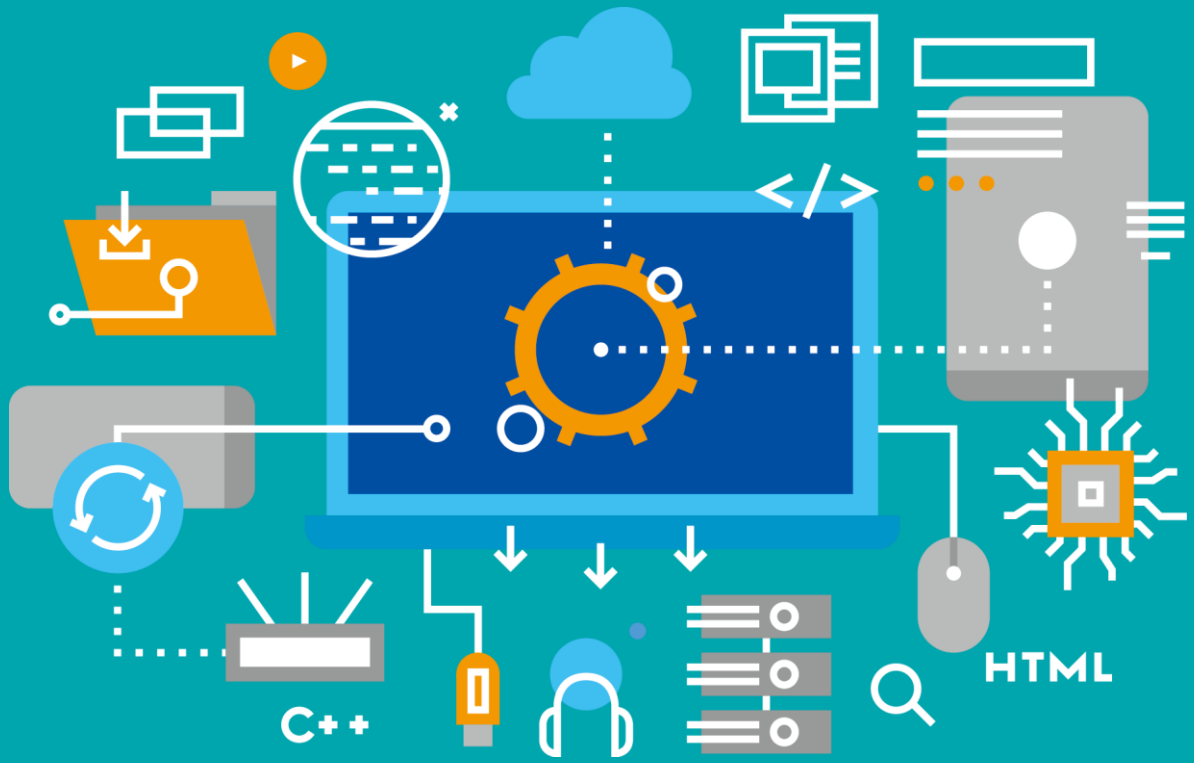
동양미래대학교

DMMU

동양미래대학교 전문기술 석사과정

클라우드와 네트워크 보안

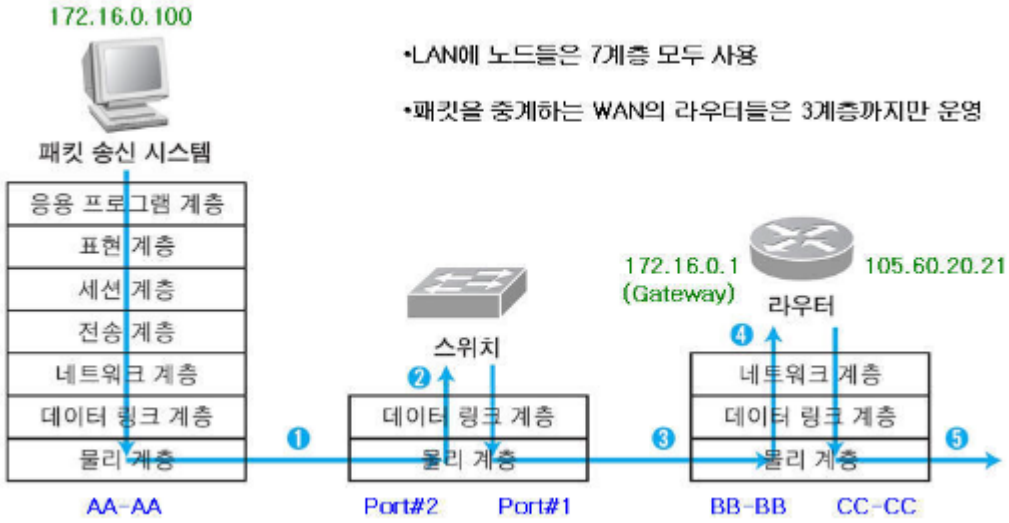
Dongyang Mirae University



라우터/L3스위치 : 3계층 장비

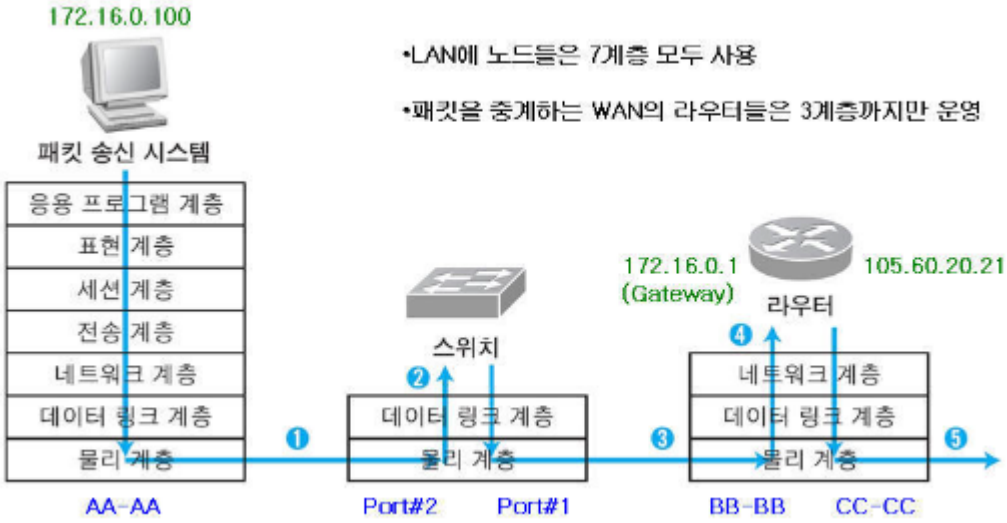
라우터/L3스위치 : 3계층 장비

- IP주소에 따라 Routing Table 정보를 이용하여 패킷을 최적의 경로로 forwarding
- L2 스위치는 패킷의 목적지(MAC 주소)가 MAC table에 없으면 패킷을 로컬 망에 broadcast
- 라우터(L3 스위치)는 패킷의 목적지가 Routing Table에 없으면 패킷을 버림



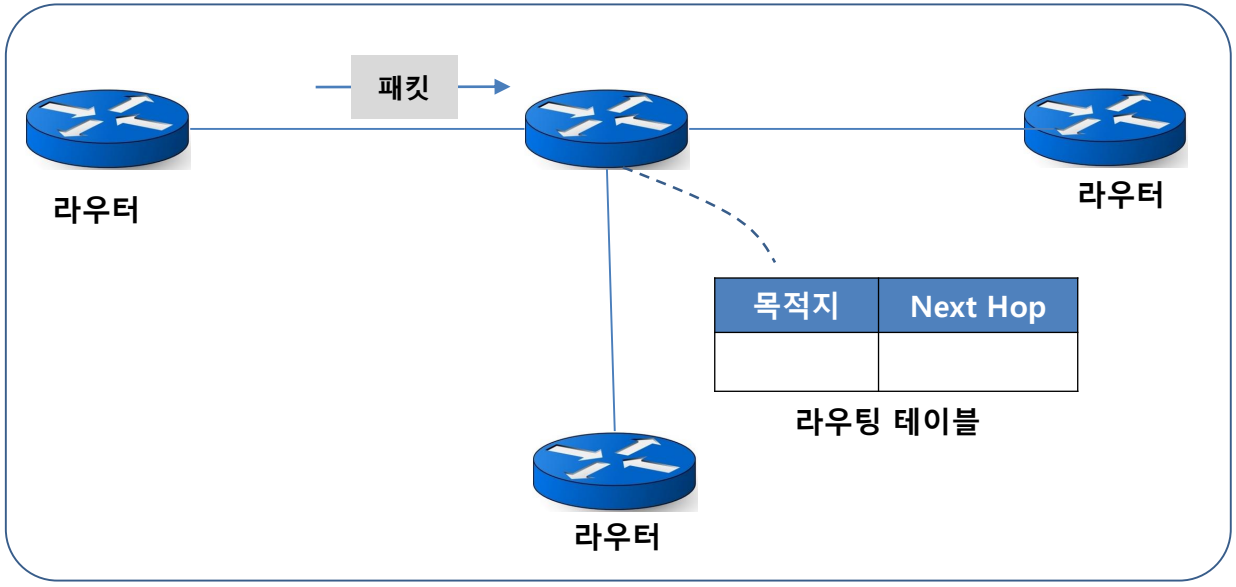
라우터의 동작 방식과 역할

- 라우터는 패킷 포워딩 과정에서 기존 2계층 헤더 정보를 제거 후, 새로운 2계층 헤더를 생성
- ❶ 경로지정, ❷ 브로드캐스트 컨트롤, ❸ 프로토콜 변환 과정을 거침



라우터의 동작 방식과 역할 – ❷ 브로드캐스트 컨트롤

- 라우터는 패킷 포워딩 과정에서 기존 2계층 헤더 정보를 제거 후, 새로운 2계층 헤더를 생성
- 경로지정, 브로드캐스트 컨트롤, 프로토콜 변환 과정을 거침

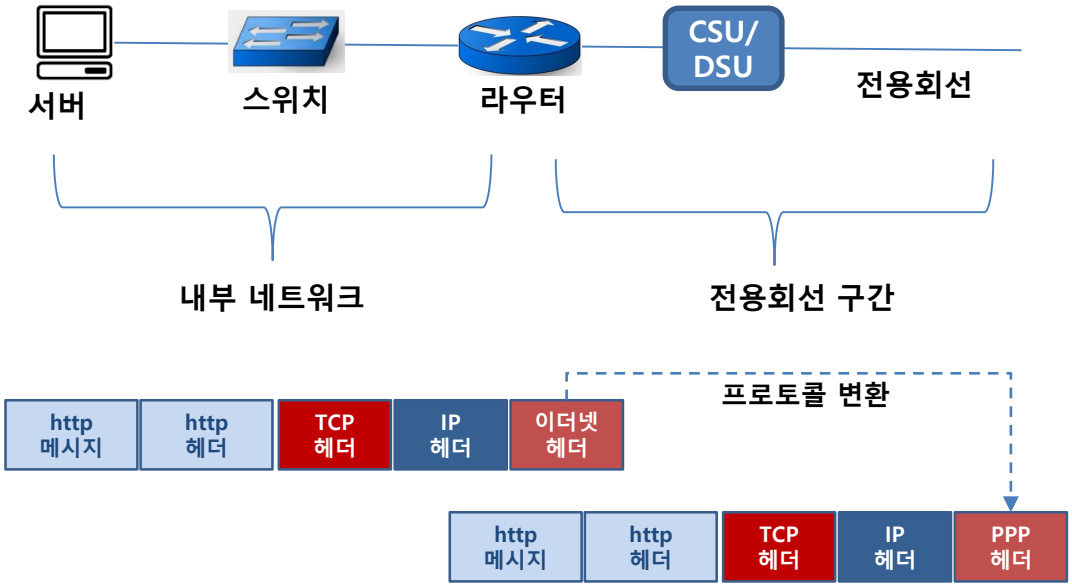


브로드캐스트 콘트롤

1. 브로드캐스트 패킷은 전달하지 않음
2. 패킷의 목적지 주소가 라우팅 테이블에 없으면 패킷을 폐기

라우터의 동작 방식과 역할 – ❸ 프로토콜 변환

- 라우터는 패킷 포워딩 과정에서 기존 2계층 헤더 정보를 제거 후, 새로운 2계층 헤더를 생성
- 경로지정, 브로드캐스트 컨트롤, 프로토콜 변환 과정을 거침

