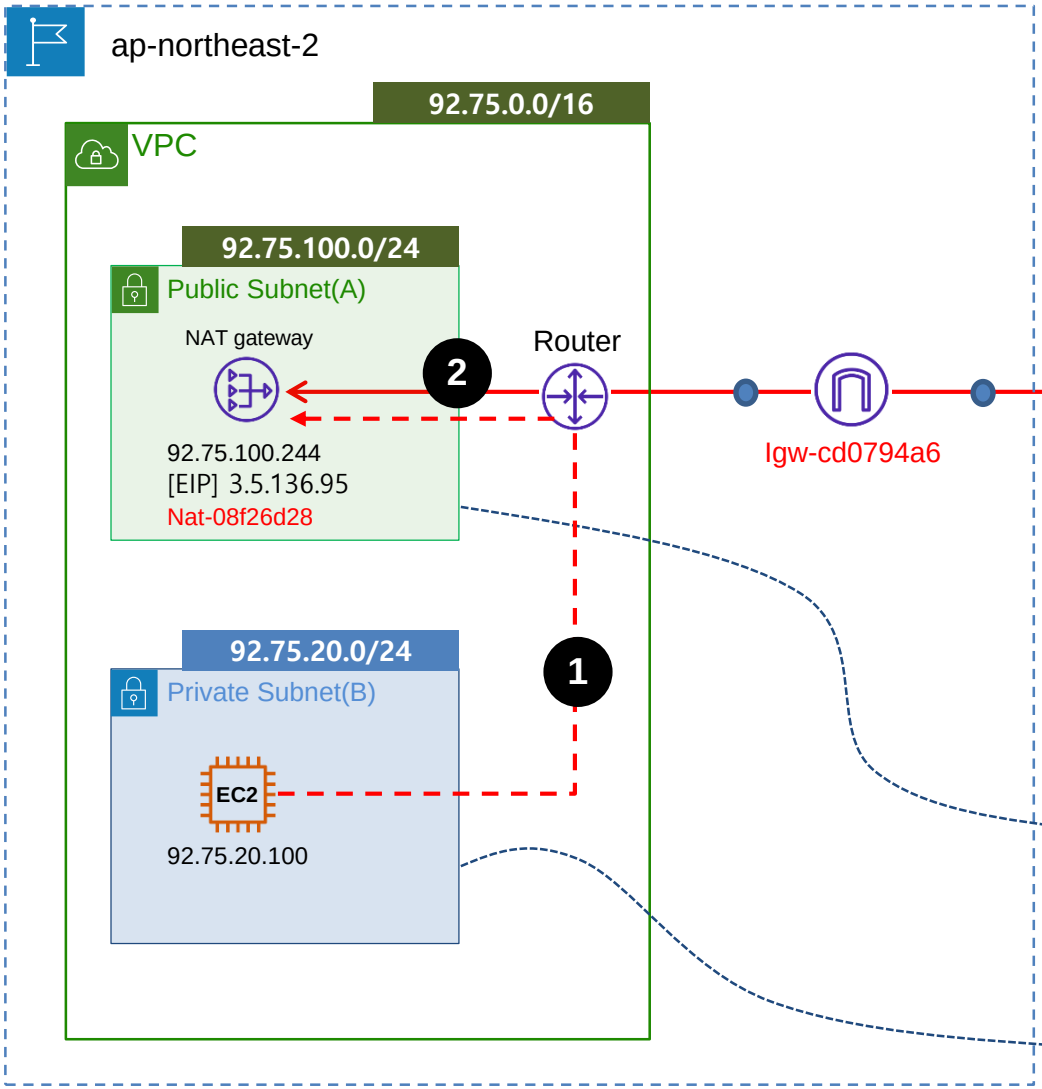
① EC2(92.75.100.128) instance가 public IP 108.128.15.25(EIP)와 연결되면 IGW는 두 IP를 NAT 테이블에 저장함

② EC2(92.75.100.128) instance가 122.248.2.9로 트래픽 전달 요청

③ Subnet 라우팅 테이블 정보에 따라 트래픽을 IGW를 경유시킴

④ IGW는 92.75.100.128(Source IP)를 NAT 테이블에서 찾아 Source IP를 매핑된 IP(122.248.2.9)로 변환하여 트래픽을 외부 망으로 전송

Internet Gateway와 NAT Gateway



NAT Gateway 동작 순서

① EC2(92.75.20.100) instance가 122.248.192.71 연결 요청

② Subnet(B)의 라우팅 테이블 정보에 따라 트래픽을 NAT를 경유시킴

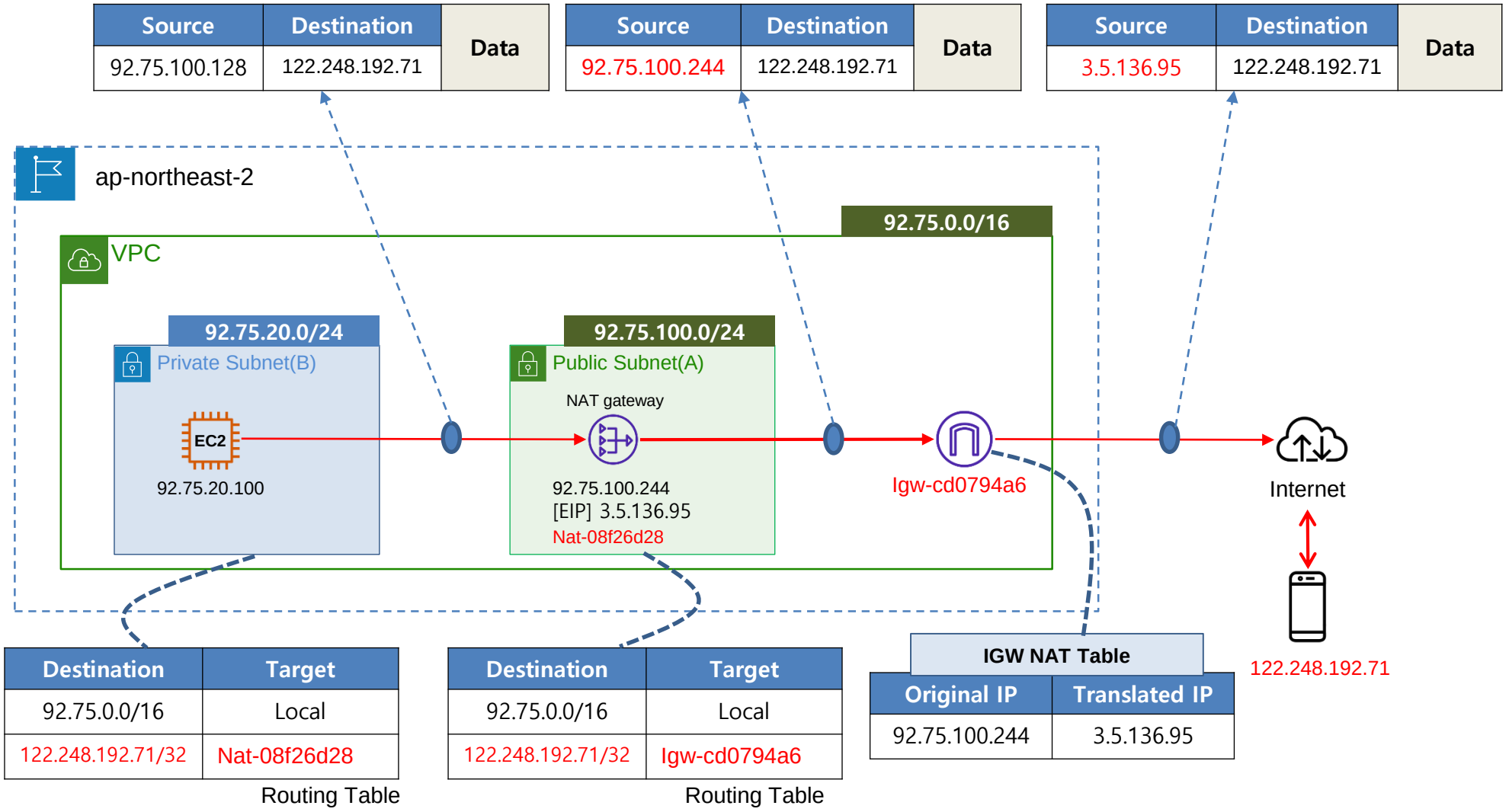
③ NAT는 Subnet(A)의 라우팅 테이블 정보에 따라 트래픽을 IGW를 경유시킴

