

Amazon VPC(Virtual Private Cloud)

VPC란?

Amazon 사용설명서에 따르면

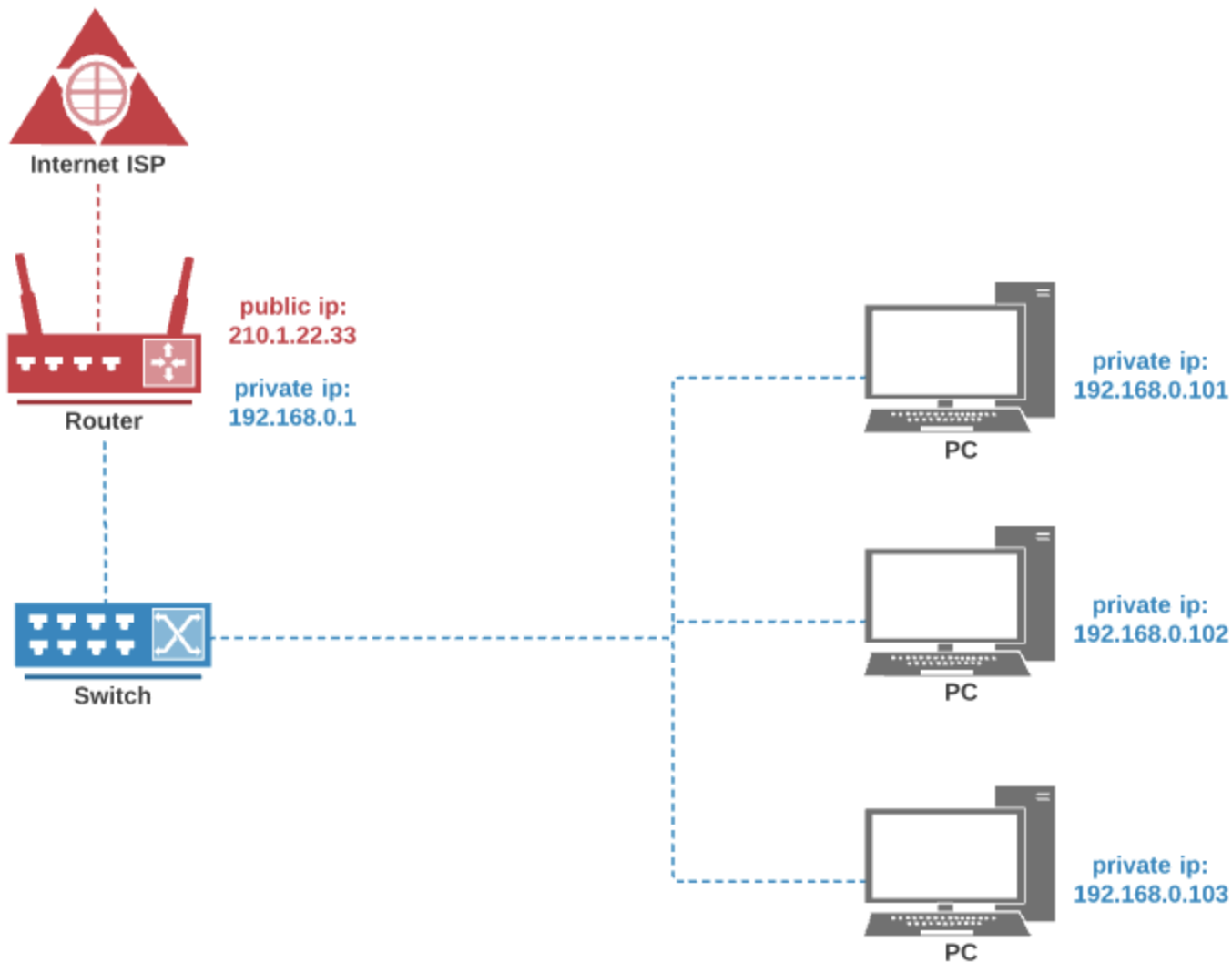
VPC는 사용자의 AWS 계정 전용 가상 네트워크를 의미한다.

그래서 그게 뭐라고...?

물리 네트워크와의 비교를 통해 araboja.