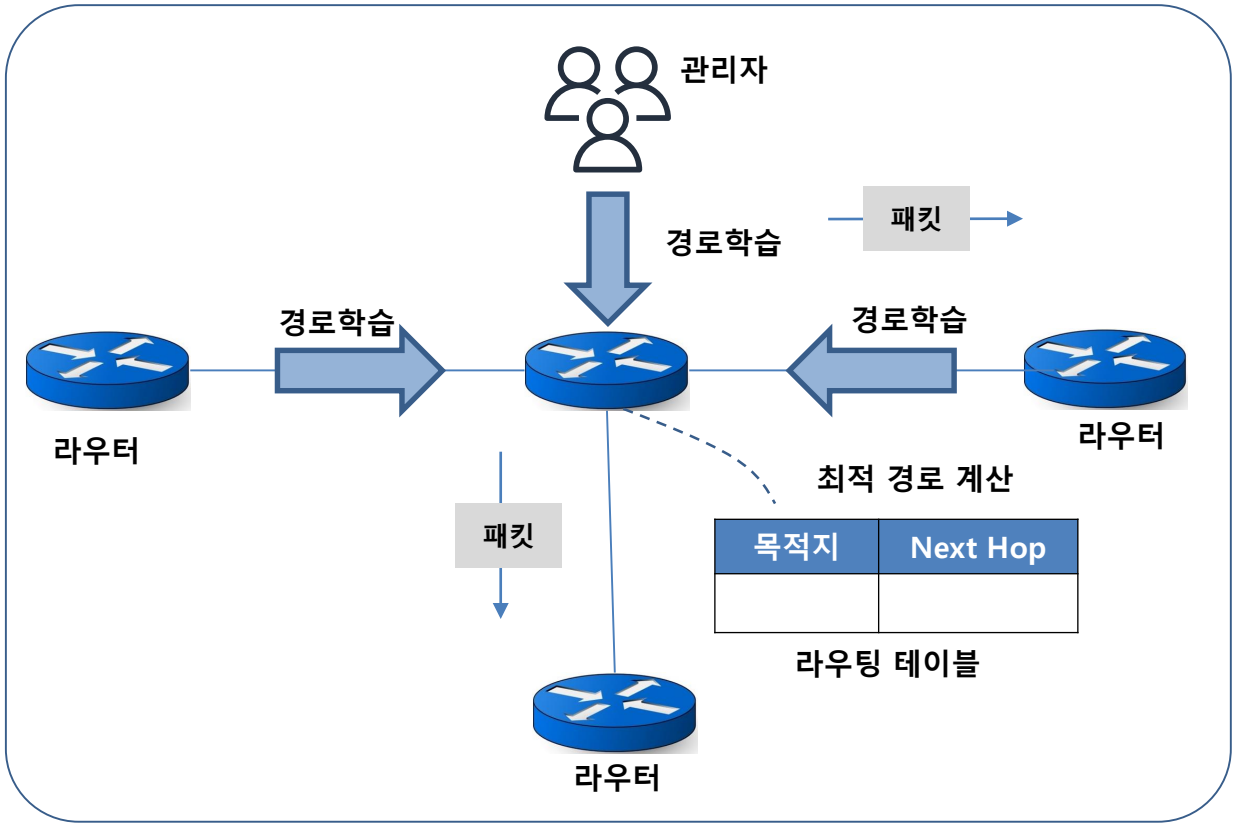


프로토콜 변환

1. LAN 환경과 WAN 환경에서 서로 다른 프로토콜 사용
2. 구간 망에서 사용하는 L2 프로토콜 헤더 정보 변환

라우터의 동작 방식과 역할 – ❶ 경로 지정

- 라우터는 패킷 포워딩 과정에서 기존 2계층 헤더 정보를 제거 후, 새로운 2계층 헤더를 생성
- 경로지정, 브로드캐스트 컨트롤, 프로토콜 변환 과정을 거침

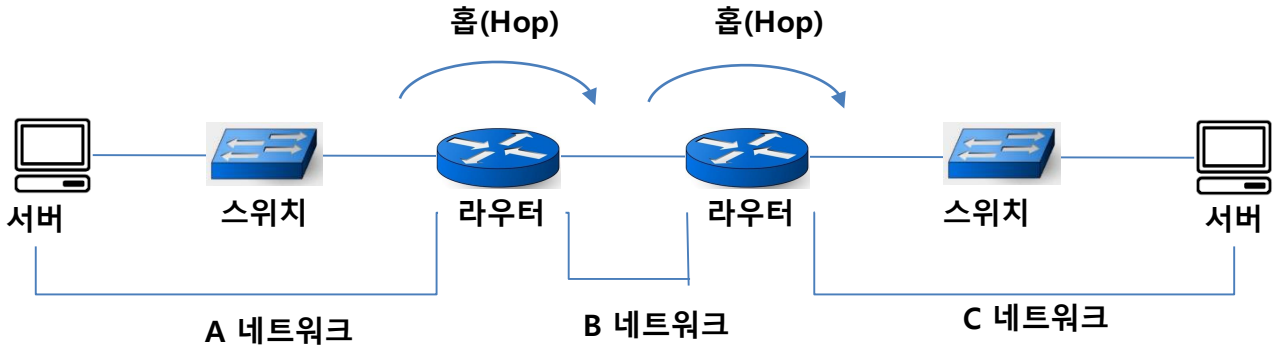


경로 지정

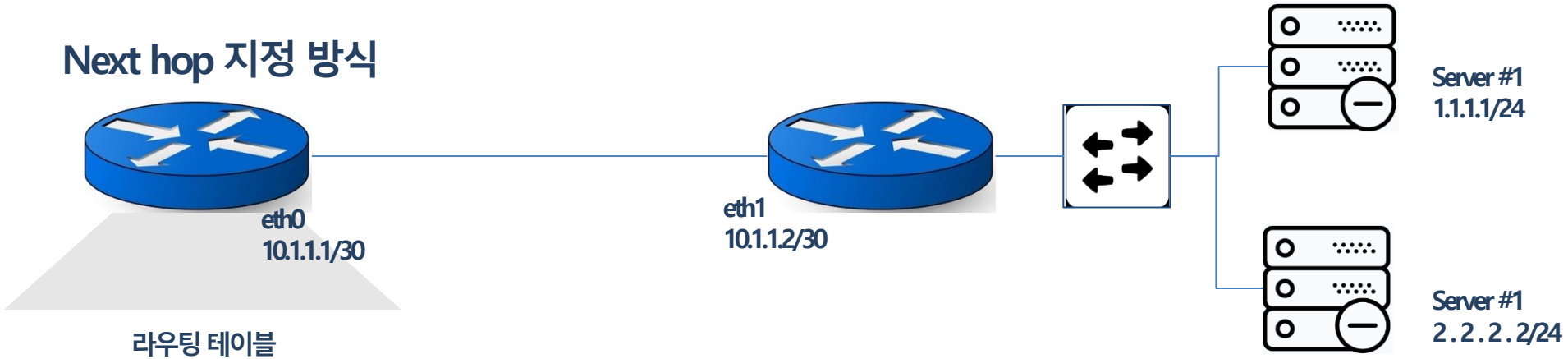
1. 경로 정보 얻기 (최적 경로 연산 – 라우팅 테이블)
   - 관리자가 직접 경로 정보 입력
   - IP 주소 입력시 자동으로 인접 네트워크 정보 확득
   - 라우터 끼리 경로 정보 교환
2. 얻은 경로 정보로 패킷을 포워딩

라우터의 동작 방식과 역할 – ❶ 경로 지정

- Hop-by-Hop 라우팅 : 인접한 라우터 까지만 최적의 경로를 지정
  - 단말에서 목적지 까지의 모든 경로를 책임지는 것은 아님
  - 인접 라우터 경로를 지정하면, 인접 라우터에서 다시 최적의 경로를 파악
- Next Hop : 인접한 라우터
- 라우터는 최적의 Next Hop을 선택



라우터의 동작 방식과 역할 – ❶ 경로 지정



라우팅 테이블

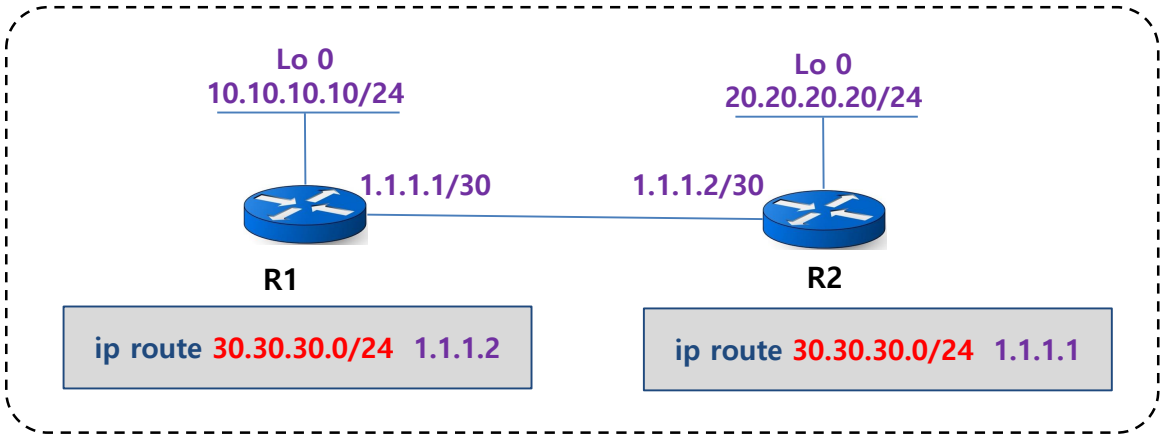
ip route 1.1.1.0/24 **eth0** ① 목적지 주소 + 로컬 인터페이스로 표현

ip route 2.2.2.0/24 **10.1.1.2** ② 목적지 주소 + next Hop 라우터 IP 주소로 표현

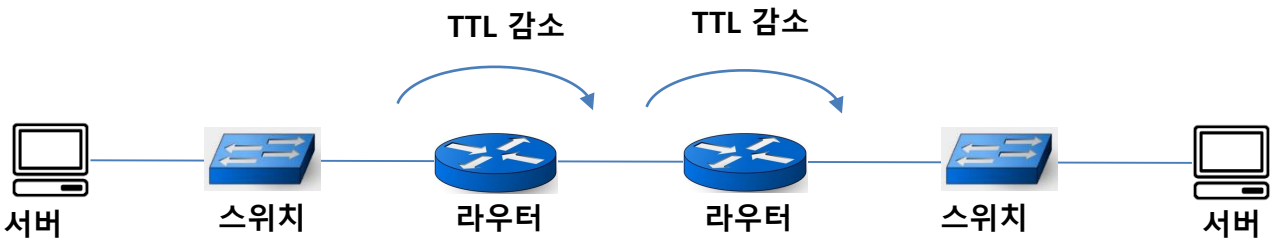
라우팅 테이블에 next hop을 지정하기 위해 일반적으로 next Hop 라우터 IP 주소 지정 방법을 사용 함

라우터의 동작 방식과 역할 – ❶ 경로 지정

TTL (Time to Live)



1. 잘못된 라우팅으로 Loop 발생
2. IP 해더에는 TTL 필드가 있음 (라우터를 지날 때마다 1씩 감소 후, 0이면 폐기)



라우터의 동작 – 경로 지정

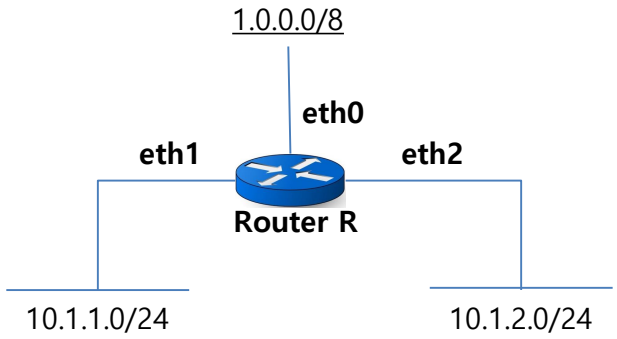
- 라우팅 (라우터가 경로 정보를 얻는 방법)

- 다이렉트 커넥티드(Direct Connected)
- 스태틱 라우팅(Static Routing)
- 다이나믹 라우팅(Dynamic Routing)

라우터의 동작 – 경로 지정

- 라우팅 (라우터가 경로 정보를 얻는 방법)

- **Direct Connected**
  - ✓ 라우터 IP를 입력할 때 라우터에 인접(**직접 연결 된**)한 네트워크 정보로 라우팅 테이블 자동 생성
  - ✓ 라우팅 테이블 정보를 강제로 지울 수 없고, 네트워크 설정을 삭제하거나 비활성화 되는 경우 자동으로 사라짐



