

1 एक network को
Subnetting → logically divided
or करा

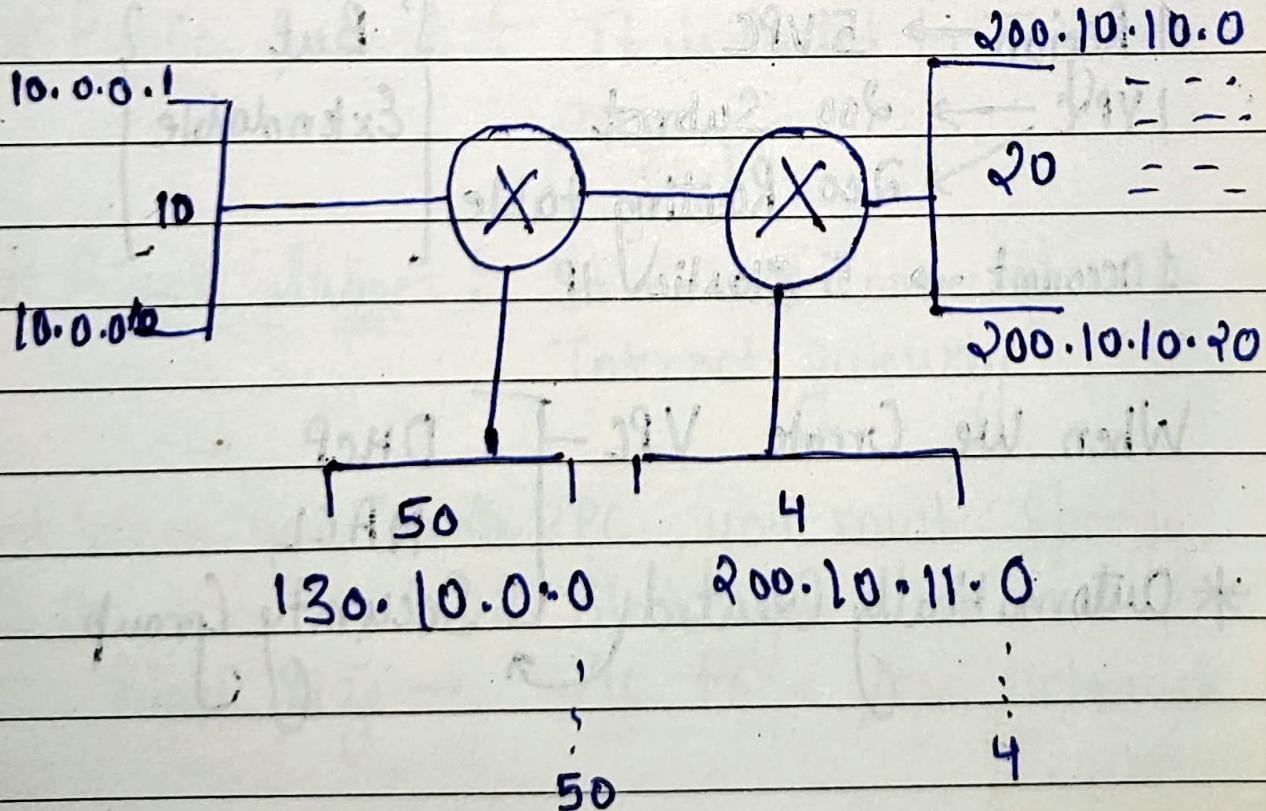
Why we → IPv4 limited

- ① Private IP
- ② use IPv6
- ③ use Subnetting

Networking within a network
OR

Logically division of IP address

* Router → Internetwork device



Virtual private Cloud

A Virtual private Cloud is a Virtual n/w that closely Resembles a traditional networking that you operate in your own data center with benefit of using AWS Infrastructure OR

