* Introduction to VPC Peering
- VPC 와 VPC 를 연결하는 기능
- Routing table 을 통해 VPC 간 통신이 이루어짐
- 동일 계정뿐만 아니라 다른 계정간 Peering 가능
- Public Internet 을 지나가지 않고 Amazon Backbone Newtork 를 통해 지나감
- VPC 는 서로 다른 IP 대역을 보유해야 함
- Routing table 에는 'pcx-nnnn nn'로 시작하는 Routing 이 상대방 VPC 를 Next hop 으로 잡혀있어야 함
- Transit Peering 이 지원되지 않음
    - VPC 1, VPC 2, VPC 3 가 있고, VPC 1 < - > VPC 2 < - > VPC3 형태일 경우, VPC 1 는 VPC 2 를 통해 VPC 3 로 갈 수 없음
    - VPC 1 와 VPC 3 가 통신하기 위해서는 VPC 1, VPC 3 간 Peering 이 맺어져야 함
- Transit Peering 이 지원되지 않는 이유
    - VPC 1(Account 1), VPC 2(Account 2), VPC(Account 3)가 있고 Transit Peering 이 가능한 경우
    - VPC 3 가 VPC 1 와의 통신을 원치 않아도 연결되어있기 때문에 의도하지 않은 통신이 가능해짐

* VPC Peering Design
- 문서 참조 중요! : https://docs.aws.amazon.com/ko_kr/vpc/latest/peering/peering-configurations-partial-access.html
- 공유 서비스 사례 : 모든 사용자가 접근하는 서비스(AD, File Server 등)을 둔 VPC 를 중심으로 다른 VPC 를 연결함
- Overlapping CIDR Range
    - 하나의 VPC 에 연결된 VPC A(10.0.0.0/16), B 가 같은 대역(10.0.0.0/16)을 가지고 있을 경우
    - Static routing 을 보다 구체적으로 설정하면 사용 가능(Longest match rule 적용)
    - 예를 들어, VPC A 에 대하여 Static routing 10.0.1.0/24 를 설정한다면 Longest match rule 에 의거 10.0.1.0/24 에 한해서는 VPC A 로 Routing 됨
    - 10.0.1.0/24 가 VPC B 에도 있다면 해결 불가능
- Multiple Subnet
    - Subnet 마다 각각 Routing table 을 보유한다는 것에서 착안한 설정
    - 모든 사용자가 접근하는 서비스(AD, File Server 등)을 둔 VPC 를 중심으로 동일한 CIDR 의 VPC(VPC A, VPC B)가 2 개 있을 경우

- 중심 VPC 의 Subnet 을 여럿으로 나눈 뒤, 중심 VPC 의 Subnet 1 은 VPC A 에 대한 routing(pcx-1111)을 갖게 하고 중심 VPC 의 Subnet 2 는 VPC B 에 대한 routing(pcx-2222)만을 갖게 함

* VPC Peering and Overlapping CIDR Range
- 10.0.0.0/16 VPC 2 를 중심으로 양쪽에 동일한 CIDR(192.168.0.0/16) VPC 1, VPC 3 가 있음
- VPC 1 과 VPC 3 는 동일한 IP(192.168.0.20)의 인스턴스을 보유함
- 여기까지 살펴보면 VPC 2 에서 양쪽 VPC 1, VPC 3 의 192.168.0.20 인스턴스에 접근할 수 없음
- 해결방법
    - Longest Match Rule 을 활용한 방법
    - VPC 1, VPC 3 의 Subnet 을 생성하되 VPC 1 은 192.168.1.0/24, VPC 2 는 192.168.2.0/24 로 생성
    - VPC 1 의 192.168.0.20 인스턴스를 192.168.1.20 로 변경함, VPC 3 의 192.168.0.20 인스턴스를 192.168.2.20 으로 변경함
    - VPC 2 에서 각각에 대한 Routing 을 2 개 생성하여 사용하면 통신 가능

* VPC Peering and DNS Resolutions
- VPC Peering 상태에서 DNS Query 시 발생가능한 문제점
- 상황 가정
    - VPC 1 의 Bastion host EC2 1 은 Public IP 를 소유하고 있으나 Public DNS 는 없음
    - VPC 2 의 Bastion host EC2 2 는 Public IP 를 소유하고 있고 Public DNS 소유하고 있음
- 상황 재현
    - VPC 1 의 Bastion host 에서 'nslookup' query 를 실행하면 결과값으로 EC2 2 의 Public IP 를 받아옴
    - 해당 IP 를 사용할 경우 공인 IP 이므로 VPC Peering 이 아닌 외부 인터넷을 경유하여 VPC 2 의 EC2 에 도달함
    - VPC Peering 을 사용하지 않는 문제점이 생김
- 문제점 해결
    - VPC Peering 옵션의 Accepter / Receiver DNS resolution 을 활성화하여 DNS query 시 Private IP 를 전달하도록 함

* VPC Peering 비용

- 동일 리전에 대하여 가용 영역 또는 VPC Peering 연결에 걸쳐 EC2, RDS, Redshift, DynamoDB, DAX, ElastiCache 혹은 ENI 에서 송신 및 수신되는 데이터는 각 방향에 대해 요금 부과
- GB당 0.01 USD 부과