Routing Table

Destination	Target
92.75.0.0/16	Local
122.248.192.71/32	Igw-cd0794a6

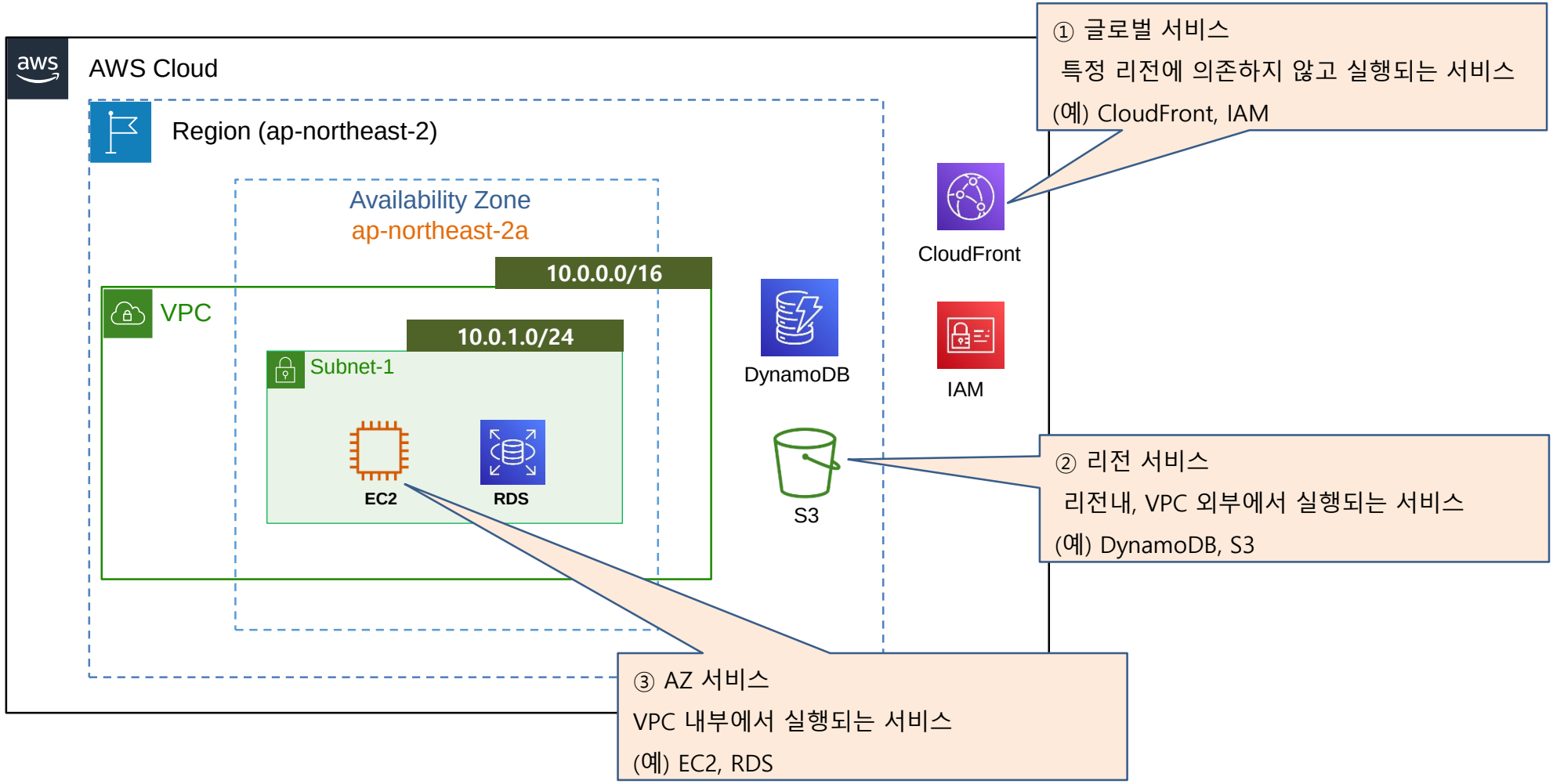
Destination	Target
92.75.0.0/16	Local
122.248.192.71/32	Nat-08f26d28

Internet Gateway와 NAT Gateway



※ VPC와 AWS 서비스

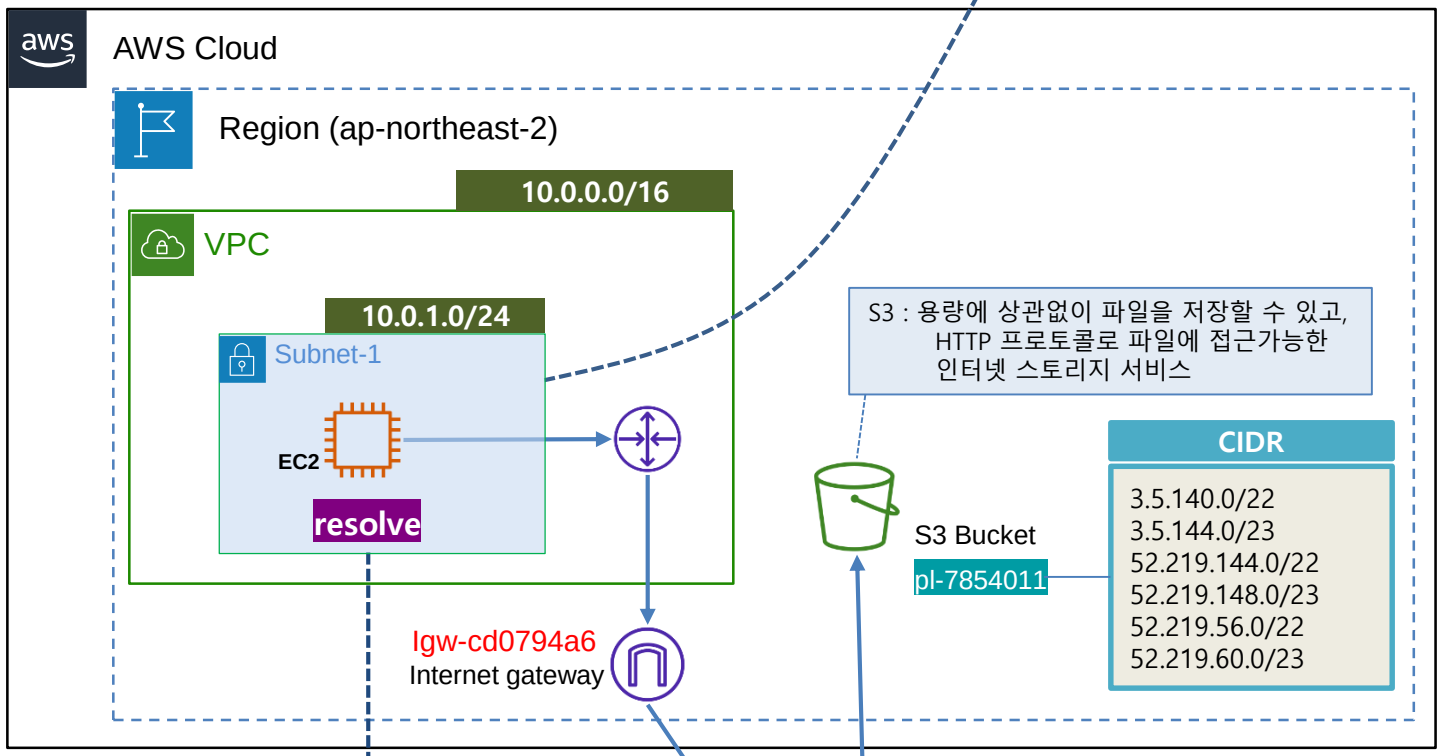
- AWS 서비스는 실행 위치에 따라 3가지 유형으로 구분 가능



※ VPC와 AWS 서비스

Routing Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Igw-cd0794a6



Domain Name	Resolved IP
s3.ap-northeast-2.amazonaws.com	52.219.144.65

Amazon S3 서비스 (리전 서비스)

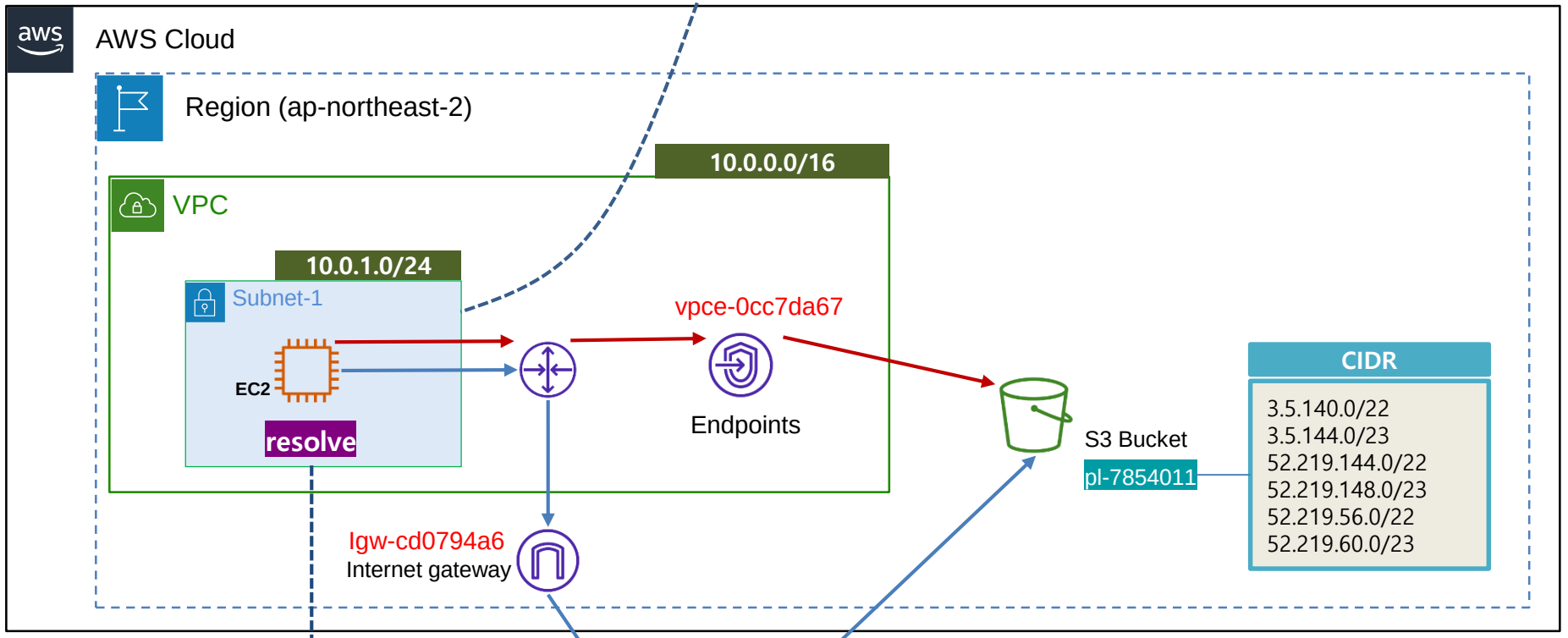
① S3는 리전 내, VPC 외부에서 실행되는 리전 서비스임
② S3 액세스는 여러 CIDR 블록으로 가능(pl-7854011)
③ EC2에서 서울 리전의 S3(s3.ap-northeast-2.amazonaws.com)에 접속하기 위해 DNS 요청하면 S3에 해당 public IP(52.219.144.65) 응답
④ S3(52.219.144.65) 접속을 위해서는 IGW를 통해(인터넷) 접속함