It is Virtual n/w or data center inside AWS for 1 Client

→ logically Isolated with other VPC

1 Region → 5 VPC

1 VPC → 200 Subnet

→ 200 Routing table

{ But }

Extensible

1 Account → 5 Elastic IP

When we Create VPC -

DHCP

NACL

* Automatically Created Security Group

VPC Types

Default VPC

Custom VPC

Internet gateway By default

Create Internet gateway

* VPC dab → Create VPC

Subnet

Steps

Internet gateway
Routing Table

* Public Subnet :- It is Routed to Internet gateway

* Private Subnet :- It is not Connected with Internet gateway

→ When you Create VPC , you must specify an IPv4 CIDR Block for VPC
Block Size → /16 to /28 netmask

→ First 4 and last IP address of Subnet
cannot be assigned.

Eg. $10 \cdot 0 \cdot 0 \cdot 0$ → Network address

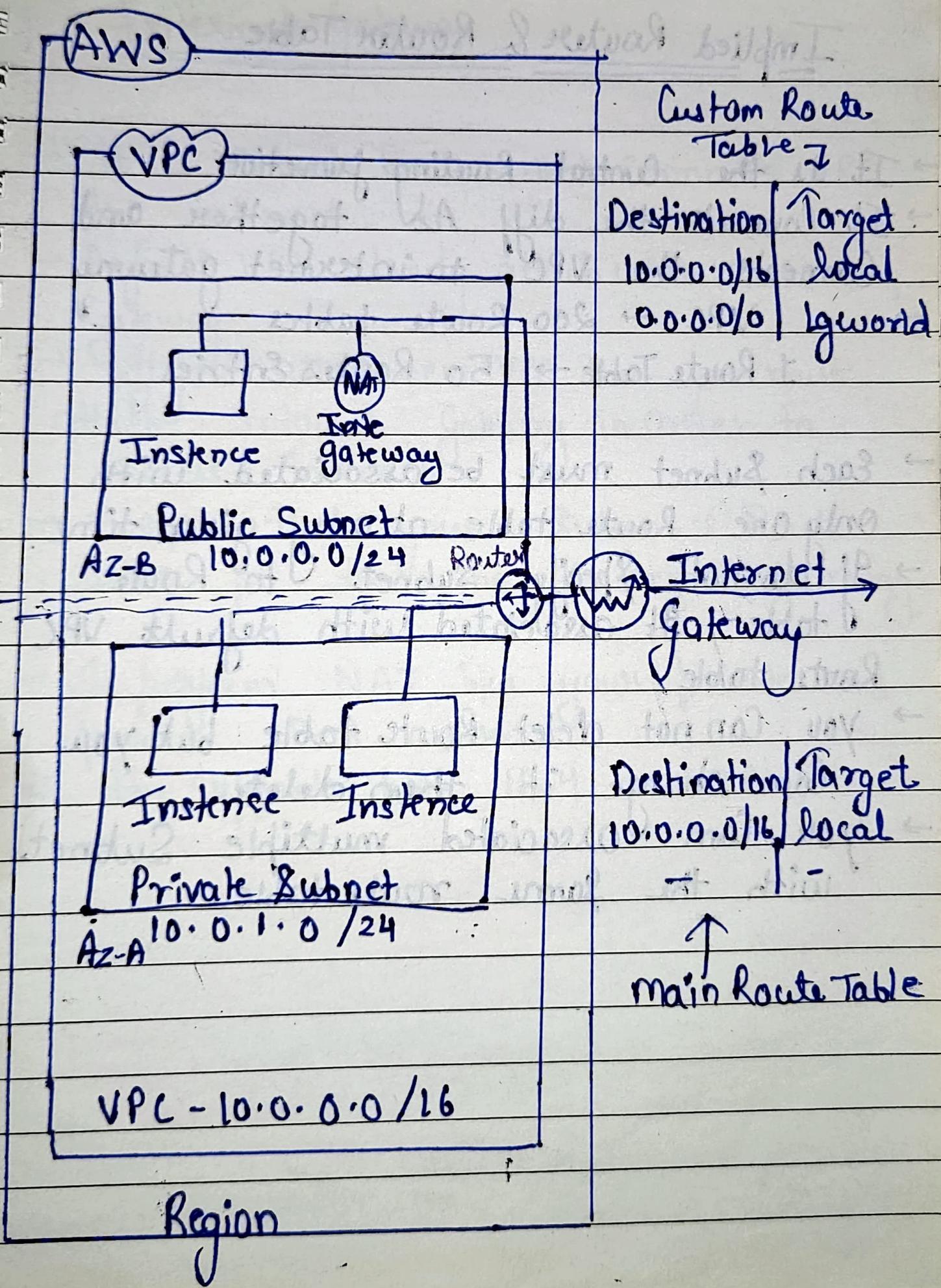
$10 \cdot 0 \cdot 0 \cdot 1$ → Reserved by AWS for VPC
Route