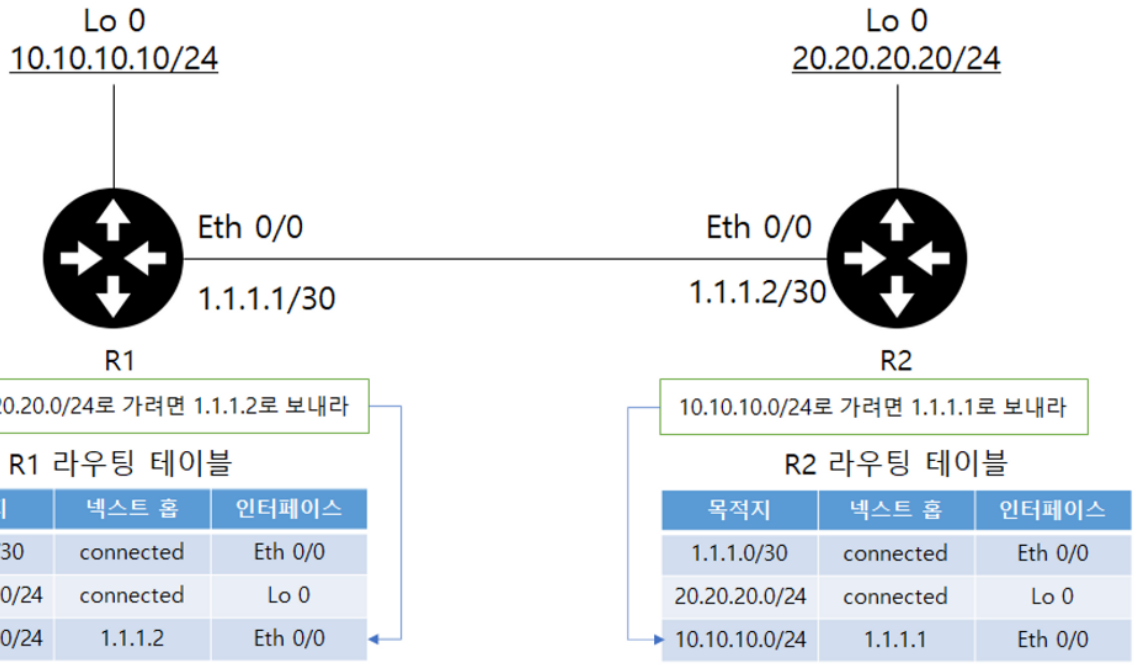
R의 라우팅 테이블

목적지	넥스트홉	인터페이스
1.0.0.0/8	connected	eth0
10.1.1.0/24	connected	eth1
10.1.2.0/24	connected	eth2

라우터의 동작 – 경로 지정

- 라우팅 (라우터가 경로 정보를 얻는 방법)

- **Static Routing**
  - ✓ **관리자가** 목적지 네트워크와 **Next Hop 정보를 라우팅 테이블에 직접 입력**(ip route)
  - ✓ 라우터는 Network 변화에 자동으로 반응하지 못하며, 관리자가 라우터에 직접 설정해 주어야 함



R1 라우팅 테이블

목적지	넥스트 홉	인터페이스
1.1.1.0/30	connected	Eth 0/0
10.10.10.0/24	connected	Lo 0
20.20.20.0/24	1.1.1.2	Eth 0/0

R2 라우팅 테이블

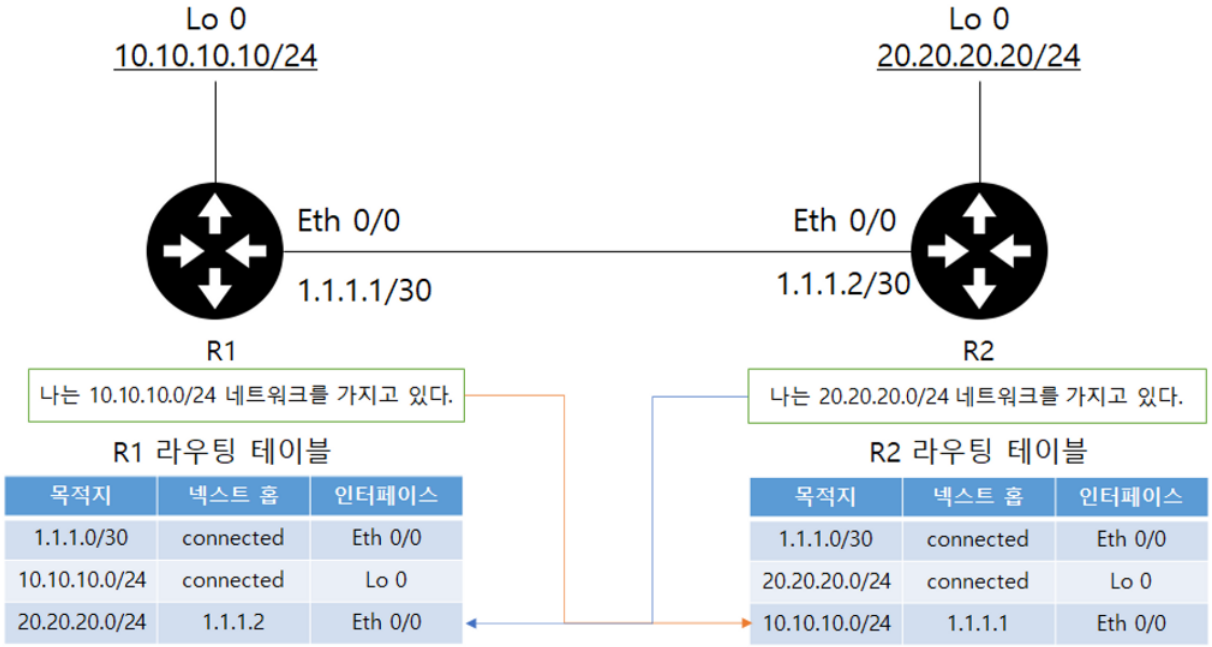
목적지	넥스트 홉	인터페이스
1.1.1.0/30	connected	Eth 0/0
20.20.20.0/24	connected	Lo 0
10.10.10.0/24	1.1.1.1	Eth 0/0

스태틱 라우팅

라우터의 동작 – 경로 지정

- 라우팅 (라우터가 경로 정보를 얻는 방법)

- **Dynamic Routing**
  - ✓ 큰 네트워크에서, static routing은 라우터 너머이 다른 라우터 정보 파악이 어려워 관리가 어려움
  - ✓ 라우터 사이 회선이나 라우터 장애 발생시, 장애 상황 파악 및 대체 경로 설정 등이 어려움
  - ✓ 관리자의 개입 없이 라우터끼리 자신이 알고 있는 경로 정보, 상태 정보를 교환



R1 라우팅 테이블

목적지	넥스트 홉	인터페이스
1.1.1.0/30	connected	Eth 0/0
10.10.10.0/24	connected	Lo 0
20.20.20.0/24	1.1.1.2	Eth 0/0

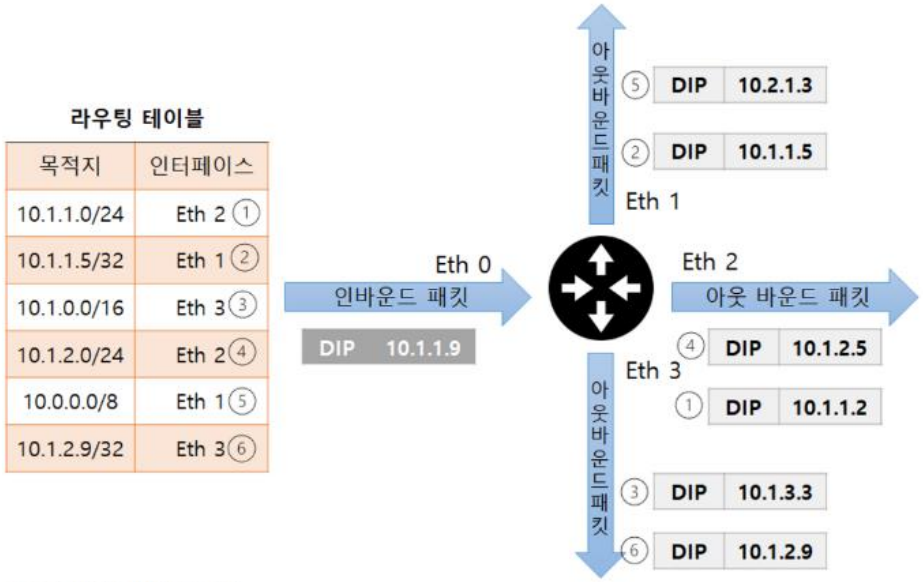
R2 라우팅 테이블

목적지	넥스트 홉	인터페이스
1.1.1.0/30	connected	Eth 0/0
20.20.20.0/24	connected	Lo 0
10.10.10.0/24	1.1.1.1	Eth 0/0

다이나믹 라우팅

라우터의 동작 – 경로 지정

- 스위칭 (라우터가 경로를 지정하는 방법)



라우팅 테이블과 패킷 스위칭

LPM : Longest Prefix Match

1. 10.1.1.9 IP가 목적인 패킷이 라우터로 들어옴
2. 라우터는 도착지 IP와 가장 가깝게 매치되는 경로 정보를 찾는다.
3. 완전히 일치하는 경로 정보는 없기에 `롱기스트 프리픽스 매치(Longest Prefix Match) 기법`을 이용해 갖고 있는 경로 정보 중 가장 가까운 경로를 선택한다.
   - 라우팅 테이블과 도착지 정보가 매칭되는 정보는 `10.0.0.0/8`, `10.1.0.0/16`, `10.1.1.0/24`이다.
     ⇒ *10.0.0.0/8은 10.0.0.0 ~ 10.255.255.255 범위*
     ⇒ *10.1.0.0/16은 10.1.0.0 ~ 10.1.255.255 범위*
     ⇒ *10.1.1.0/24는 10.1.1.0 ~ 10.1.1.255 범위*
   - 10.1.2.0/24, 10.1.2.9/32는 세 번째 자리부터 매치되지 않기에 제외된다.
   - 10.1.1.5/32도 마지막 옥텟 정보가 달라 제외된다.
4. 선택된 3개의 라우팅 정보 중 목적지에 가장 가까운 정보는 `10.1.1.0/24`이다.
5. 10.1.1.0/24를 가장 매칭되는 정보로 파악해 Eth 2 인터페이스 쪽으로 패킷을 포워딩한다.

라우터의 동작 – 경로 지정

- 라우팅, 스위칭 우선 순위

- **일반적인 경로 정보를 모아 놓은 토폴로지 테이블에서 최적 정보를 선정하여 라우팅 테이블에 기록**

목적지 네트워크 정보가 동일한 서브넷을 사용하면 정보를 얻은 소스에 따라 가중치를 정한다.

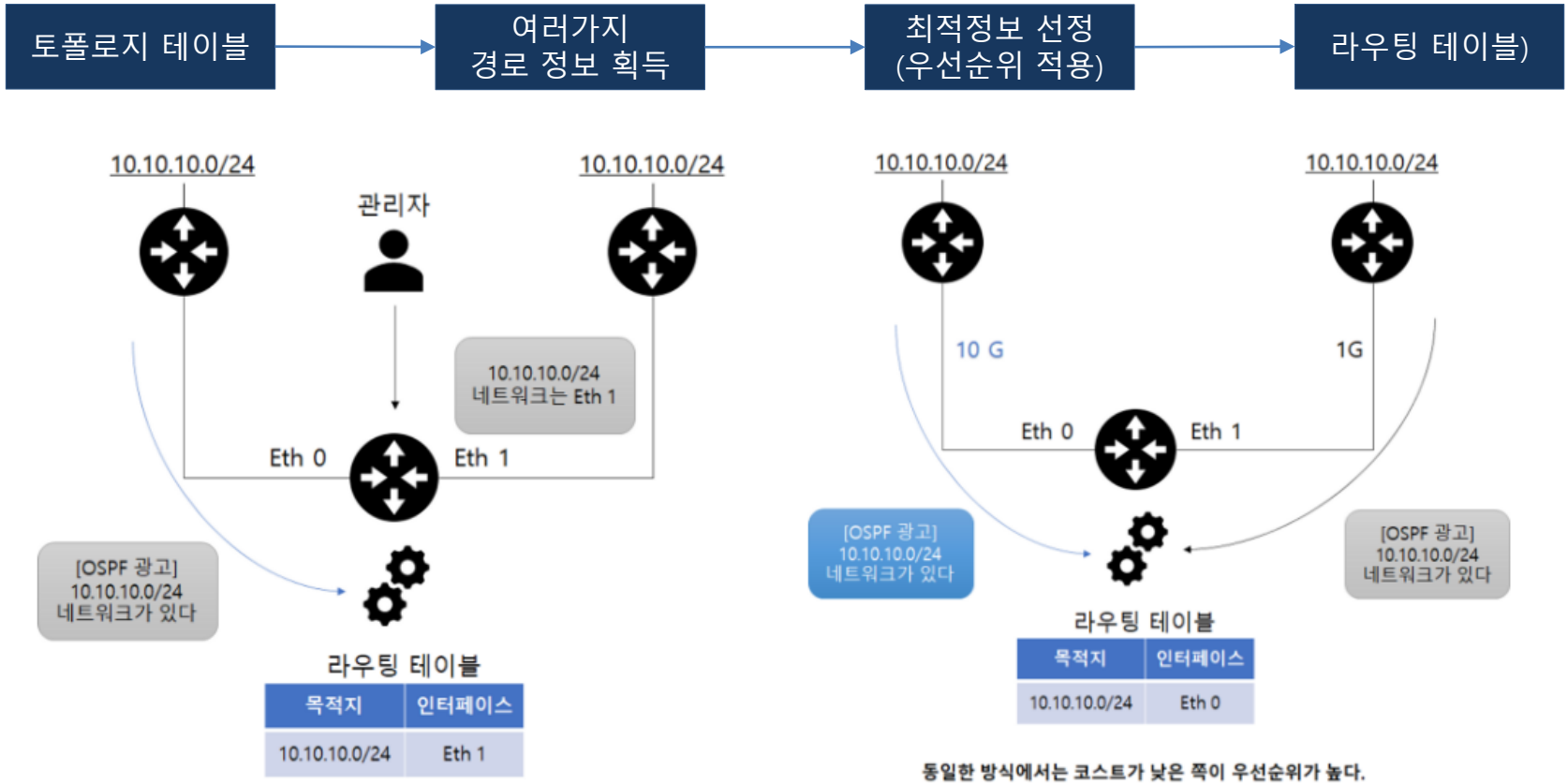
이 가중치 값은 라우팅 정보의 분류와 마찬가지로 크게 3가지로 나뉜다.