- **인터넷 데이터 송신 요금**
- **NAT 사용시 시간당 비용**
- **보안상 문제(0.0.0.0/0)**

※ VPC와 AWS 서비스

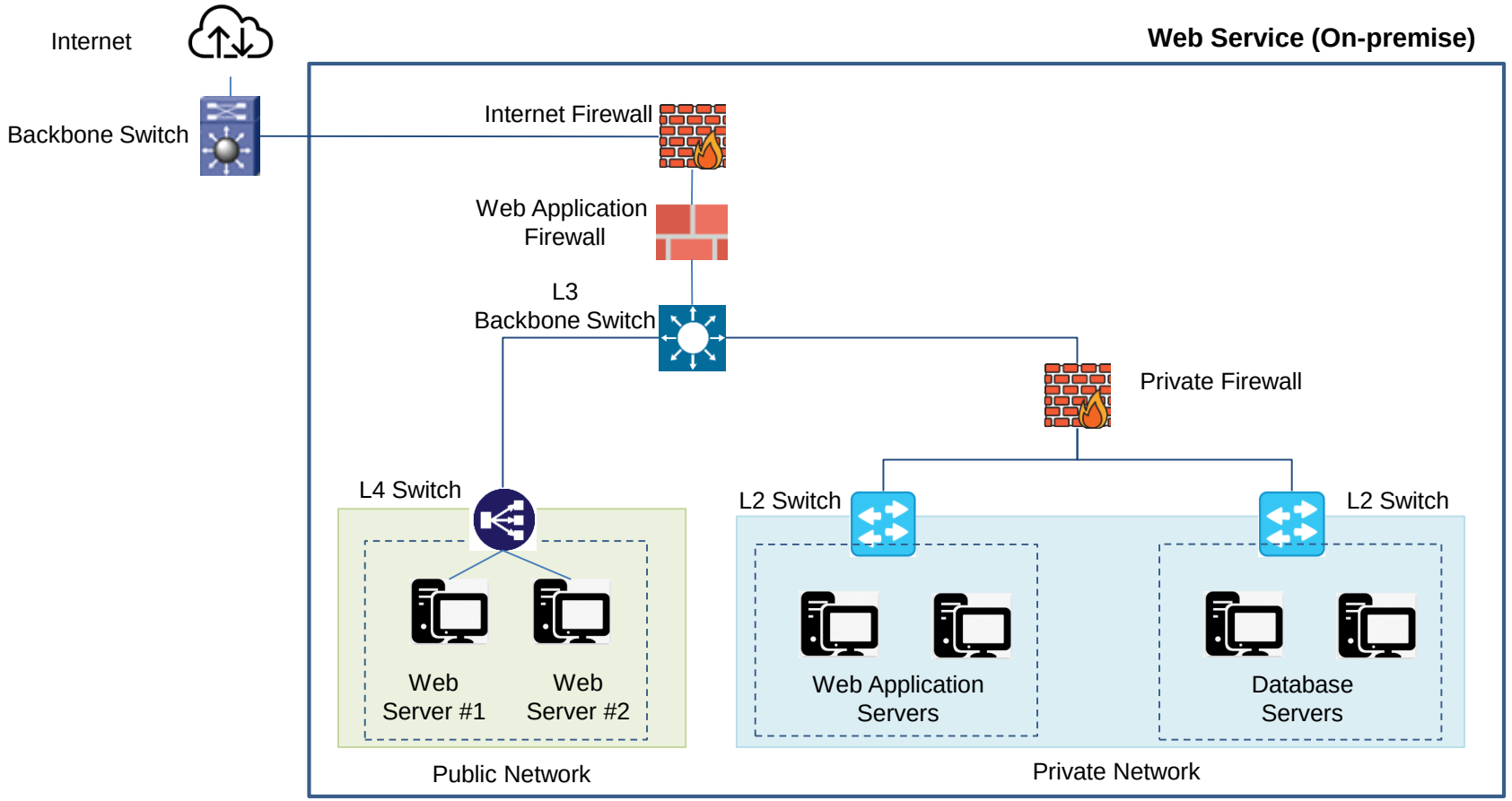
Routing Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Igw-cd0794a6
Pl-7854011	vpce-0cc7da67