$10 \cdot 0 \cdot 0 \cdot 2$ → Reserved by AWS for IP
address of DNS server

$10 \cdot 0 \cdot 0 \cdot 3$ → Reserved for future use.

$10 \cdot 0 \cdot 0 \cdot 255$ → Broadcast Address

* AWS does not support Broadcasting
in VPC But Reserved this address



Implied Router & Router Table

- It is the Central Routing function.
- It connects the diff AZ together and connects the VPC to internet gateway
- 1 VPC → 200 Route tables
1 Route Table → 50 Routes Entries
- Each Subnet must be associated with only one Route table at any given time
- If do not specify Subnet to Route table, it associated with default VPC Route table
- You can not delete Route table but you can change it then delete.
- You can associate multiple Subnet with the same route table.

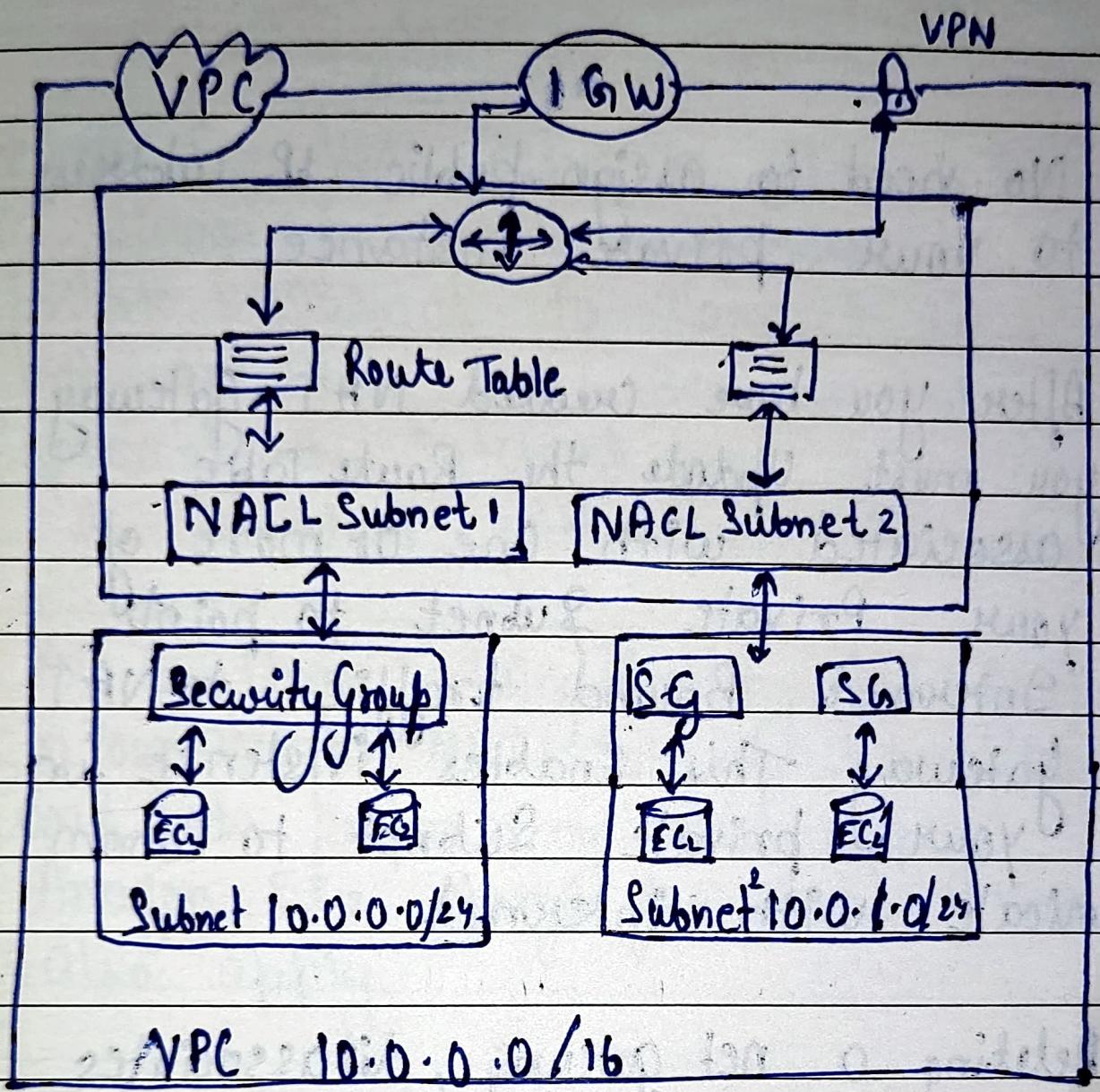
Internet Gateway

- It is Virtual Router that connects VPC to internet
- Default VPC already attach with Internet Gateway.
- If you attach new VPC then you must attach Internet Gateway in Order to access internet
- Ensure that your Subnet's Route table pt. to the internet gateway.
- It performs NAT b/w your private and public IPv4 address.
- * It supports both IPv4 and IPv6

NAT Gateway

- you can use Network address translation gateway to enable instances in a private subnet to connect to internet or other AWS services but prevent the internet from initiating a connection with those instances.
- You can charge for using / creating NAT gateway in your account. NAT gateway hourly usage and data processing rates apply. Amazon ETL charges for data transfer also apply.
- To create NAT gateway, you must specify public subnet in which NAT gateway should reside.
- You must also specify the ~~public subnet~~ IP address to associate with NAT gateway when you create it.

- No need to assign public IP address to your private instance
- After you have created NAT Gateway you must update the Route Table associated with one or more of your Private Subnet to point Internet Bound traffic to NAT Gateway. This enables instances in your private Subnet to communicate with internet.
- Deleting a net gateway, disassociates its Elastic IP address but does not release address from your account.



VPC 10.0.0.0/16

Security Group :- It is a Virtual firewall
works at ENI level.

→ Up to 5 SG per EC₂ instance interface
can be applied.

* Only have permit Rules, Cannot have
deny Rule.