- 내가 갖고 있는 네트워크(다이렉트 커넥티드) - **우선순위: 제일 높음**
- 내가 경로를 직접 지정한 네트워크(스태틱 라우팅) - **우선순위: 중간**
- 경로를 전달받은 네트워크(다이나믹 라우팅) - **우선순위: 낮음**

라우터의 동작 – 경로 지정

- 라우팅, 스위칭 우선 순위

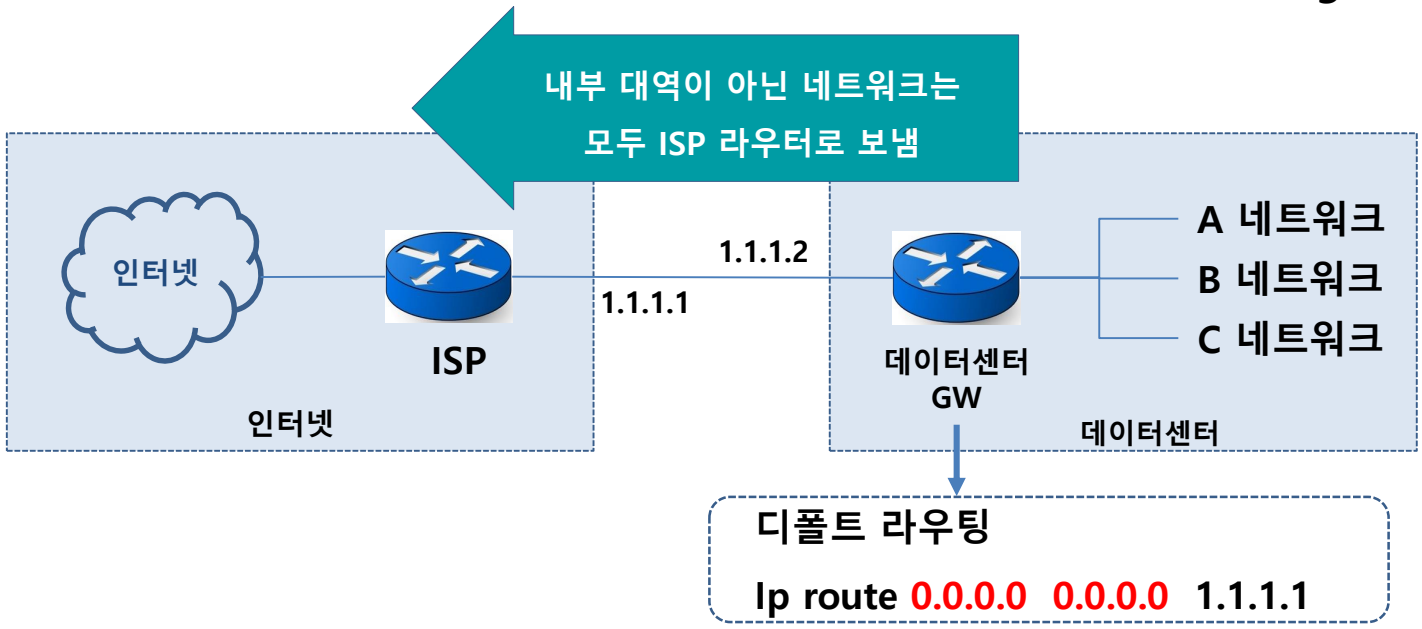
- 일반적인 경로 정보를 모아 놓은 토폴로지 테이블에서 최적 정보를 선정하여 라우팅 테이블에 기록



라우팅 설정 방법

– Default Routing

- 라우터는 목적지를 위한 적절한 경로가 없으면 패킷을 폐기
- 네트워크 규모가 커질수록 관련 경로 정보를 라우팅 테이블에 기록하는 것은 불가능(2021년 라우터 880,000개 이상, https://www.cidr-report.org/as2.0/)
- ISP(KT, SK broadband, LGU+ 등)는 모든 인터넷 정보를 보유한 대형 라우터 운영
- 회사내 외부 패킷을 모두 ISP 라우터로 라우팅하면 통신 가능 (default Routing)

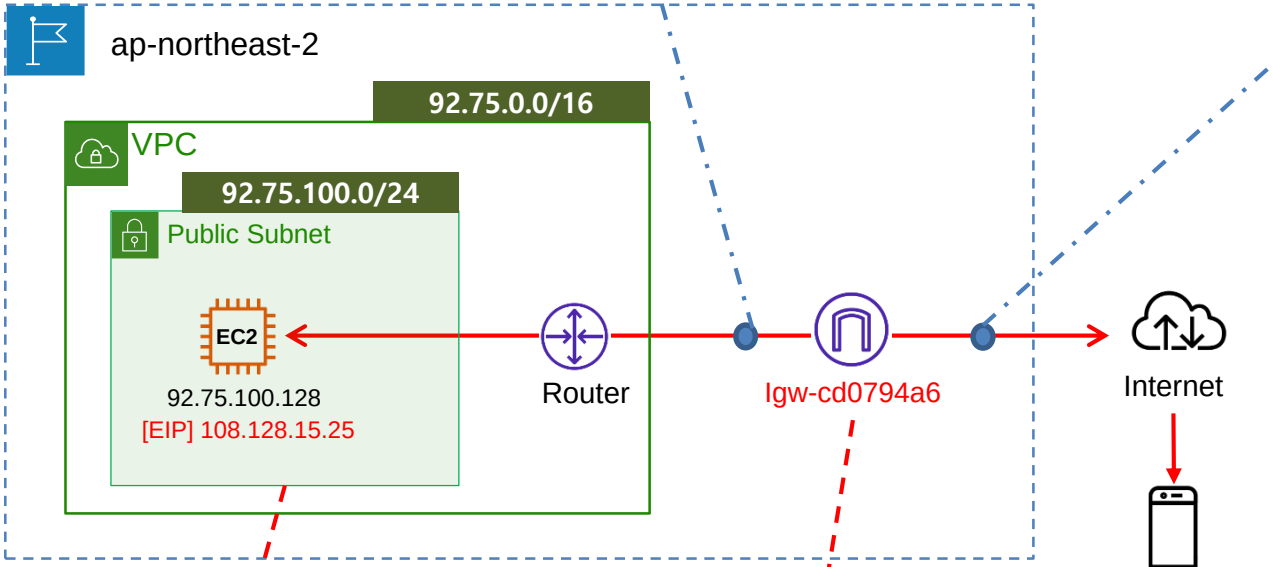


AWS VPC와 Routing

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
122.248.2.9/32	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

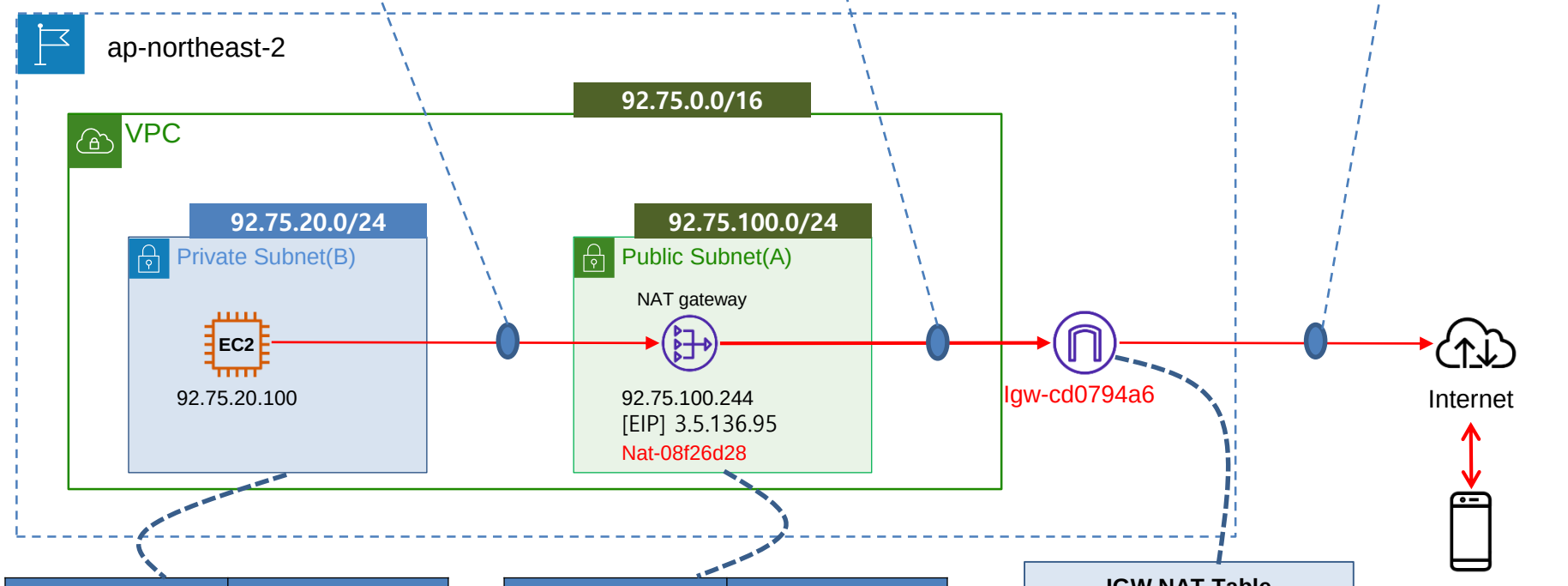
④ IGW는 92.75.100.128(Source IP)를 NAT 테이블에서 찾아 Source IP를 매핑된 IP(122.248.2.9)로 변환하여 트래픽을 외부 망으로 전송

