AWS VPC WITH VARIABLE-SIZE SUBNETS

Objective

Design and deploy a **highly complex AWS VPC architecture** using Terraform, where each subnet has a different size based on the required IP capacity. This setup simulates a **production-grade environment** supporting both public-facing and private resources.

1. Create a New VPC

Name the VPC **"asymmetric-vpc"**.

Use a **/16 CIDR block**.

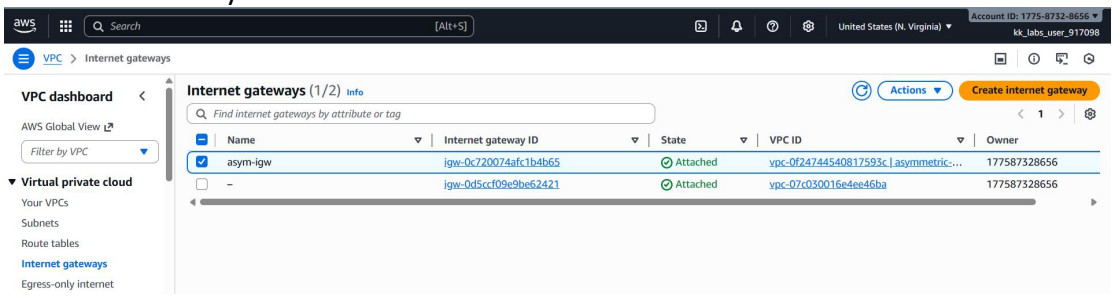
Enable **DNS resolution** and **DNS hostnames**.

Tag all resources with:

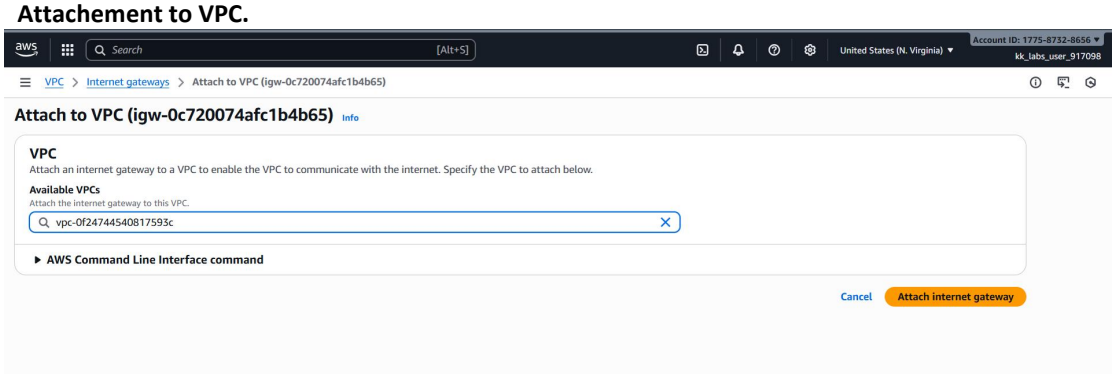
```
Environment = "production"
Owner       = "network-team"
Project     = "asymmetric-vpc-build"
CostCenter  = "AWS-Networking"
```

2.Internet Gateway:

Internet Gateway Creation



Attachement to VPC.



3.Create SIX Subnets with Different Capacities

AWS VPC Architecture – Documentation

This document outlines the network architecture deployed on AWS including VPC design, CIDR strategy, Internet Gateway configuration, Route propagation, Public/Private subnet distribution and routing policies.

VPC Details

- **Name:** Production-VPC
- **CIDR Block:** 10.0.0.0/16
- **Network Scope:** Supports multi-AZ deployment for scalable application topology.

CIDR Allocation – Subnets

Public and private subnets follow non-overlapping hierarchical CIDR blocks.

Public Subnets:
- Public Subnet A → 10.0.0.0/24
- Public Subnet B → 10.0.16.0/20
- Public Subnet C → 10.0.32.0/19

Private Subnets:
- Private Subnet A → 10.0.64.0/22
- Private Subnet B → 10.0.68.0/23
- Private Subnet C → 10.0.96.0/19

Multi-AZ architecture ensures availability zone distribution for fault tolerance.

Internet Gateway (IGW)

- **Name:** Prod-IGW
- IGW enables public outbound & inbound access for public subnets.
- Attached directly to the VPC.