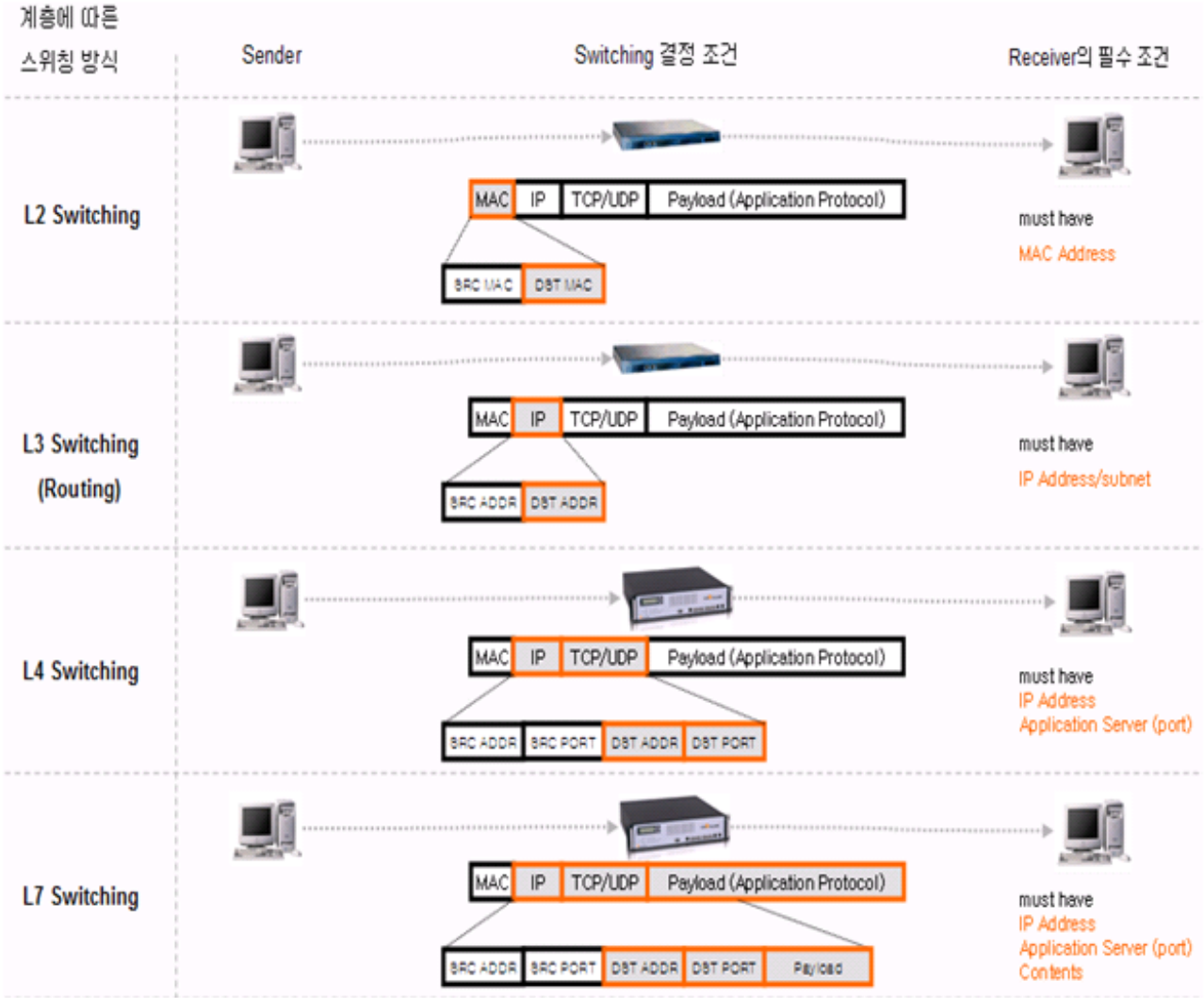


Domain Name	Resolved IP
s3.ap-northeast-2.amazonaws.com	52.219.144.65

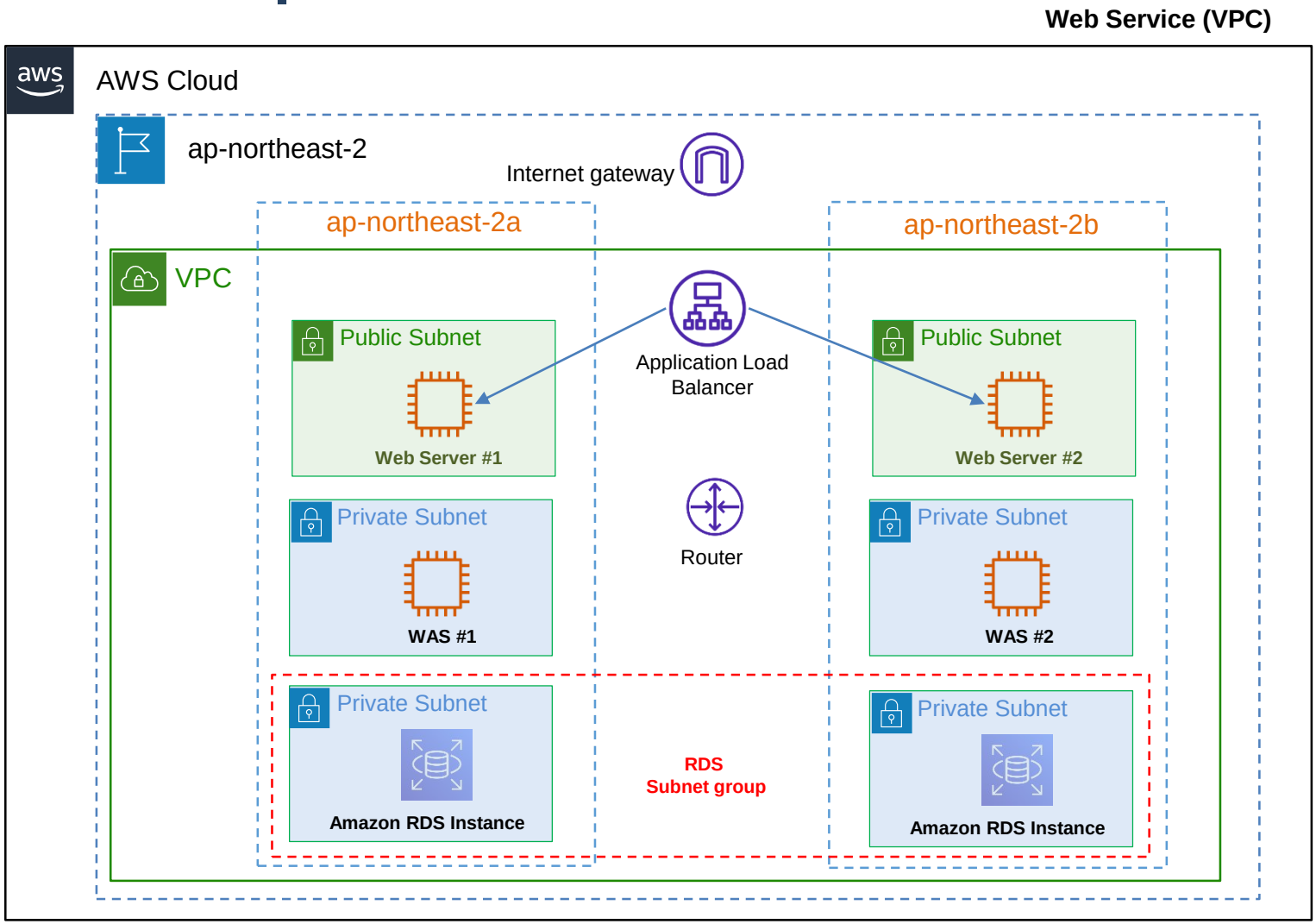
※ VPC와 On-premise 비교



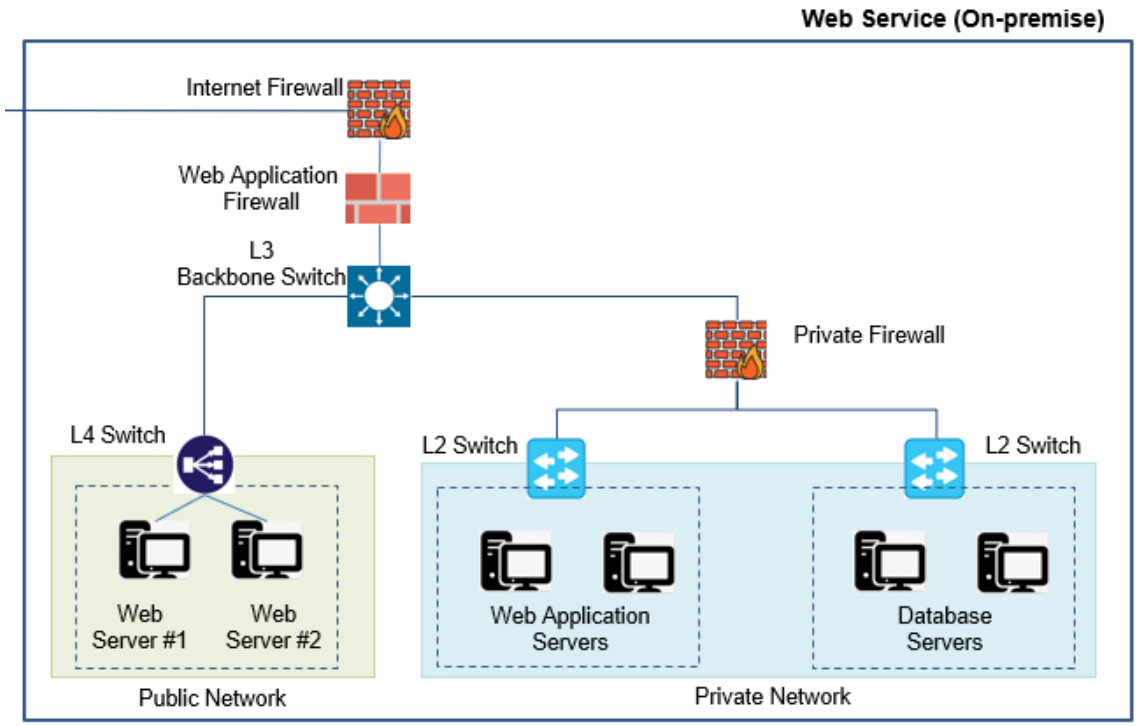
※ Layer Switch

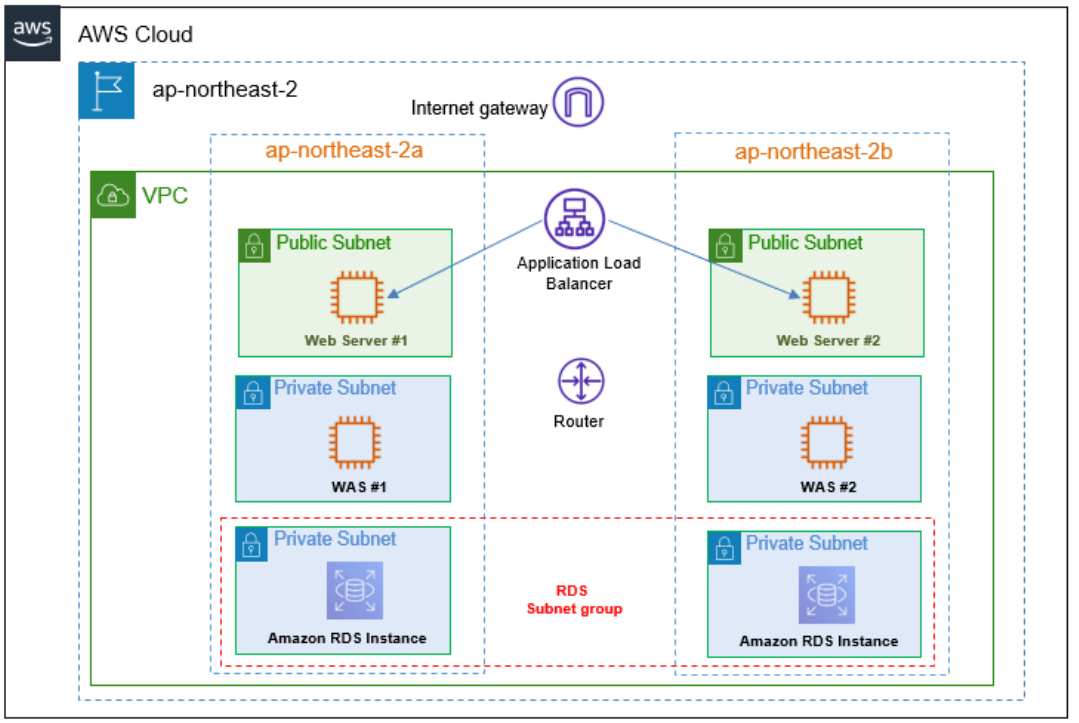


※ VPC와 On-premise 비교



AWS 네트워킹 원리



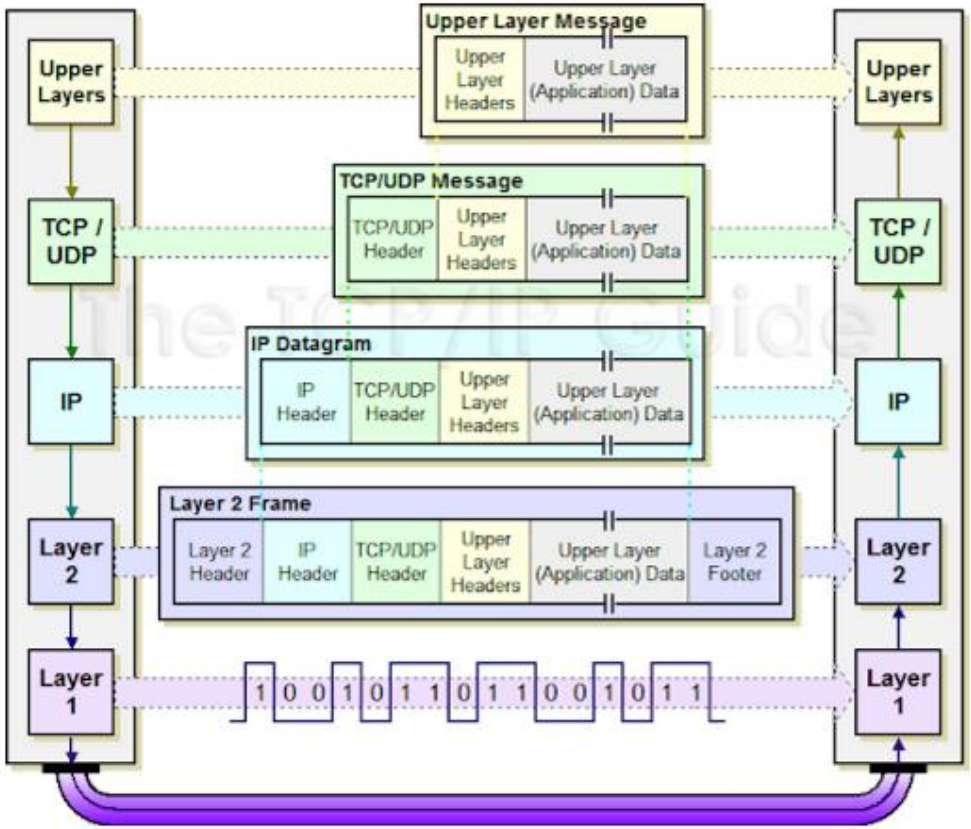


On-premise	AWS Cloud
L4 Switch	Load Balancer
Firewall	보안그룹(SG: Security Group), NACL
L3 Backbone Switch	Router (Routing Table)