Internet Gateway와 NAT Gateway

Source	Destination	Data
92.75.100.128	122.248.192.71	

Source	Destination	Data
92.75.100.244	122.248.192.71	

Source	Destination	Data
3.5.136.95	122.248.192.71	



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

Routing Table

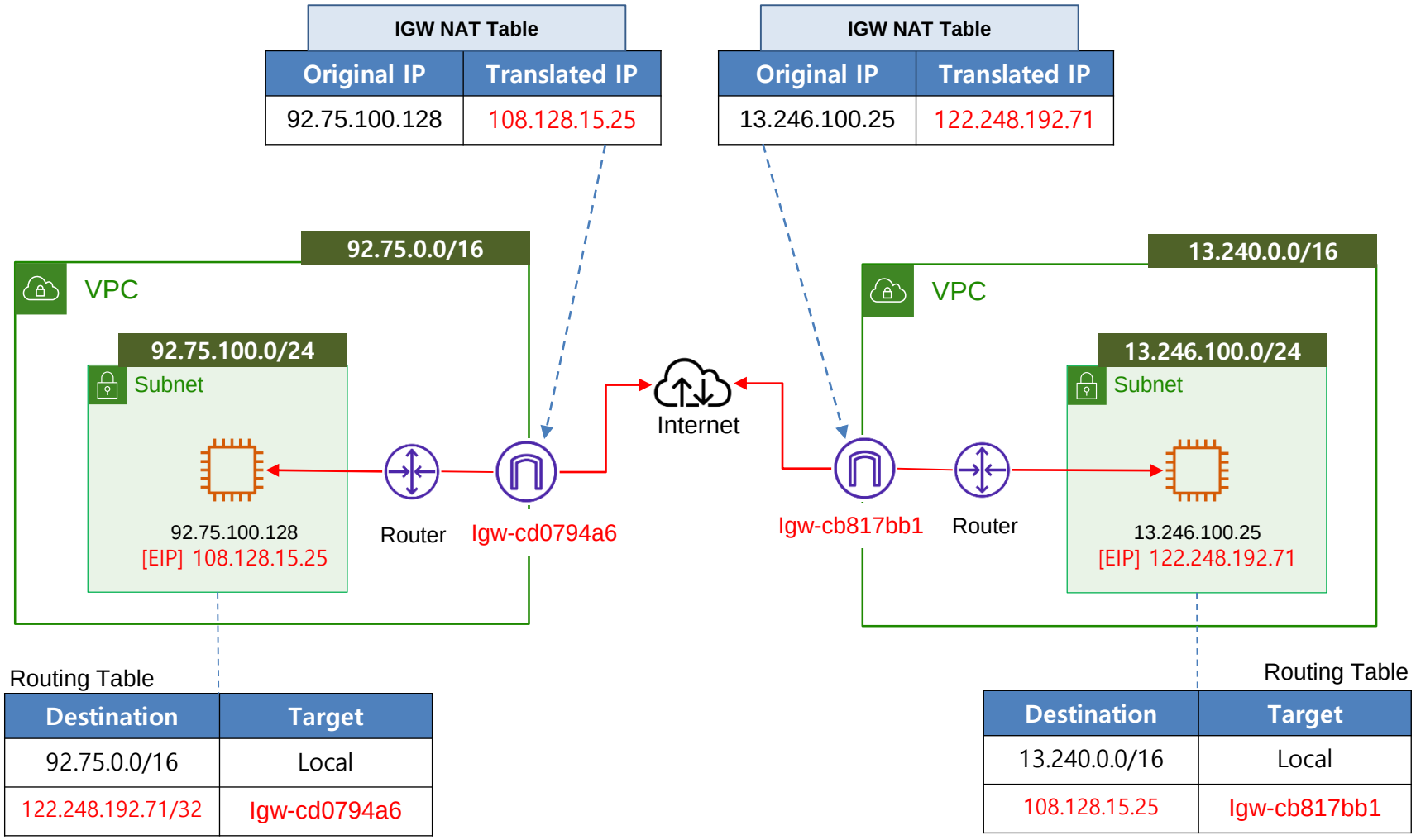
Destination	Target
92.75.0.0/16	Local
122.248.192.71/32	Igw-cd0794a6

Routing Table

IGW NAT Table

Original IP	Translated IP
92.75.100.244	3.5.136.95

VPC internet 통신



Routing Table

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

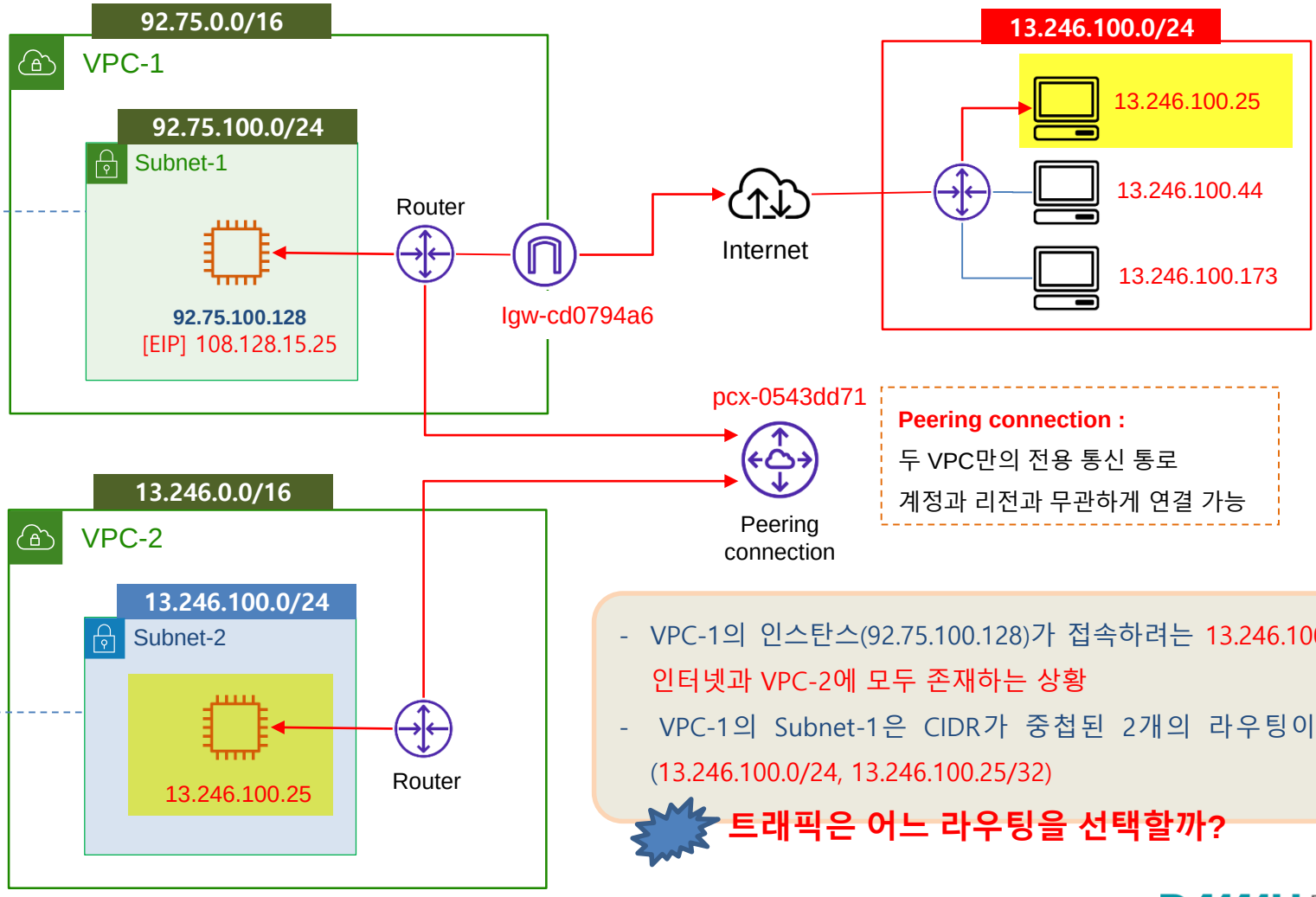
Routing Table

Destination	Target
13.240.0.0/16	Local
108.128.15.25	Igw-cb817bb1

라우팅 경로지정 LPM : Longest Prefix Match

Routing Table

Destination	Target
92.75.0.0/16	Local
13.246.100.0/24	Igw-cd0794a6
13.246.100.25/32	pcx-0543dd71



Routing Table

Destination	Target
13.246.0.0/16	Local
92.75.100.128/32	pcx-0543dd71

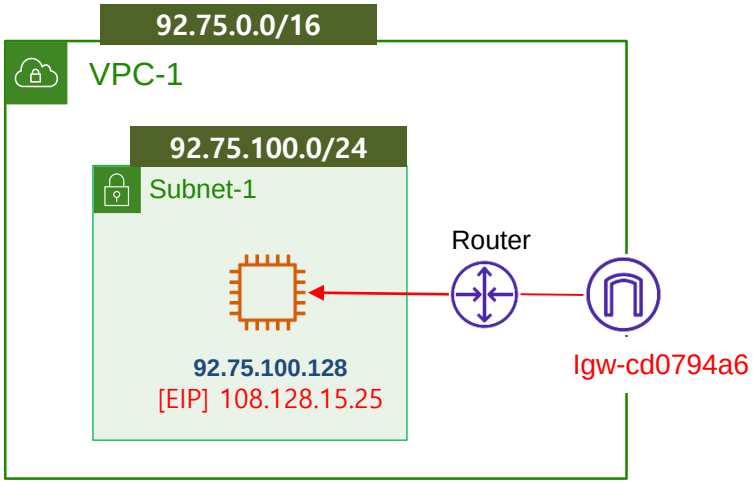
Peering connection :
두 VPC만의 전용 통신 통로
계정과 리전과 무관하게 연결 가능

- VPC-1의 인스탄스(92.75.100.128)가 접속하려는 13.246.100.25은 인터넷과 VPC-2에 모두 존재하는 상황
- VPC-1의 Subnet-1은 CIDR가 중첩된 2개의 라우팅이 존재 (13.246.100.0/24, 13.246.100.25/32)

트래픽은 어느 라우팅을 선택할까?

라우팅 경로지정 LPM : Longest Prefix Match

- 신규 라우팅 등록 절차 1



Routing Table

Destination	Target
92.75.0.0/16	Local

+

사용자 신규 라우팅 등록 요청

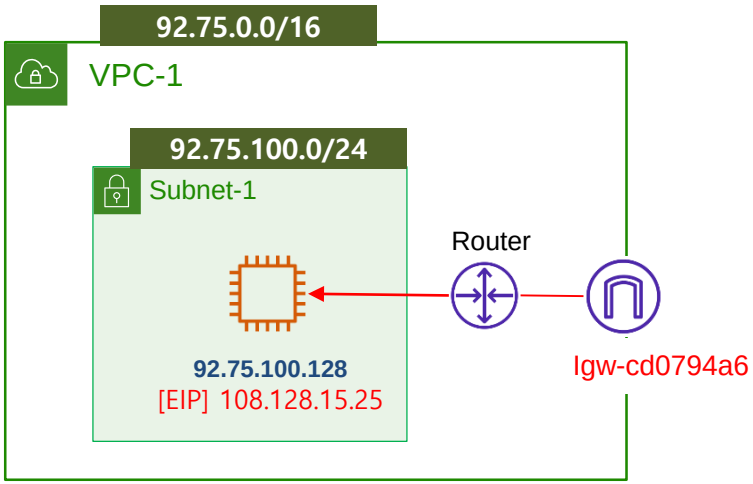
Destination	Target
92.75.0.0/16	Igw-cd0794a6

Reject

- 사용자가 92.75.0.0/16에 대해 IGW로 라우팅 등록을 요청
- 기존 routing Table의 라우팅 대상과 일치 여부 검사
- 기존 routing Table에 92.75.0.0/16이 존재하므로 등록 요청 거부

라우팅 경로지정 LPM : Longest Prefix Match

- 신규 라우팅 등록 절차 2



Routing Table

Destination	Target
92.75.0.0/16	Local

+

사용자 신규 라우팅 등록 요청

Destination	Target
13.246.100.0/24	Igw-cd0794a6

Routing Table

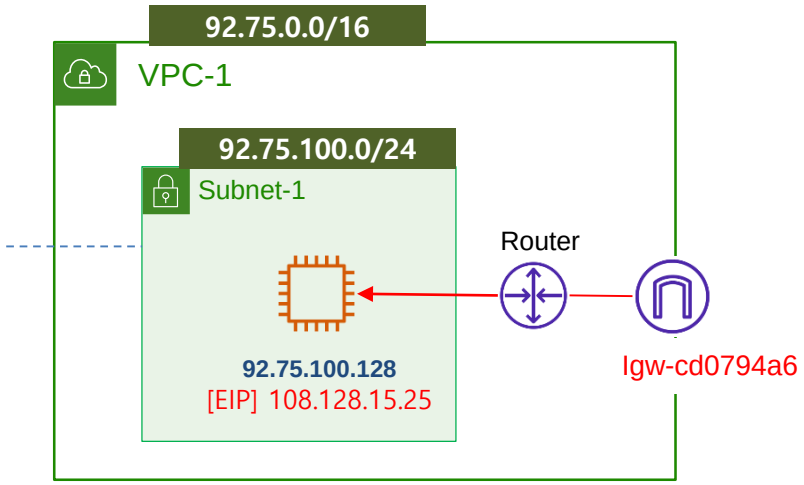
Destination	Target
13.246.100.0/24	Igw-cd0794a6
92.75.0.0/16	Local

Subnet mask 내림차순으로 등록

- 사용자가 13.246.100.0/24에 대해 IGW로 라우팅 등록을 요청
- 기존 routing Table에 13.246.100.0/24 이 없으므로 등록 진행
- 기존 라우팅 정보(92.75.0.0/16)와 subnet mask (/24, /16)을 비교하여 내림 차순으로 정렬하여 등록

라우팅 경로지정 LPM : Longest Prefix Match

- 신규 라우팅 등록 절차 3



Routing Table

Destination	Target
13.246.100.0/24	Igw-cd0794a6
92.75.0.0/16	Local

+

사용자 신규 라우팅 등록 요청

Destination	Target
13.246.100.25/32	pcx-0543dd71

Routing Table

Destination	Target
13.246.100.25/32	pcx-0543dd71
13.246.100.0/24	Igw-cd0794a6
92.75.0.0/16	Local