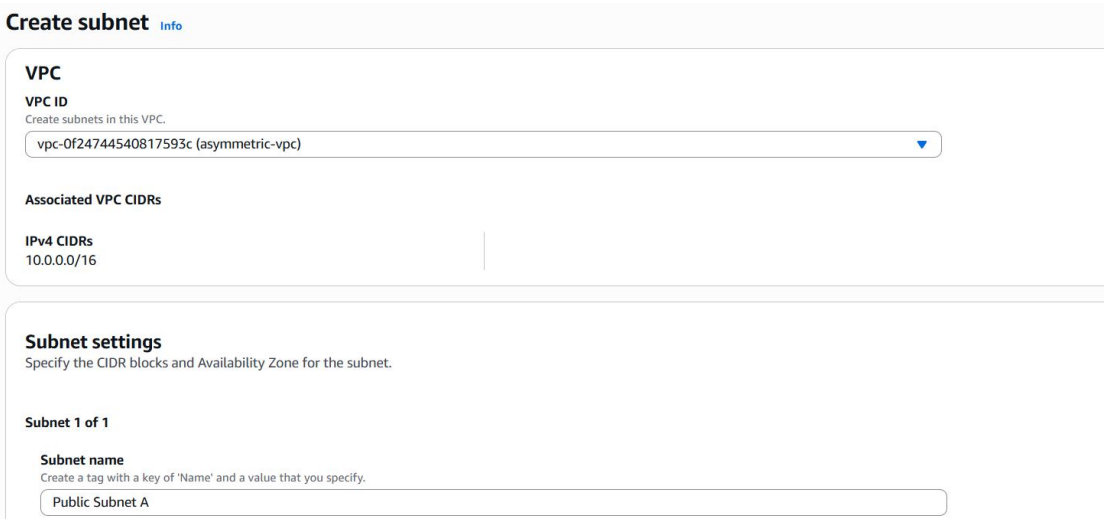
Route Tables

Public Route Tables (Attached to Public Subnets):
- Public-rt-A → Subnet: Public Subnet A
- Public-rt-B → Subnet: Public Subnet B
- Public-rt-C → Subnet: Public Subnet C

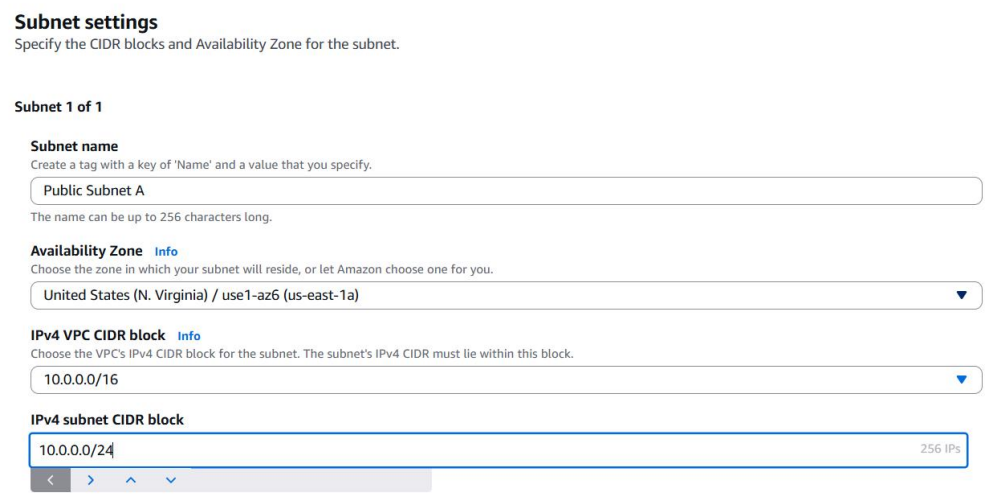
Route entries:
- 0.0.0.0/0 → Target: IGW

Private Route Tables (Attached to Private Subnets):
- Private-rt-A → Subnet: Private Subnet A
- Private-rt-B → Subnet: Private Subnet B
- Private-rt-C → Subnet: Private Subnet C