통신 Protocols

TCP와 UDP

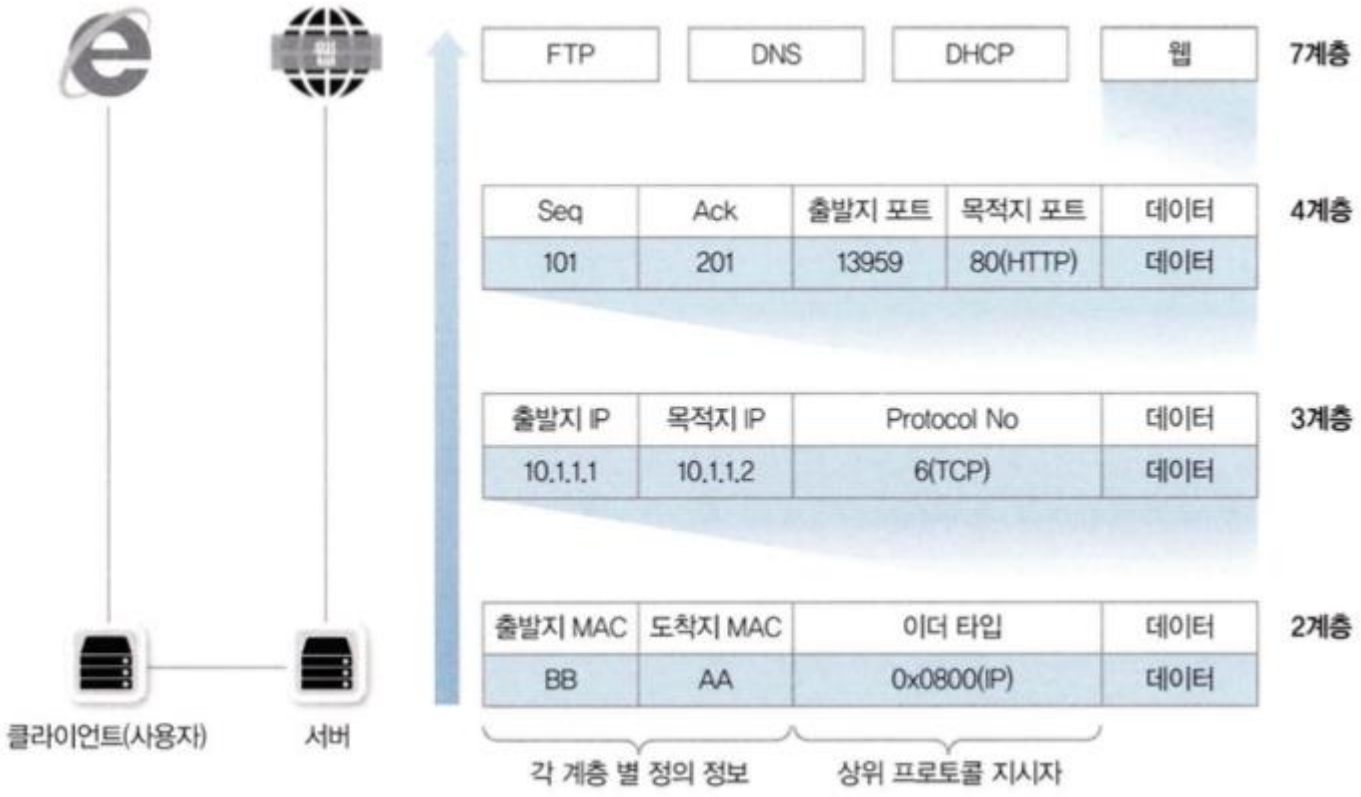
- 2계층(MAC 주소), 3계층(IP 주소)의 목적은 목적지를 정확히 찾아가기 위한 주소 제공
- 4계층(port 번호)의 목적은 목적지 호스트에서 동작하는 여러 응용 프로세스 중 통신할 목적지 프로세스를 찾아가고, 패킷 순서가 바뀌지 않도록 조합하여 원래 데이터를 잘 만드는 목적