Subnet mask 내림차순으로 등록

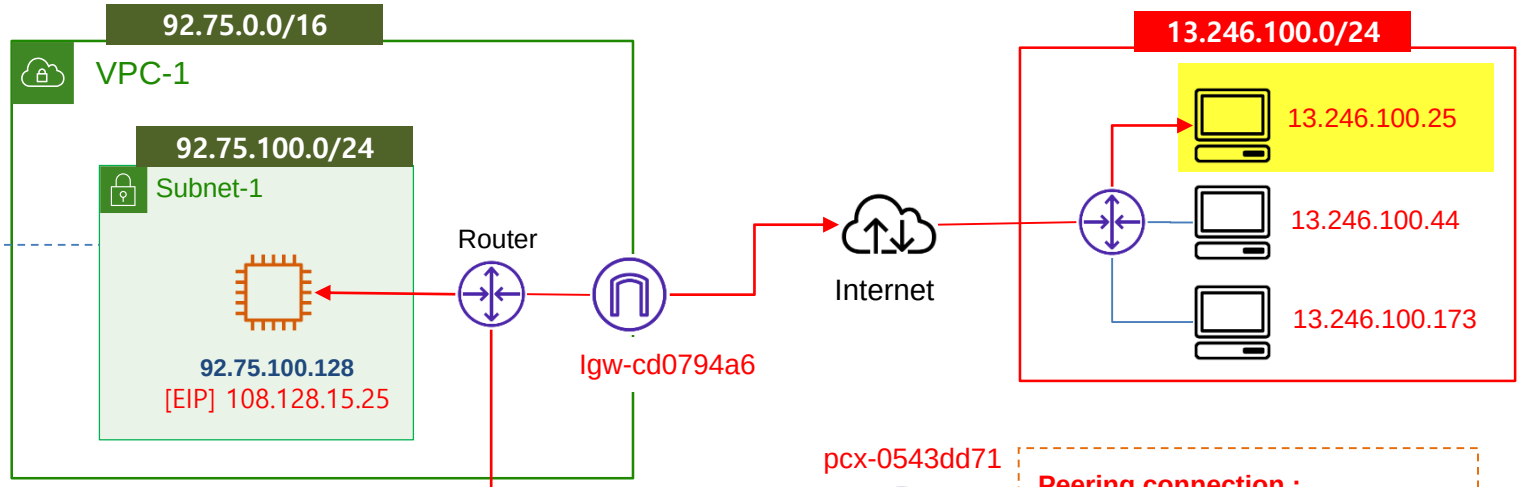
- 사용자가 13.246.100.25/32에 대해 pcx-0543dd71로라우팅 등록을 요청
- 기존 routing Table에 13.246.100.25/32 이 없으므로 등록 진행
- 기존 라우팅 정보(92.75.0.0/16, 13.246.100.0/24)와 subnet mask (/24, /16, /32)을 비교하여 내림 차순으로 정렬하여 등록

라우팅 경로지정 LPM : Longest Prefix Match

- 신규 라우팅 등록 절차 4

Routing Table

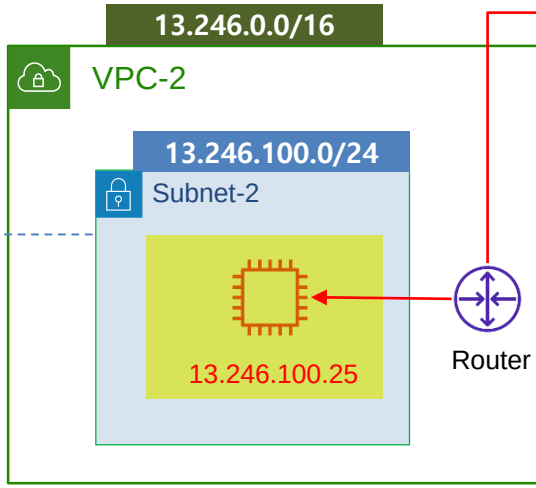
Destination	Target
13.246.100.25/32	pcx-0543dd71
13.246.100.0/24	Igw-cd0794a6
92.75.0.0/16	Local



Peering connection :
두 VPC만의 전용 통신 통로
계정과 리전과 무관하게 연결 가능

Routing Table

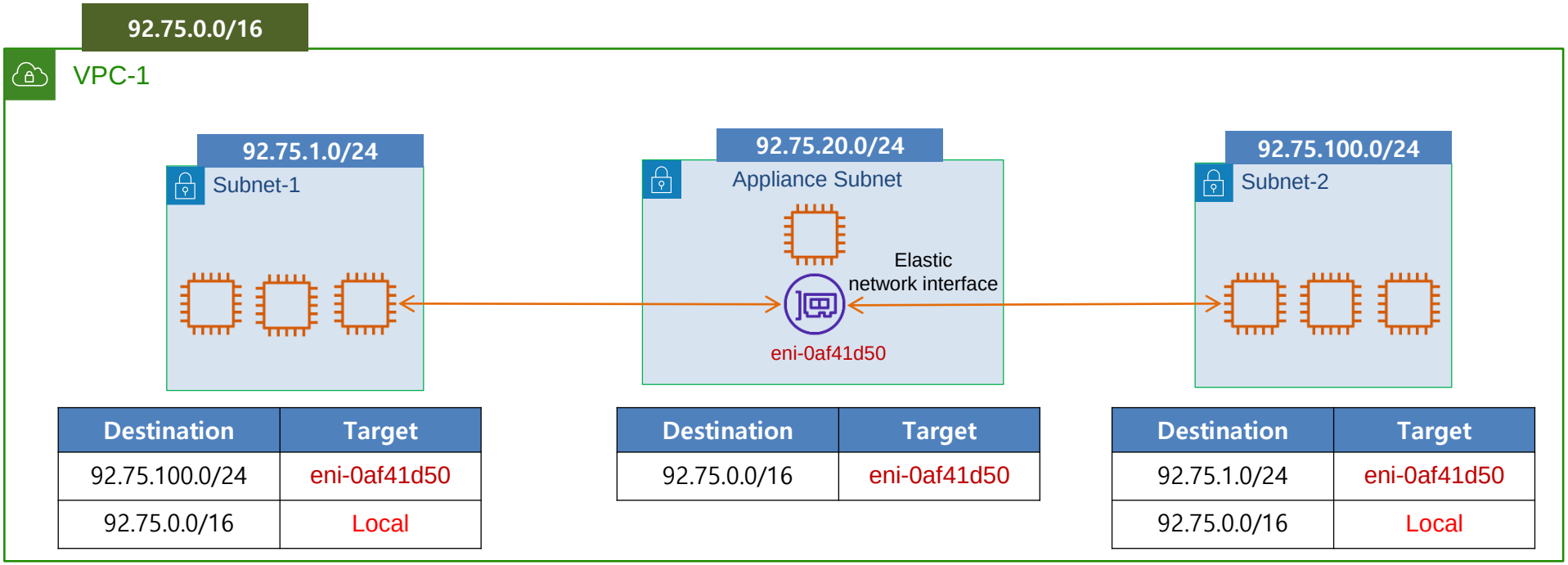
Destination	Target
13.246.0.0/16	Local
92.75.100.128/32	pcx-0543dd71



- VPC-1의 인스탄스(92.75.100.128)가 13.246.100.25로 연결하면
- VPC-1의 Subnet-1의 routing Table을 순차적으로 검색
- 먼저 matching 되는 라우팅 정보로 트래픽 전송
- **13.246.100.25/32 에 먼저 matching되어 pcx-0543dd71로 라우팅**

라우팅 시나리오 사례 - East-West 트래픽 검사 (subnet 간)

방화벽 어플라이언스를 통해 해당 서브넷 간의 트래픽을 검사하려는 시나리오



Destination	Target
92.75.100.0/24	eni-0af41d50
92.75.0.0/16	Local

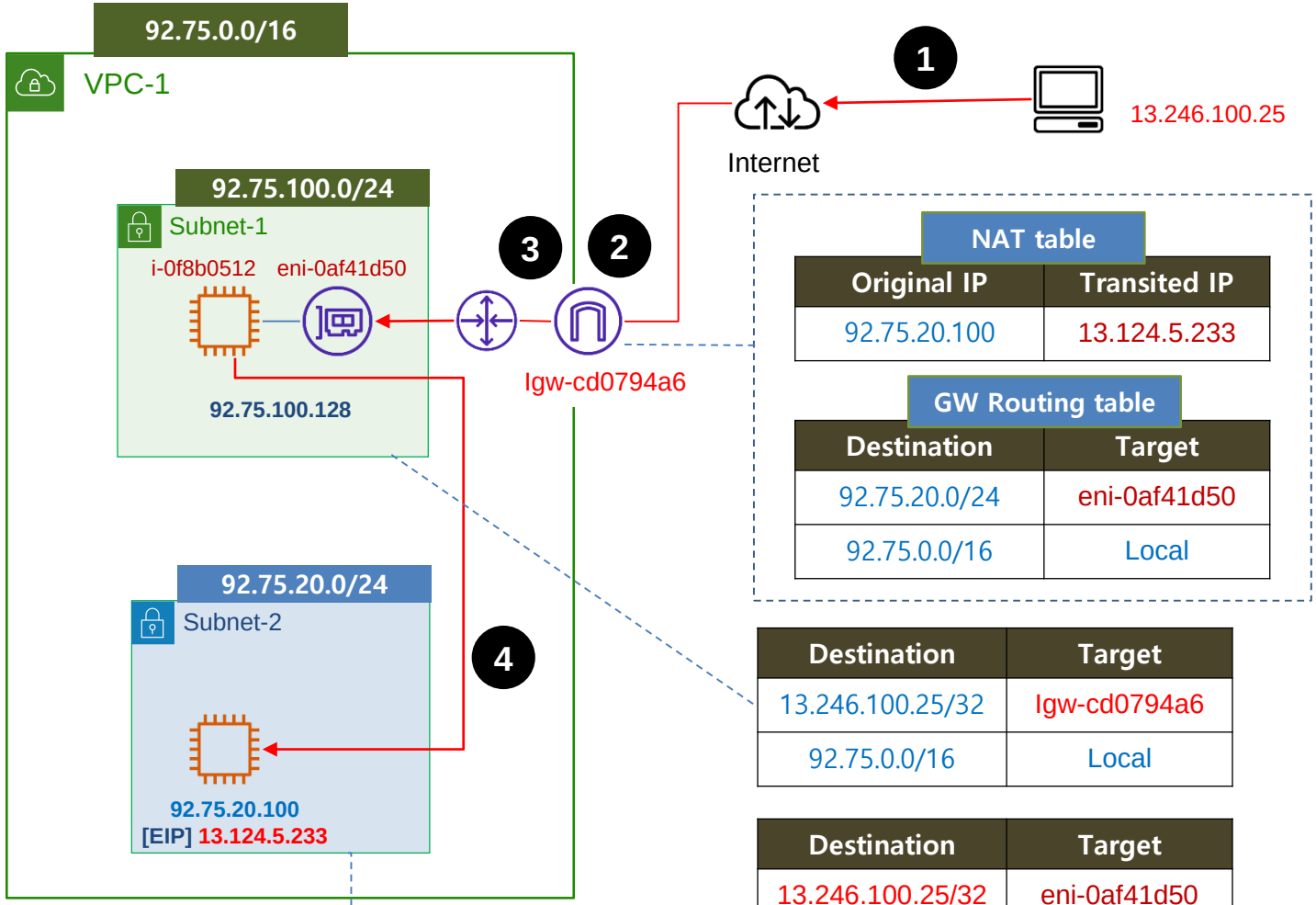
Destination	Target
92.75.0.0/16	eni-0af41d50

Destination	Target
92.75.1.0/24	eni-0af41d50
92.75.0.0/16	Local

- Appliance Subnet에 보안 Appliance 나 모니터링 Appliance를 설치
- **VPC의 내부 Subnet 사이의 모든 트래픽은 Appliance Subnet의 Instance를 경유 시킴**
- Appliance Subnet의 Instance는 최종 목적지 도달 전 패킷에 대한 검사(보안, 모니터링)

라우팅 시나리오 사례 - North-South 트래픽 검사 (Gateway Routing)