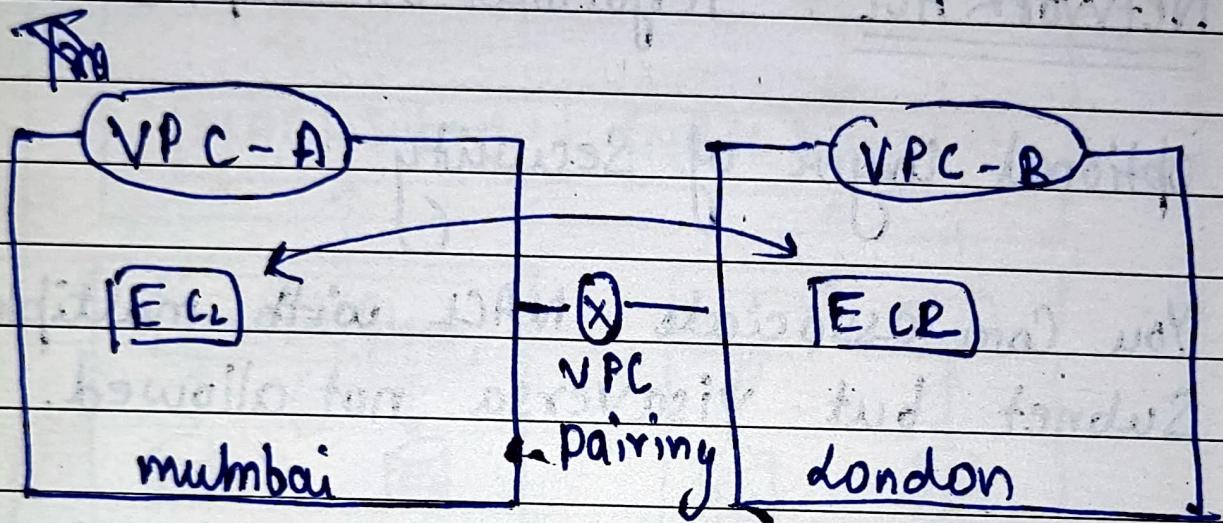
Stateful, Returns traffic, of allowed inbound traffic is allowed, Even if there are no Rule to allow it.

Network ACL :- Performed on Implicit Rules

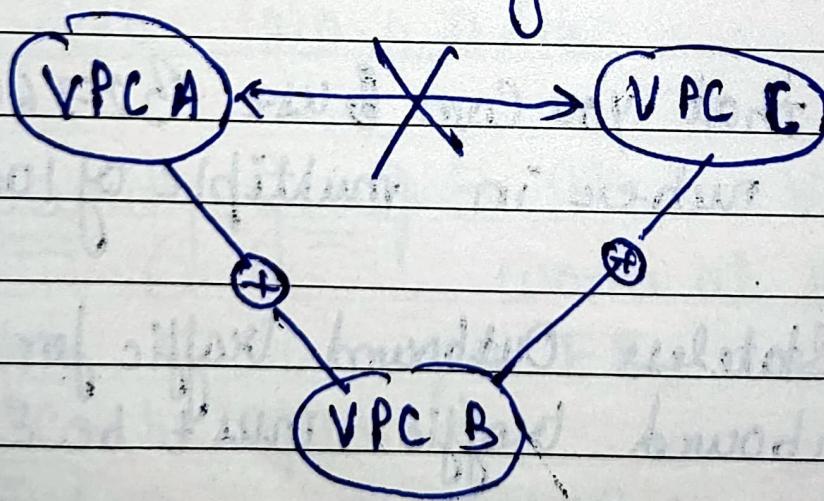
- Optional layer of Security
- You Can associate NACL with multiple Subnet but visavera not allowed.
- NACL Contains no. of Rules that we are Evaluate in Order { Start → End }
- Highest no. that you Can Use 32766
Recommend number in multiple of 100
- NACL are Stateless Outbound traffic for an allowed inbound traffic must be Explicitly allowed.
- You can permit and deny Rules in NACL

VPC Pairing

- two VPC Connection that Enables:
 - * you to route traffic b/w them Using Private IPv4 address or IPv6 address.



* Transitive pairing NOT allowed



How to Create VPC

↓
Create VPC :- Tenancy \rightarrow default \rightarrow 16

↓
Create Subnet :- IPv4 CIDR \rightarrow 10.0.0.0/24

↓
Create Internet gateway :- Select VPC \rightarrow Then attach

Create RouteTable
"j"

Select VPC

{
 Subnet association
 Connect
 Routes
 Edit \rightarrow 0.0.0.0/0