각 계층에서 정의하는 정보와 프로토콜 지시자

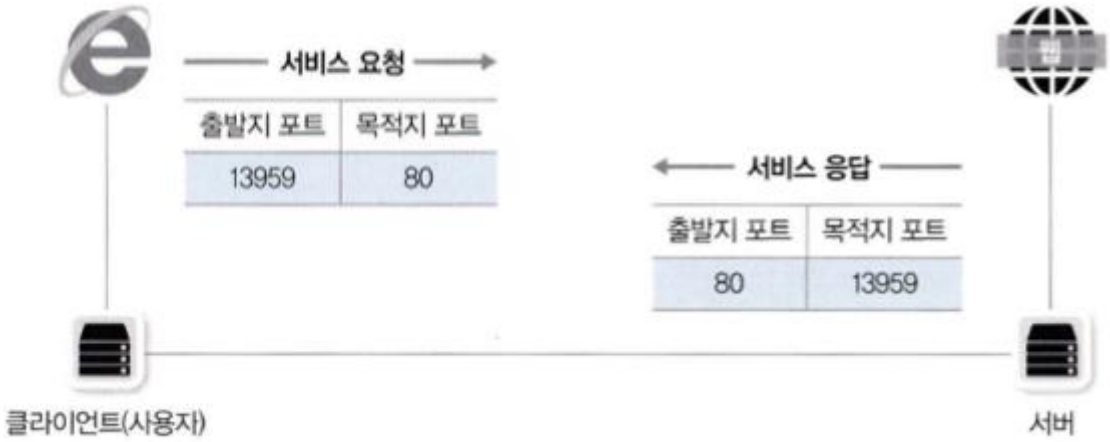
TCP와 UDP

- 4계층 프로토콜(TCP, UDP)과 서비스 포트



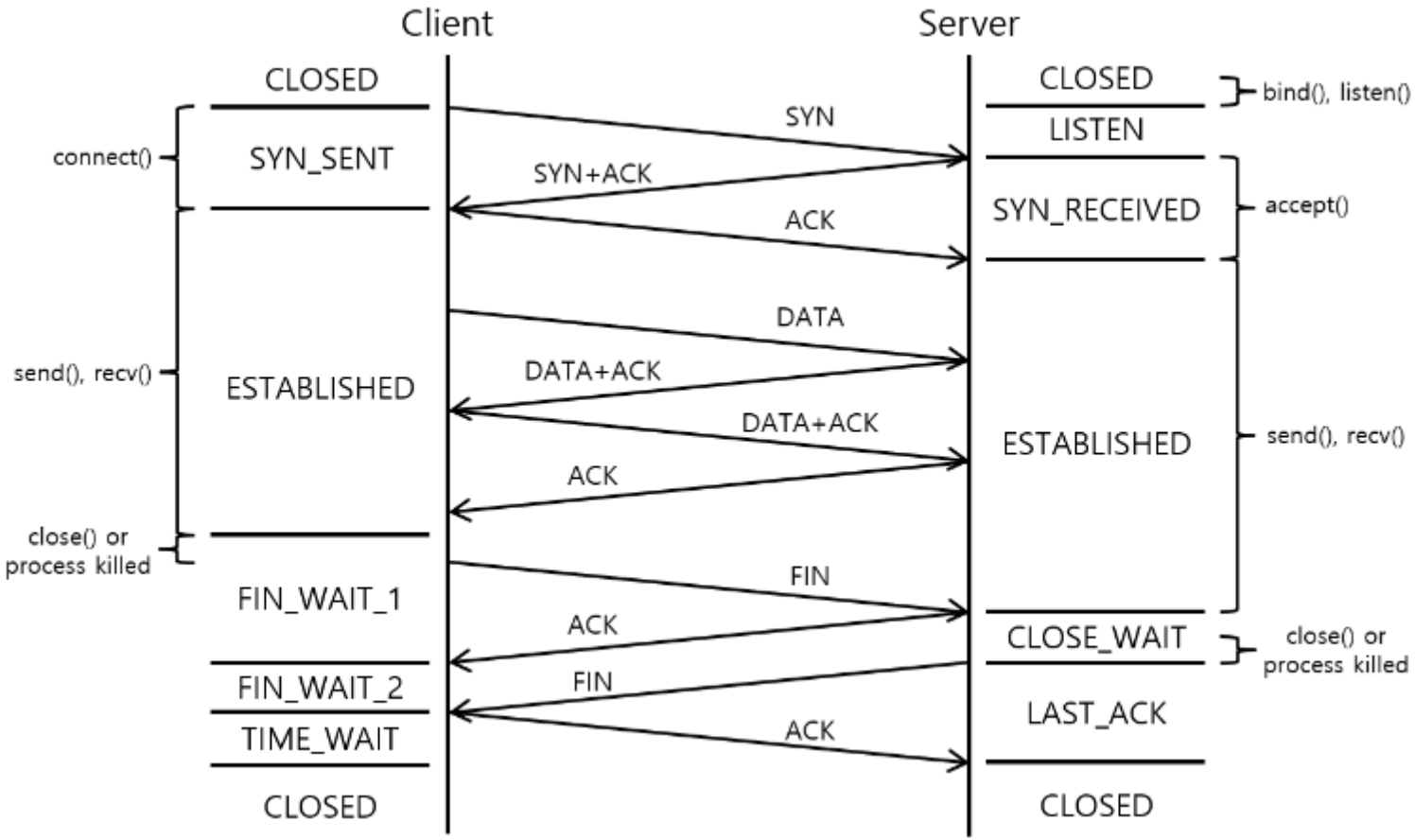
TCP와 UDP

- 4계층 프로토콜(TCP, UDP)과 서비스 포트



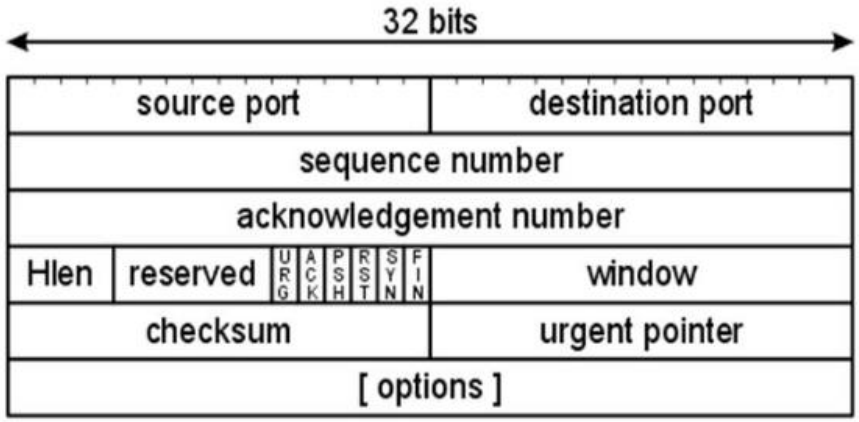
TCP와 UDP

- TCP – connection 연결 / 3 way-handshake



TCP와 UDP

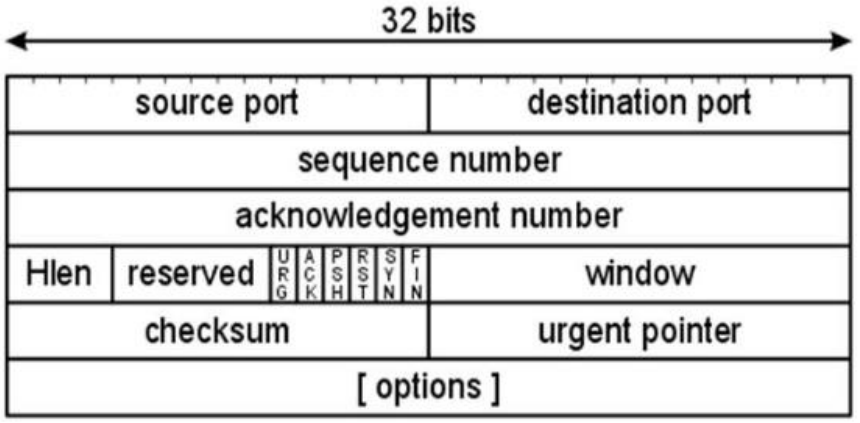
- TCP Header



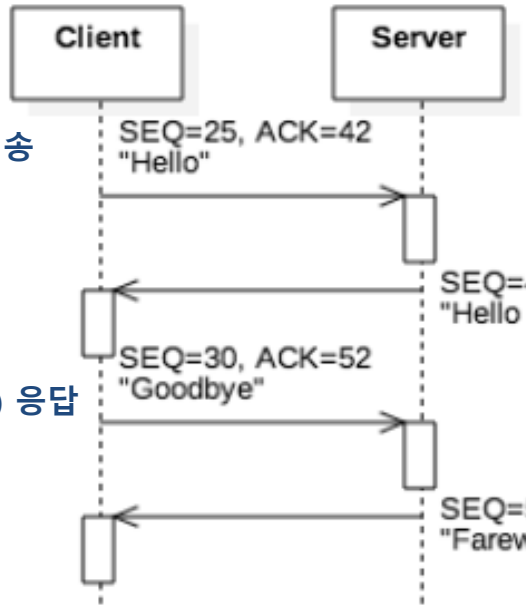
TCP 헤더

TCP와 UDP

- TCP Header



TCP 헤더



- SEQ 25 "Hello"(5자) 전송
  ACK 42

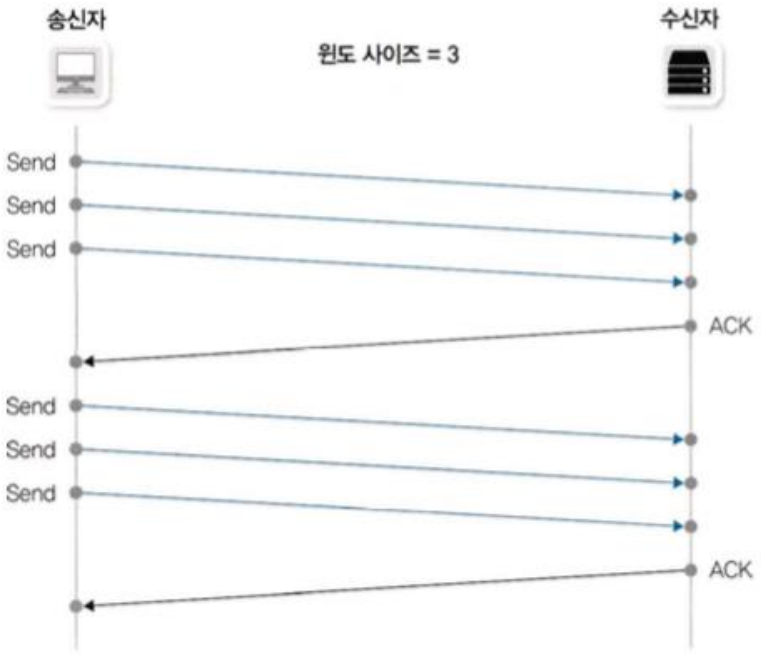
- ACK 30에 대한 응답 의미로 SEQ 30로 응답
  "Goodbye"(7자) 전송
- SEQ 42 데이터 수신 의미로 ACK 52(42+10자) 응답

- ACK 42에 대한 응답 의미로 SEQ 42로 응답
  "hello back"(10자) 전송
- SEQ 25 데이터 수신 의미로 ACK 30(25+5글자) 응답

- ACK 52에 대한 응답 의미로 SEQ 52로 응답
  "Farewell"(8자) 전송
- SEQ 30 데이터 수신 의미로 ACK 37(30+7자) 응답

TCP와 UDP

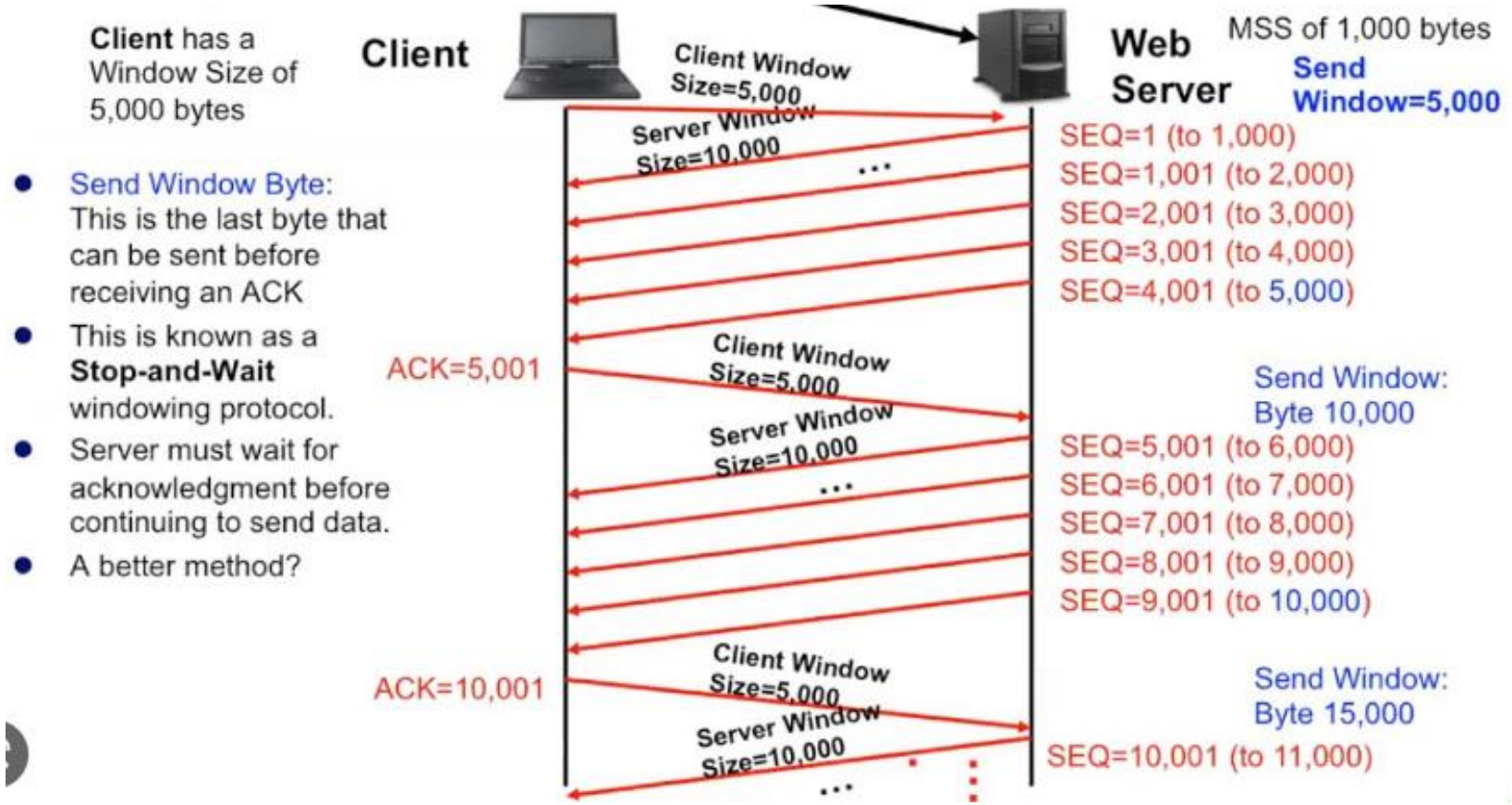
- TCP – 윈도우 사이즈와 슬라이딩 윈도우



- TCP는 일방적으로 패킷을 보내는 것이 아니라 상대방이 잘 받았는지 확인하기 위해서 ACK번호를 확인하고 다음 패킷을 전송합니다.
- 이러한 패킷을 주고받는 과정에서 통신시간이 늘어나며, 송신자와 수신자 거리가 멀 경우 왕복 지연시간이 더욱 길어집니다.
- 이때 작은 패킷 하나를 보내고 응답한다면 모든 데이터를 주고받는데 긴 시간이 걸릴 것입니다.
- 그래서 데이터를 보낼 때는 한 패킷만 보내는 것이 아닌 많은 패킷을 한번에 보내고응답은 하나만 받습니다.
- 네트워크 상대가 안좋아 패킷이 유실될 가능 성이 있으므로 적절한 송신량을 결정해야 하는데, 이때 한번에 데이터를 받을 수 있는 크기를 윈도사이즈라 합니다.
- 그리고 네트워크 상황에 따라서 이 윈도 사이즈를 조절하는 것을 슬라이딩 윈도라 합니다.