VPC로 inbound 되는 트래픽에 대해 서브넷 간의 트래픽을 검사하려는 시나리오



NAT table

Original IP	Transited IP
92.75.20.100	13.124.5.233

GW Routing table

Destination	Target
92.75.20.0/24	eni-0af41d50
92.75.0.0/16	Local

Destination	Target
13.246.100.25/32	Igw-cd0794a6
92.75.0.0/16	Local

Destination	Target
13.246.100.25/32	eni-0af41d50
92.75.0.0/16	Local

1 (트래픽 전송)
13.246.100.25가 13.124.5.233으로 트래픽 전송

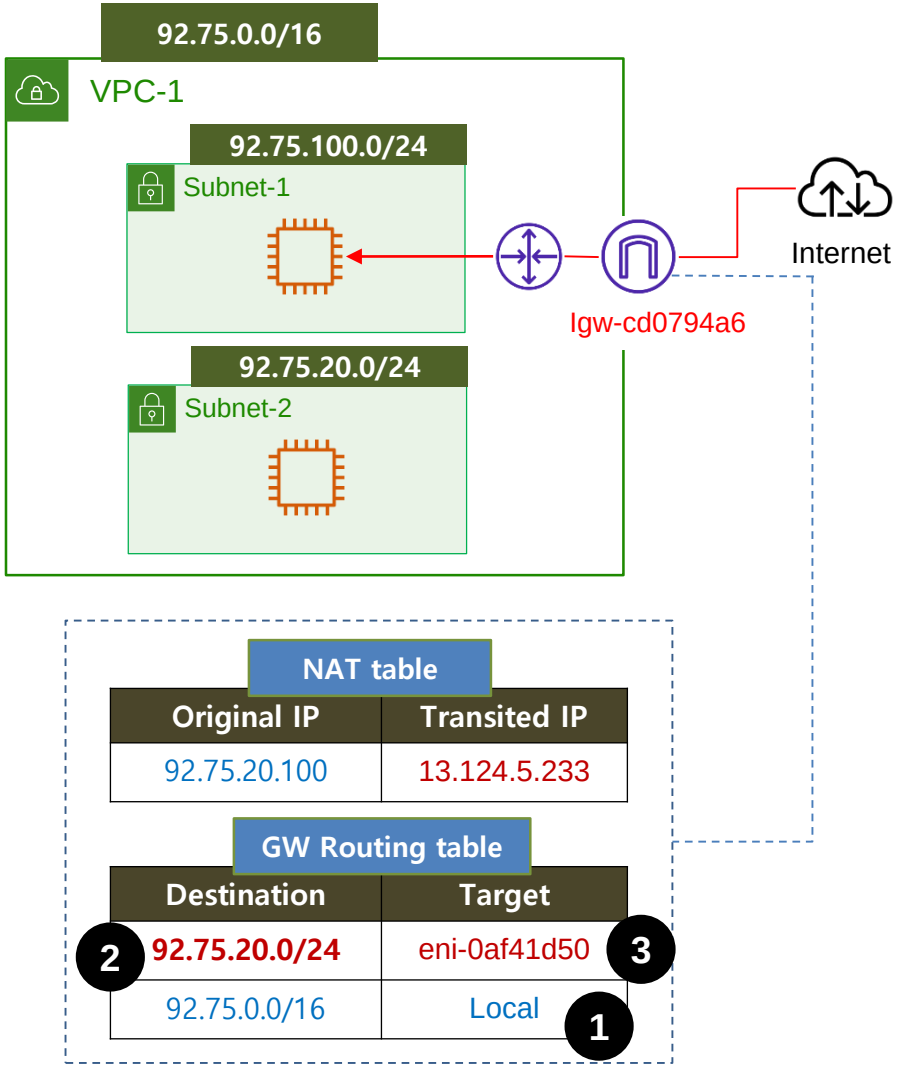
2 (NAT 변환)
트래픽의 목적지를
13.124.5.233에서 92.75.20.100으로 변환

3 (Gateway Routing)
GW Routing Table에서 목적지(92.75.20.100)로 가기 위한 Target eni-0af41d50을 찾아 전달

4 (트래픽 포워딩)
라우팅 기능이 설치된 **92.75.100.128는** subnet의 로컬 라우팅에 따라
목적지(92.75.20.100)로 트래픽을 포워딩함

- 92.75.100.128 인스턴스 위치에 보안 어플라이언스를 설치하면, 트래픽이 최종 목적지(**92.75.20.100)에 도달하기 전 검사 가능**

게이트웨이 라우팅 테이블 – VPC inbound 트래픽에 대해서만 제어



1. VPC 기본 라우팅 정보는 삭제할 수 없음
2. 추가되는 라우팅 정보의 대상(Destination)은 서브넷 단위(subnet CIDR)만 가능
   (예) subnet-1(92.75.100.0/24), subnet-2(92.75.20.0/24)
3. 추가되는 라우팅 정보의 타깃(Target)은 다음 3 종류만 가능
   - ENI (또는 instance)
   - Gateway Load Balancer Endpoint
   - Local

IGW에 연결된 게이트웨이 라우팅 테이블 작동 순서

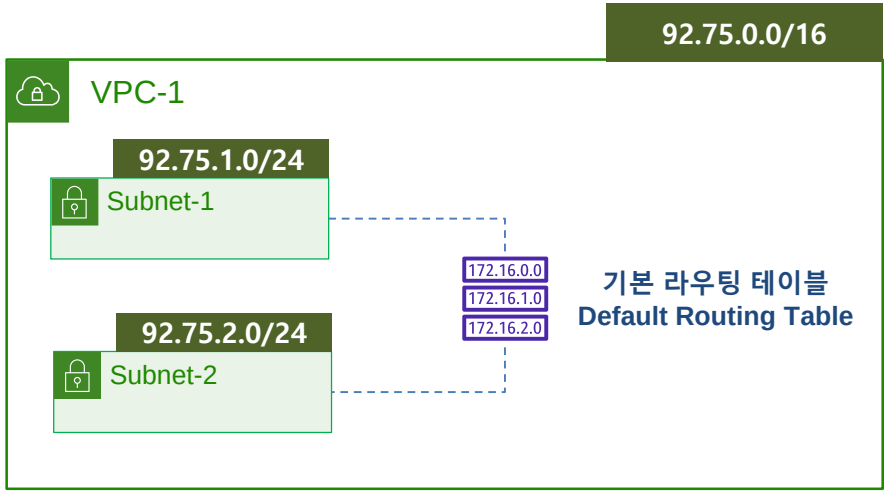
inbound 트래픽이 IGW로 유입되면

(1) NAT 변화(public -> private)을 수행

(2) 게이트웨이 라우팅 테이블이 있으면 :
- (1)에서 변환한 private IP를 게이트웨이 라우팅 테이블에서 확인 후, 관련 타깃으로 트래픽 전달

(3) 게이트웨이 라우팅 테이블이 없으면 :
- (1)에서 변환한 private IP로 트래픽 전달

라우팅 테이블의 특징(1)

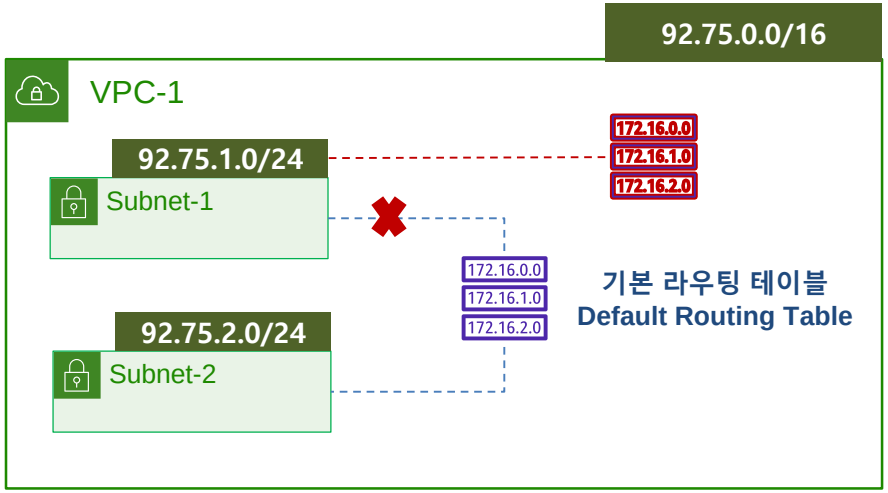


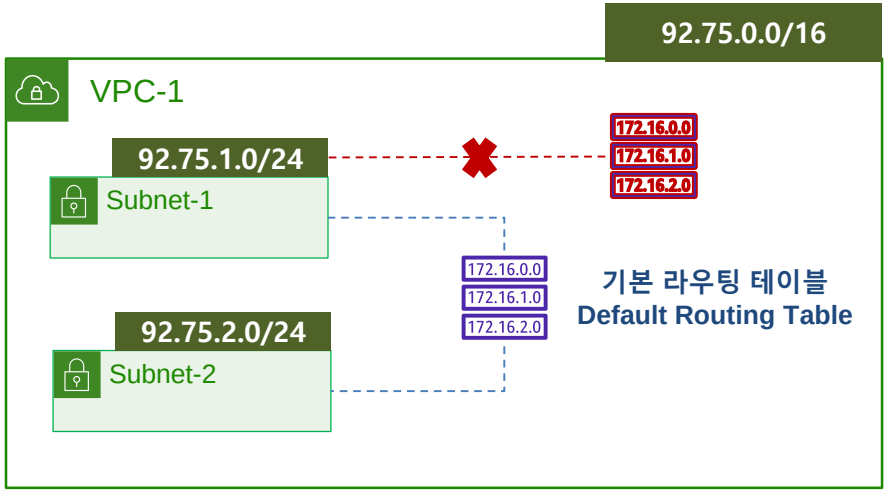
1. VPC를 생성하면 기본 라우팅 테이블도 함께 생성됨
   - Known as the **Main Route Table**
   - 명시적으로 Route Table이 연결되지 않은 모든 Subnet의 라우팅을 제어한다.
   - Main Route Table은 삭제할 수 없음
   - Local Route만 포함

Destination	Target
92.75.0.0/16	Local

2. Subnet을 만들면, 기본 라우팅 테이블에 자동으로 연결됨

라우팅 테이블의 특징(2)

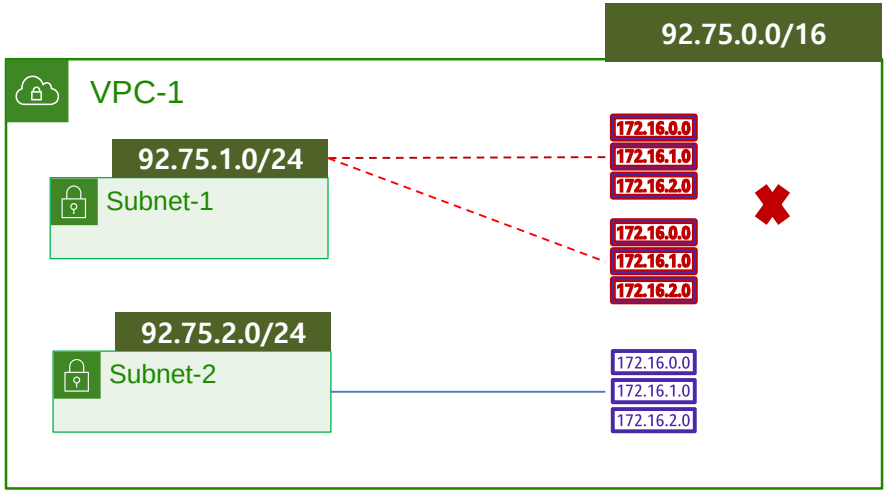




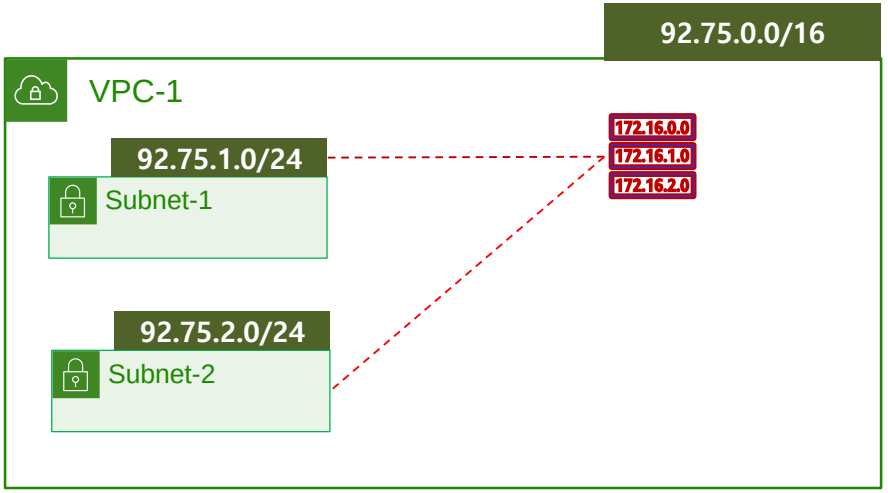
❸ 새로운 라우팅 테이블을 만들어 Subnet-1에 연결하면,
기존 연결은 자동으로 끊어진다.
- Known as the **Custom Route Table**

❹ Subnet-1에 연결된 라우팅 테이블을 해제하면
기본 라우팅 테이블과 자동 연결됨
(subnet은 반드시 하나의 라우팅 테이블과 연결돼야 함)

라우팅 테이블의 특징(3)