물리 네트워크

Internet ISP에 연결된 public IP(210.1.22.33)를 가정용 공유기(Router)와 스위치를 이용해 Private IP(192.168.0.0/24)로 공유해서 인터넷을 사용하는 일반적인 홈랜 네트워크 구조



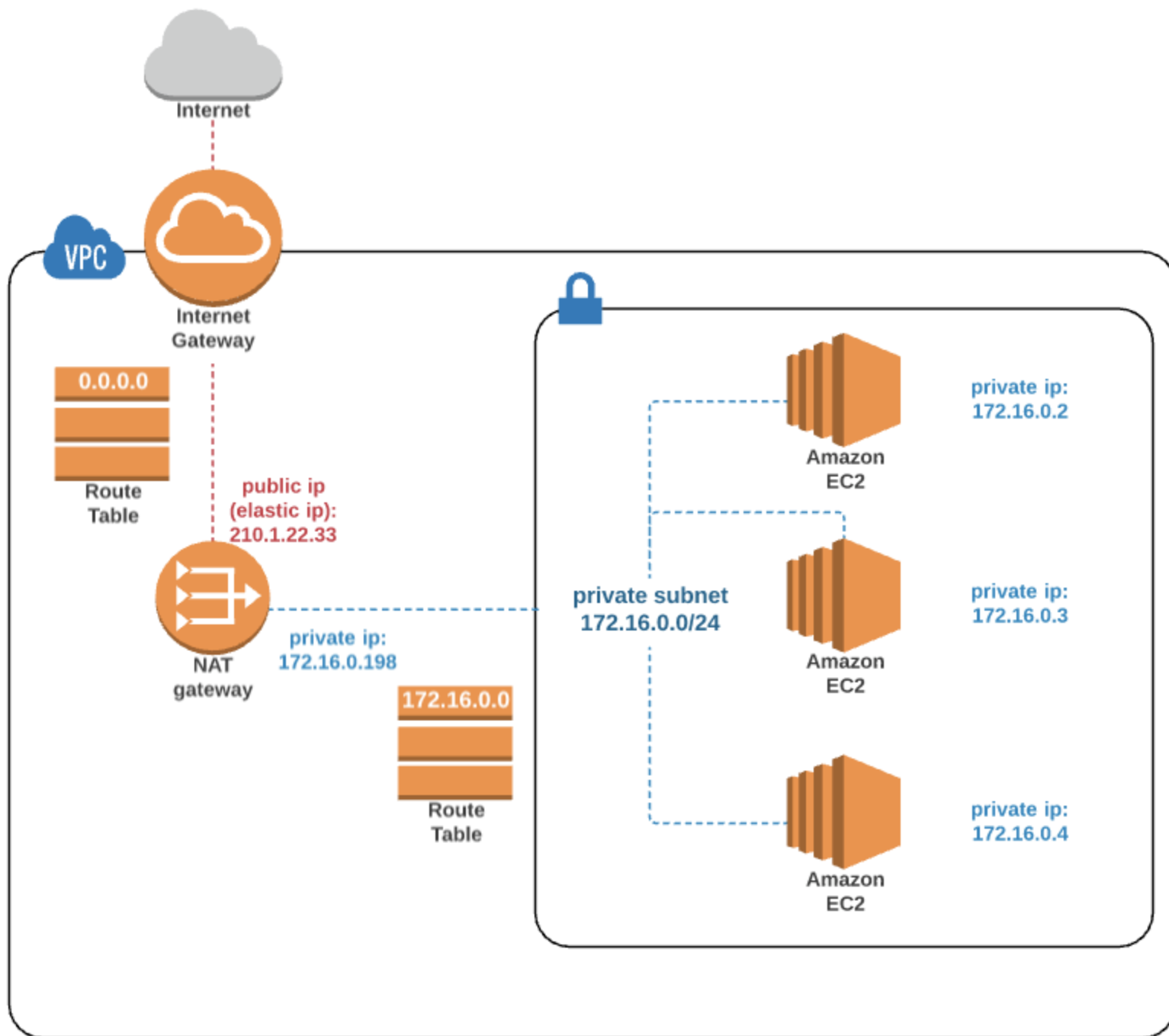
주요 기능

- 라우터(Router)
 - 서로 다른 네트워크 간의 통신을 중개한다.
- 스위치(Switch)
 - 각 포트에 연결된 MAC address를 기억한다.
 - 스위치로 들어온 요청에서 이미 기록된 destination MAC address를 읽는다.
 - 해당 MAC address로 연결된 port로 데이터를 전송한다.
- NAT(Network Address Translation)
 - 외부 네트워크와 통신할 때는 public IP를 통해서만 할 수 있다.
 - 그걸 도와준다.
 - private IP -> public IP, 혹은 반대로도 마찬가지로 마찬가지이다.

- **DHCP**(Dynamic Host Configuration Protocol)
 - 공유기에 연결되는 새로운 장비에 동적으로 IP 주소를 할당한다.
- **방화벽**(Firewall)
 - 내부로 들어오는/외부로 나가는 IP/PORT를 특정 규칙으로 통제 (*열기 or 닫기*) 할 수 있다.

물리 네트워크를 대체하는 VPC

공유기를 사용하는 물리 네트워크를 Amazon VPC resource에 매칭하면 다음과 같다.