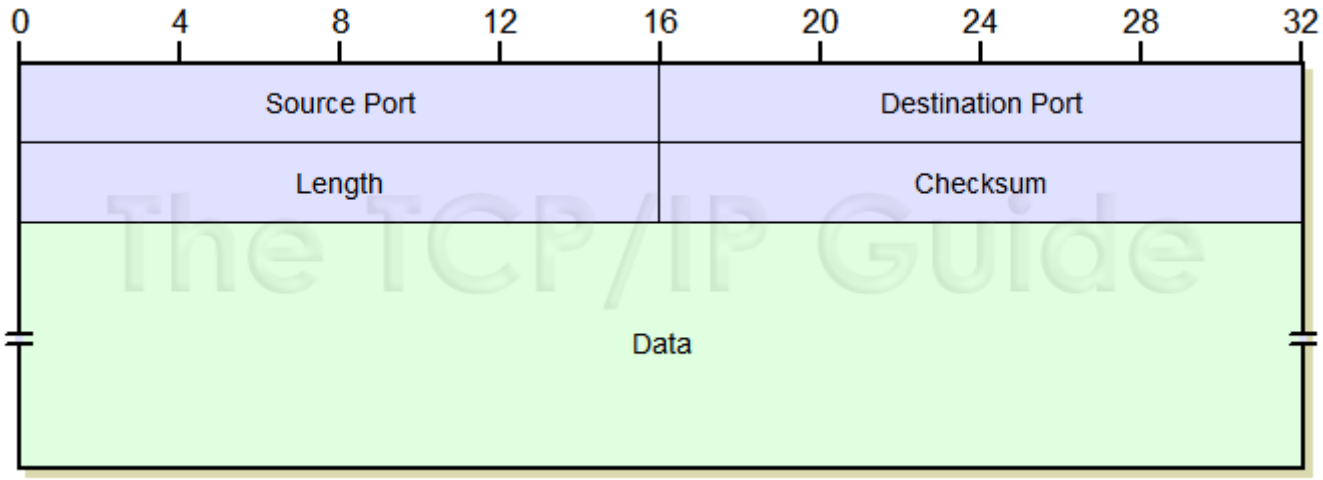
TCP와 UDP

- TCP – 윈도우 사이즈와 슬라이딩 윈도우



TCP와 UDP

- UDP



UDP 헤더

- UDP는 신뢰성 통신 (seq#, ACK 번호, Flag, Window size) 을 제공하지 않음
- 음성 데이터나 실시간 스트리밍 같이 시간에 민감한 응용 서비스에 적용
- 사내 방송이나 증권 시세 데이터 전송에 사용 되는 멀티캐스트 등 단방향

TCP와 UDP

TCP	UDP
연결지향 (Connection Oriented) - 패킷 순서 유지	비연결형 (Connectionless) - 패킷 순서 바뀜 가능
오류제어 수행 (사본 재전송)	오류제어 수행 안함
흐름제어 수행 (흐름의 양 제어))	흐름제어 수행 안함
데이터 전송	실시간 트래픽 전송

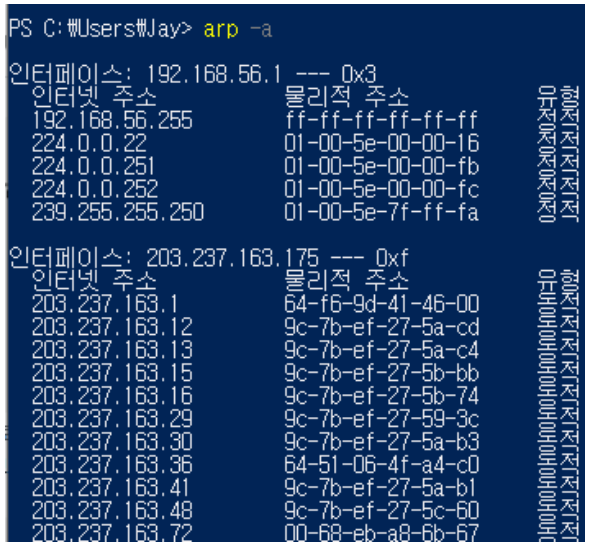
ARP

- MAC 주소 : 하드웨어 생산 업체가 임의로 할당한 주소로, 2 계층 통신에 사용하는 주소
- IP 주소 : 사용자가 직접 할당(또는 DHCP 자동 할당)한 주소로, 3계층 통신에서 사용하는 주소
- ARP(Address Resolution Protocol) :
  - IP 주소로 부터 MAC 주소를 알아내기 위해 사용하는 프로토콜
  - 실제 통신은 IP 주소를 기반으로 일어나고, MAC 주소는 ARP를 통해 자동으로 알아냄

ARP

- ARP 란 ?

- ARP 테이블
  - ARP를 사용하여, 네트워크의 도착지 IP 주소로 부터 도착지 MAC 주소를 알아냄(학습)
  - 도착지 MAC 주소를 알아내기 위해 매번 ARP를 사용하는 것은 비 효율적
  - 네트워크 통신 효율을 위해 ARP로 학습한 IP 주소에 대한 MAC 주소를 메모리에 저장
  - ARP 테이블 내용은 일정시간 통신이 없으면 자동 삭제(논리 주소는 바뀔 수 있음)



※ 윈도우에서 ARP 테이블 확인 : > arp –a

- ARP를 통해 매핑된 IP 주소와 MAC 주소의 경우 유형 “동적 "

ARP

- ARP 동작

① ping 통신 수행 시도 : > ping 1.1.1.2

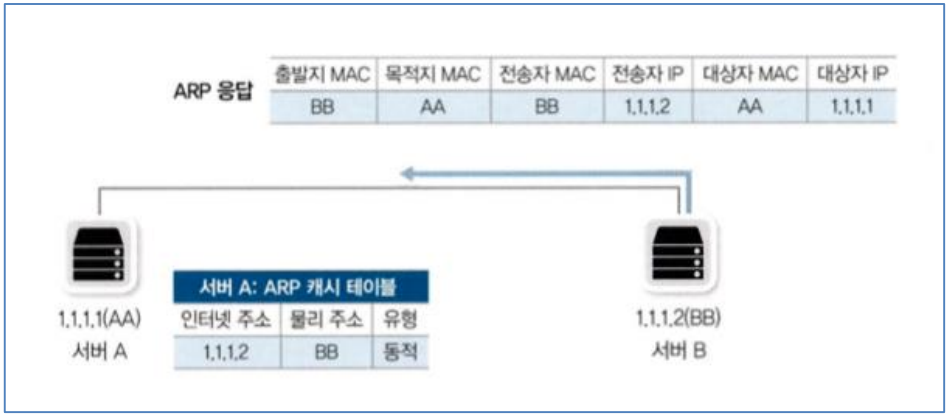
- 서버 A(1.1.1.1)가 서버 B(1.1.1.2)로 통신하려고 할 때, 목적지 MAC 주소를 알 수 없음

② ARP request

- 목적지(1.1.1.2)의 MAC 주소를 알아내기 위해 ARP 요청 패킷을 같은 네트워크에 broadcast
- 출발지 MAC 주소는 자신의 MAC 주소, 도착지 MAC 주소는 (00:00:00:00:00:00)로 채워 보냄
- ARP request 메시지는 같은 네트워크 대역의 단말로 broadcast

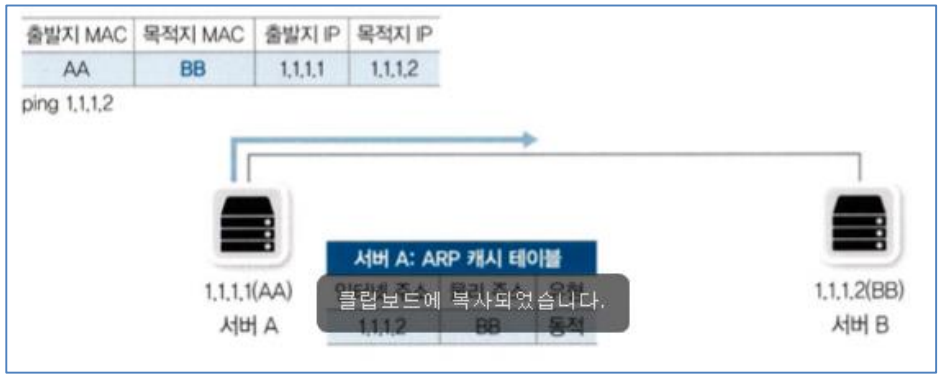
ARP

- ARP 동작



③ ARP response

- ARP 요청 패킷을 같은 네트워크 안의 모든 단말이 수신함
- **ARP request 패킷의 대상지 IP가 자신인 경우만 ARP request에 응답함**
- ARP response에는 출발지 MAC , 목적지 MAC 주소를 모두 채워 응답
- ARP response 패킷은 **unicast** 통신임
- 서버 A는 ARP response를 받아 자신의 **ARP 캐시 테이블을 갱신함** (ARP 캐시 테이블은 일정 시간만 유지된 후 통신이 없으면 삭제 됨)



④ ping 통신 수행

- 알아낸 도착지 MAC 주소로 패킷을 완성해 ping 패킷을 보냄

ARP

- GARP 동작

- 1. (못마땅함) 불필요한, 쓸데없는,
- 2. 무상의

- **GARP (Gratuitous ARP)**
  - **자신의 IP와 MAC 주소를 로컬 네트워크에 알릴 목적으로 사용**
  - **송신자 IP, MAC 주소에는 자신의 IP와 MAC 주소로 채우고, 대상자 IP에도 자신의 IP로 채움.**
    대상자 MAC 주소는 0으로 표기(00:00:00:00:00:00)하여 네트워크에 브로드캐스트함
  - **송신자와 대상자 IP 모두에 송신자 IP를 채워 보냄**

- **GARP를 사용하는 경우**
  - **IP 주소 충돌 감지**
  - **동일 서브넷 상의 상대방 ARP 테이블 갱신**
  - **HA(고가용성) 용도의 클러스터링, VRRP, HSRP**

ARP

- GARP 동작

- 1. (못마땅함) 불필요한, 쓸데없는,
- 2. 무상의

- **GARP (Gratuitous ARP)**
  - **자신의 IP와 MAC 주소를 로컬 네트워크에 알릴 목적으로 사용**
  - **송신자 IP, MAC 주소에는 자신의 IP와 MAC 주소로 채우고, 대상자 IP에도 자신의 IP로 채움.**
    대상자 MAC 주소는 0으로 표기(00:00:00:00:00:00)하여 네트워크에 브로드캐스트함
  - **송신자와 대상자 IP 모두에 송신자 IP를 채워 보냄**