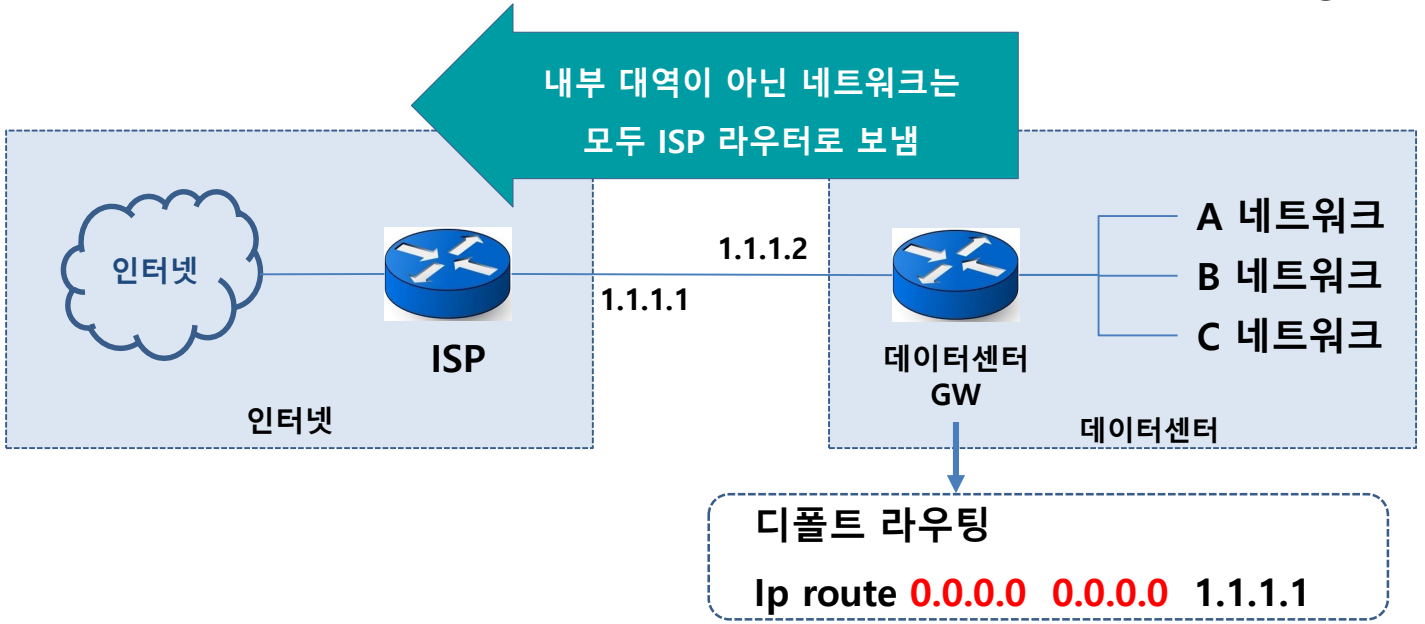
5 각각의 subnet은 한번에 하나의 route Table만 연결됨



6 여러 subnet이 하나의 Route Table에 연결될 수 있음

Default Routing

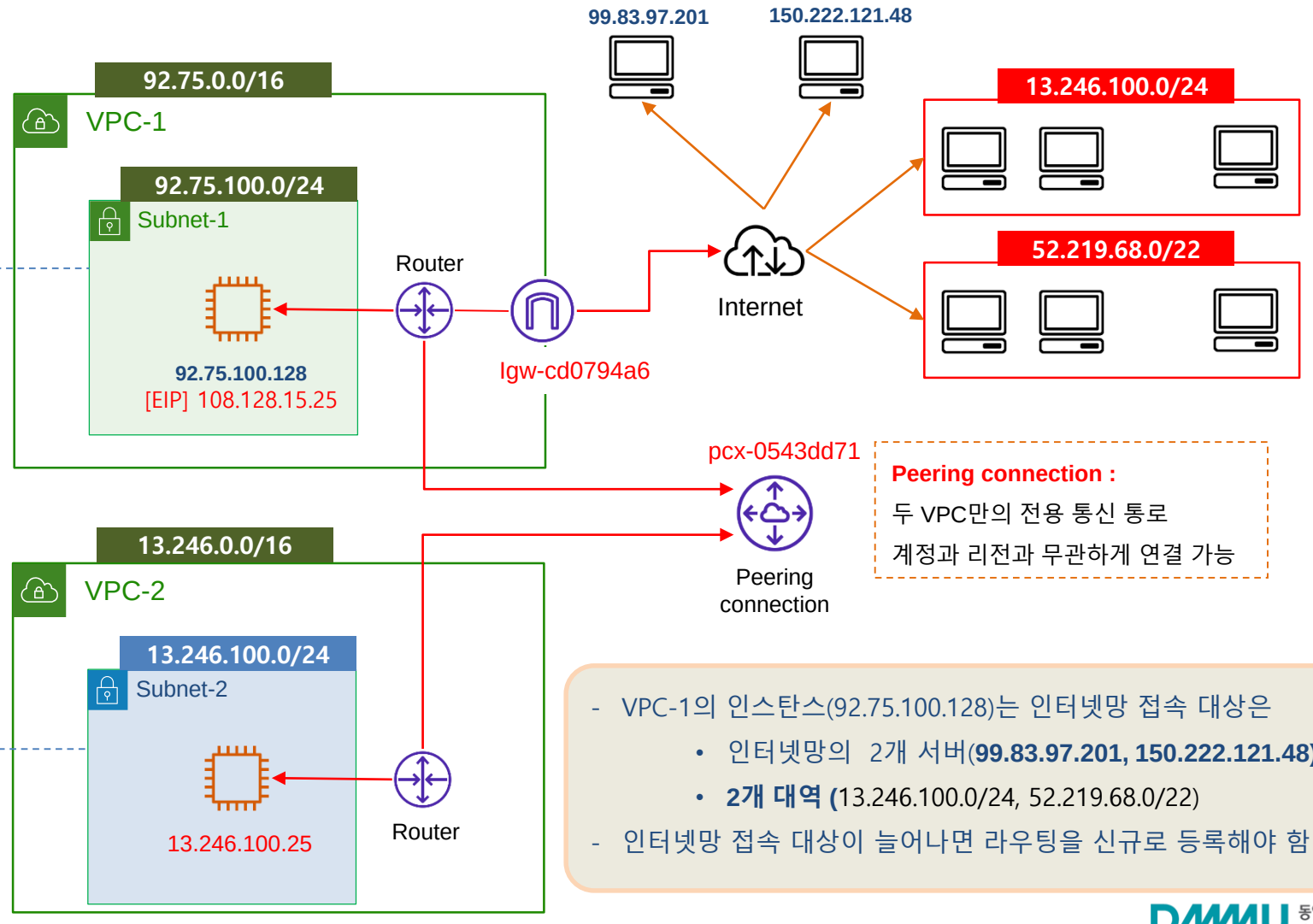
- 라우터는 목적지를 위한 적절한 경로가 없으면 패킷을 폐기
- 네트워크 규모가 커질수록 관련 경로 정보를 라우팅 테이블에 기록하는 것은 불가능(2021년 라우터 880,000개 이상, https://www.cidr-report.org/as2.0/)
- ISP(KT, SK broadband, LGU+ 등)는 모든 인터넷 정보를 보유한 대형 라우터 운영
- 회사내 외부 패킷을 모두 ISP 라우터로 라우팅하면 통신 가능 (default Routing)



Default Routing

Routing Table

Destination	Target
13.246.100.25/32	pcx-0543dd71
99.83.97.201/32	Igw-cd0794a6
150.222.121.48/32	Igw-cd0794a6
13.246.100.0/24	Igw-cd0794a6
52.219.68.0/22	Igw-cd0794a6
92.75.0.0/16	Local



Peering connection :
두 VPC만의 전용 통신 통로
계정과 리전과 무관하게 연결 가능

Routing Table

Destination	Target
13.246.0.0/16	Local
92.75.100.128/32	pcx-0543dd71

- VPC-1의 인스탄스(92.75.100.128)는 인터넷망 접속 대상은
  - 인터넷망의 2개 서버(**99.83.97.201, 150.222.121.48)와**
  - **2개 대역 (**13.246.100.0/24, 52.219.68.0/22)
- 인터넷망 접속 대상이 늘어나면 라우팅을 신규로 등록해야 함

Default Routing

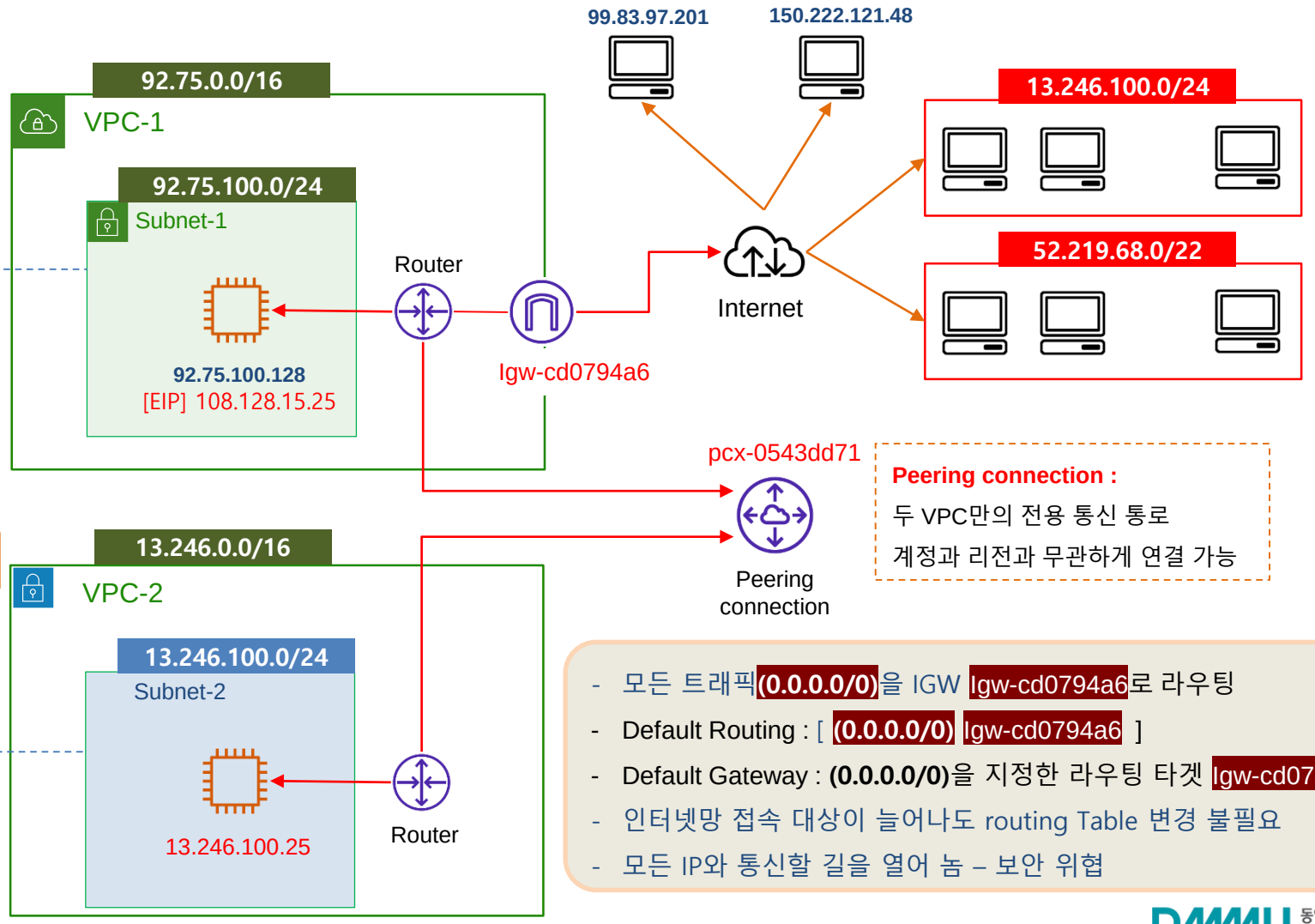
Routing Table

Destination	Target
13.246.100.25/32	pcx-0543dd71
99.83.97.201/32	Igw-cd0794a6
150.222.121.48/32	Igw-cd0794a6
13.246.100.0/24	Igw-cd0794a6
52.219.68.0/22	Igw-cd0794a6
92.75.0.0/16	Local

Destination	Target
13.246.100.25/32	pcx-0543dd71
92.75.0.0/16	Local
0.0.0.0/0	Igw-cd0794a6

Routing Table

Destination	Target
13.246.0.0/16	Local
92.75.100.128/32	pcx-0543dd71



Peering connection :
두 VPC만의 전용 통신 통로
계정과 리전과 무관하게 연결 가능

- 모든 트래픽(0.0.0.0/0)을 IGW Igw-cd0794a6로 라우팅
- Default Routing : [(0.0.0.0/0) Igw-cd0794a6]
- Default Gateway : (0.0.0.0/0)을 지정한 라우팅 타겟 Igw-cd0794a6
- 인터넷망 접속 대상이 늘어나도 routing Table 변경 불필요
- 모든 IP와 통신할 길을 열어 놈 – 보안 위협