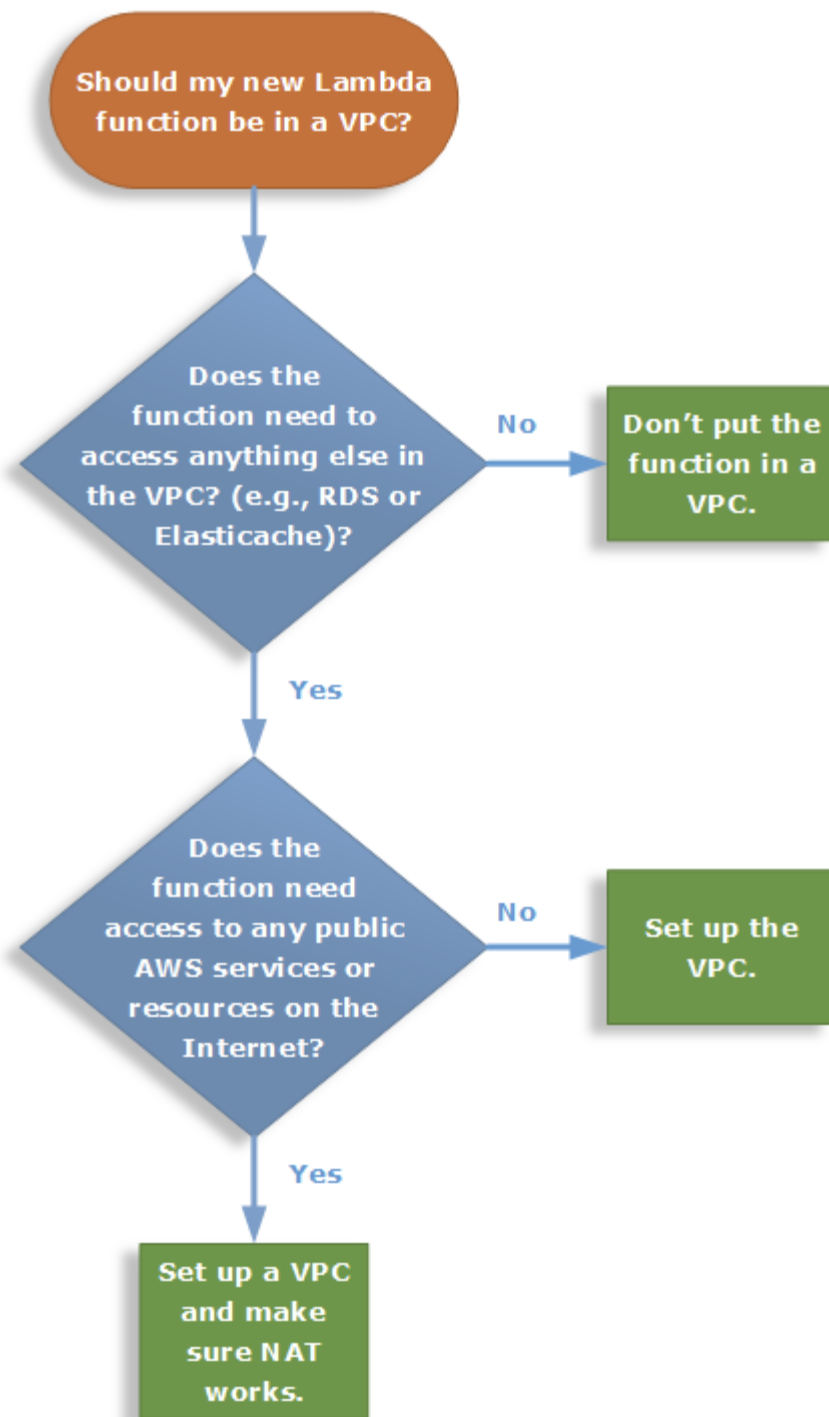


앞선 물리 네트워크의 **주요 기능**들을 각각의 AWS resource가 대신하게 된다!

- **라우터(Router)**
 - **Internet Gateway + Route Table**이 대신한다.
- **스위치, DHCP(Dynamic Host Configuration Protocol)**
 - AWS는 스위치를 별도로 구분하지 않는다.
 - **Subnet**이 스위치의 기능을 **포함**한다.
 - Subnet은 가상 머신 인스턴스가 사용할 수 있는 private IP 주소의 범위이다.
 - Subnet에 연결된 인스턴스는 기동 시 **DHCP**를 통해 private IP 주소를 할당받는다.

- **NAT**(Network Address Translation)
 - **NAT instance**나 **NAT Gateway**가 NAT를 대신한다.
- **방화벽**(Firewall)
 - **NACL**(Network ACL)과 **Security Group**이 방화벽을 대신한다.

그래서 이 VPC에 관한 지식이 **Ironmental of God Devrother** 프로젝트에 왜 필요하냐고?



감사합니다.