ARP

- GARP 동작 - IP 주소 충돌 감지

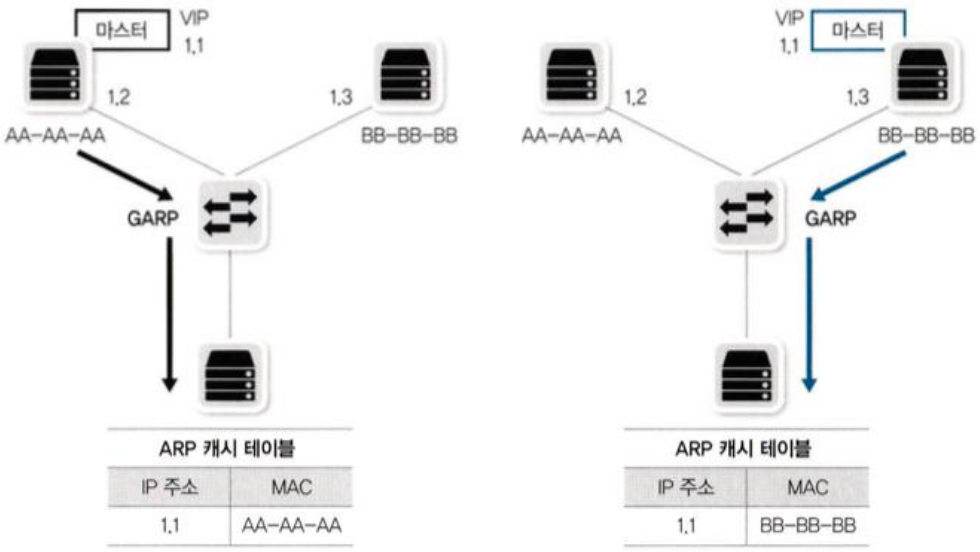
GARP request(발신, 수신 IP 모두 자신의 IP)에 누군가 ARP response를 한다면,
ARP response를 한 단말은 나와 동일한 IP를 가진 것임

- 자신에게 할당된 IP를 동일 네트워크에서 다른 단말이 사용 중인지 확인
- 충돌 : GARP로 대상지 IP를 자신의 IP로 설정하여 브로드캐스트하고, 상대방에서 응답이 오는 경우

- 통상, 컴퓨터가 부팅되거나 DHCP 서버로 부터 IP 주소를 할당 받으면
  : 자신의 IP 주소가 중복되었는지 알아보기 위해
  : 자신의 IP를 목적지로 하여 요청함으로써 중복 여부를 확인

ARP

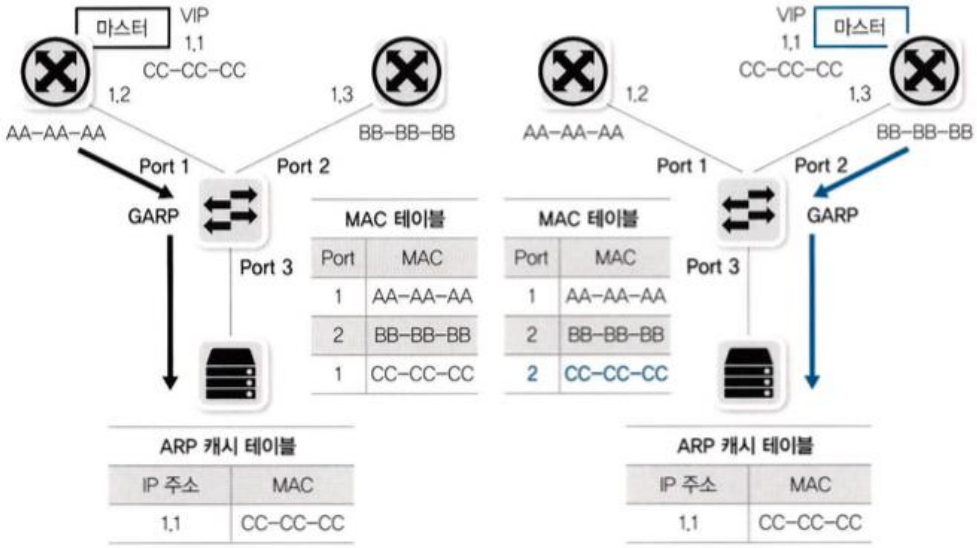
- GARP 동작 – 상대방 컴퓨터의(같은 네트워크에 있는) ARP 테이블 갱신



- HA(고가용성)을 위해 2대의 DB 서버(1.2, 1.3)을 운영하는 경우, 가상 IP(VIP)는 1.1로 서비스하고 있음
- DB 서버(1.2)가 마스터로 동작하여 ARP 캐시 테이블에는 DB 서버(1.2)의 MAC 주소 (AA-AA-AA)가 등록됨
- DB 서버(1.2) 장애로, DB 서버(1.3)이 마스터가 되면 ARP 캐시 테이블에도 DB 서버의 MAC 주소를 변경해야 함
- 새로운 AB 서버 마스터는 GARP 프로토콜로 네트워크 내 모든 PC의 ARP 캐시 테이블에 대해 자신의 MAC 주소를 갱신하도록 요청함

ARP

- GARP 동작 – 클러스터링, FHRR(VRRP, HSRP)



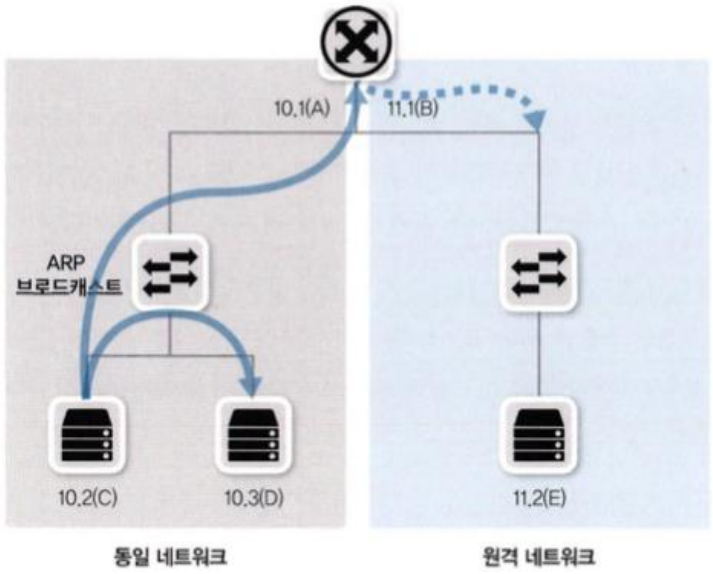
- 네트워크 장비의 MAC 테이블 갱신 목적
- 클러스터링, VRRP(Virtual Router Redundancy Protocol), HSRP(Hot Standby Router Protocol) 와 같은 FHRR(First Hop redundancy Protocol)은 가상 MAC을 사용하여 이중화
- 마스터 라우터가 변경되는 순간
  - 단말의 ARP 캐시 테이블은 가상 MAC을 사용하므로 갱신이 필요 없음
  - 스위치의 MAC 테이블은 갱신이 필요함

서브넷과 게이트웨이

- 초기 네트워크는 모든 단말이 하나의 로컬 네트워크(LAN)로 설계됨
- 이후, 로컬 네트워크들이 하나의 큰 네트워크로 묶이고, 다른 LAN 간의 통신이 중요해 짐
- 게이트웨이 (Gateway) :
  - 원격지 네트워크(다른 LAN)과의 통신에 사용 하는 장비
  - 3계층 장비(라우터와 L3 스위치)가 게이트웨이 역할 수행

서브넷과 게이트웨이

- 서브넷과 게이트웨이의 용도



- 로컬 네트워크에서는 ARP Broadcast를 이용하여 도착지 MAC 주소를 학습하여 통신 가능
- ARP Broadcast 통신은 원격 네트워크로 전달되지 않아 통신을 위해 네트워크 장비의 도움이 필요
- 이 장비를 게이트웨이라고 부름

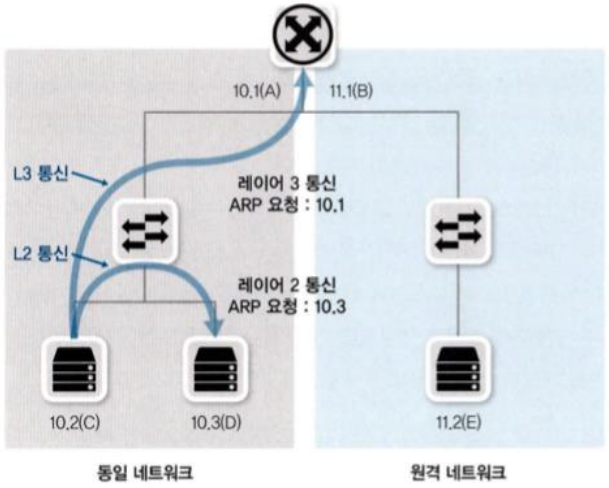
동일 네트워크에서의 통신이냐? 원격 네트워크과의 통신이냐? 에 따라 통신 방법이 달라짐

➡ **목적지가 자신과 동일한 네트워크인지 확인하는 작업이 필요 (서브넷 마스크)**

서브넷과 게이트웨이

- 2계층 통신 vs 3계층 통신

- 2계층 통신 (로컬 네트워크 통신), 3계층 통신 (원격지 네트워크 통신)



목적지 MAC	출발지 MAC	출발지 IP	목적지 IP	
D	C	10.2	10.3	로컬 통신

목적지 MAC	출발지 MAC	출발지 IP	목적지 IP	
A	C	10.2	11.3	원격 통신

- 2계층 통신 (로컬 네트워크 통신) : 동일 네트워크 단말간 통신일 경우, ARP 브로트캐스트를 이용하여 **상대방 MAC을 알아낸 뒤 직접 통신**
- 3계층 통신 (원격지 네트워크 통신) : 원격지 네트워크의 단말과 통신할 경우, ARP 브로트캐스트를 이용하여 **기본 게이트웨이 MAC을 알아낸 뒤 게이트웨이와 통신**

※ 스푸핑 공격

스니핑 공격의 종류 – ARP 스푸핑

- **Spoofing : '속이는 것 ' MAC 주소, IP 주소, 포트 등을 속여 공격함**