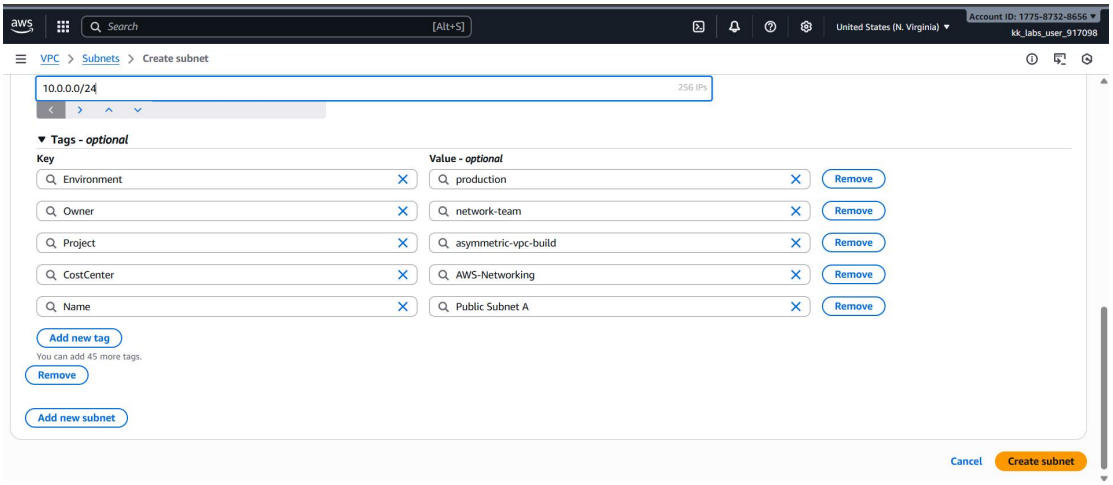
Creating subnets:



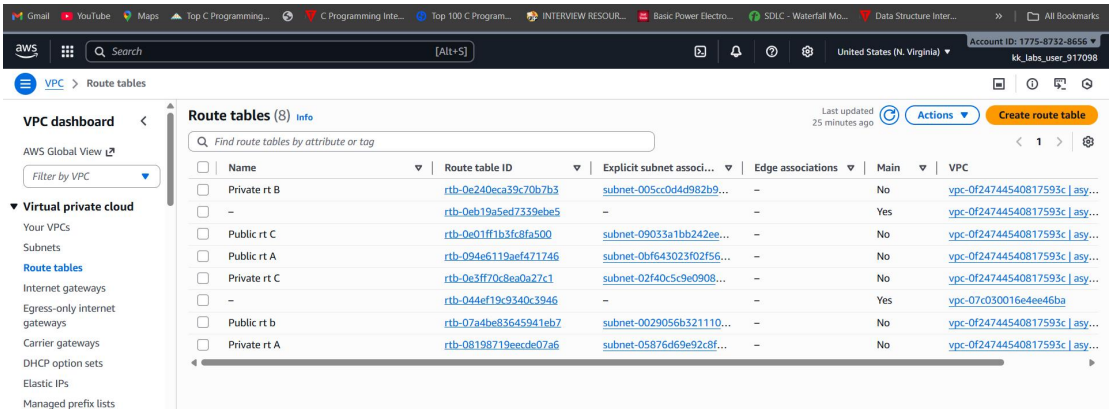
Select cidr range



Give tags



Cretae six submets with above CIDR values;



4. Route Table Creation and Subnet Association:

Route Tables, Subnet Associations, and Routes

1. Route Table Name: Public rt A
   - **Subnet Association:** Public Subnet A
   - **Routes:**
     - 0.0.0.0/0 → Internet Gateway (asymmetric-igw)

2. Route Table Name: Public rt B
   - **Subnet Association:** Public Subnet B
   - **Routes:**
     - 0.0.0.0/0 → Internet Gateway (asymmetric-igw)

3. Route Table Name: Public rt C
   - **Subnet Association:** Public Subnet C
   - **Routes:**
     - 0.0.0.0/0 → Internet Gateway (asymmetric-igw)

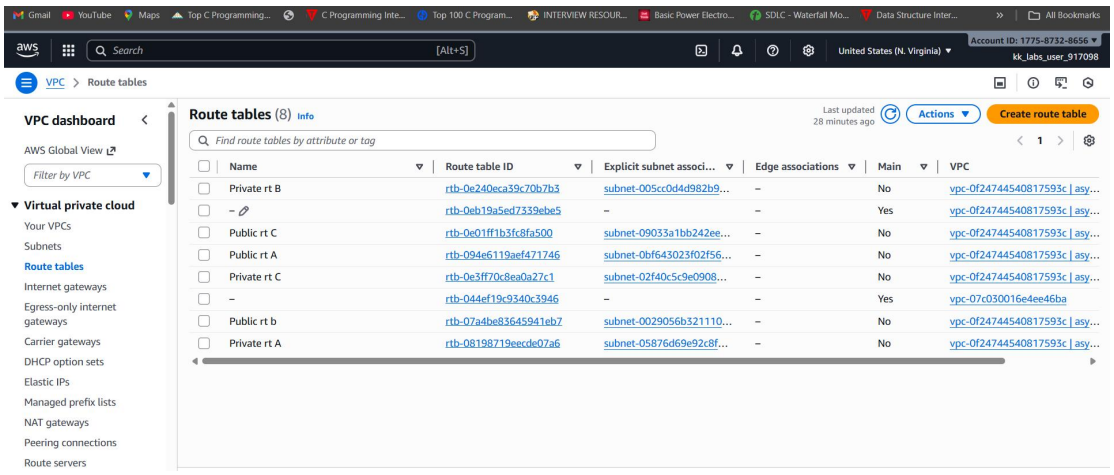
Private Route Tables:

1. **Route Table Name:** Private rt A
   - **Subnet Association:** Private Subnet A
   - **Routes:**
     - Local VPC route only (no internet route)

2. **Route Table Name:** Private rt B
   - **Subnet Association:** Private Subnet B
   - **Routes:**
     - Local VPC route only (no internet route)

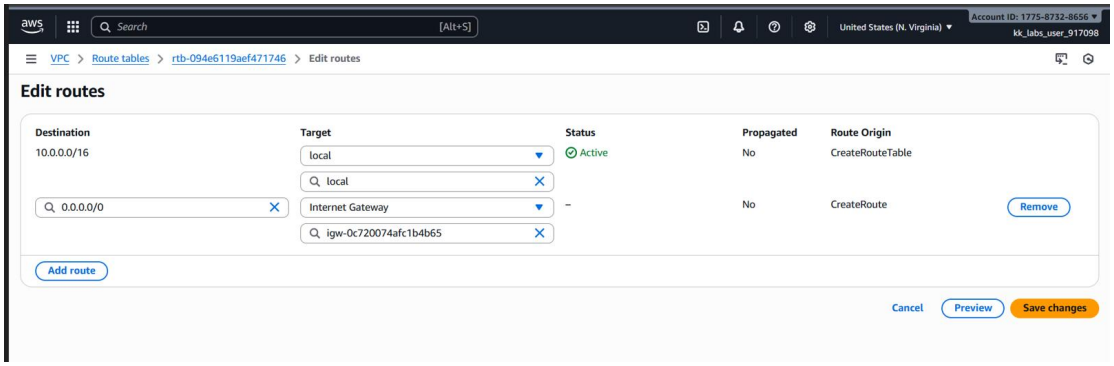
3. **Route Table Name:** Private rt C
   - **Subnet Association:** Private Subnet C
   - **Routes:**
     - Local VPC route only (no internet route)

Following are the route tables created.



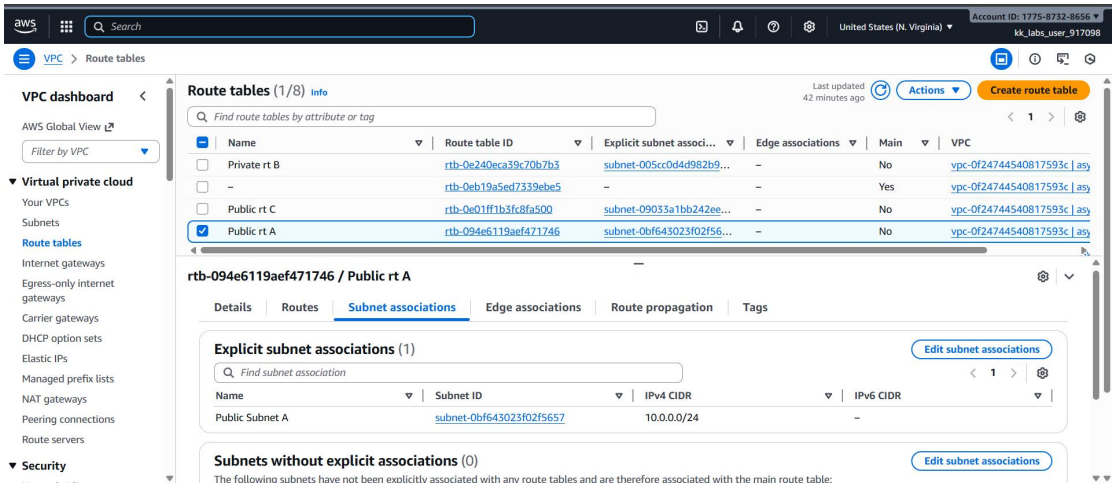
Add Routes to all the route tables

Select 0.0.0.0/0 as destination, target as internet gateway and slect Internet gateway created. Do for all the route tables.



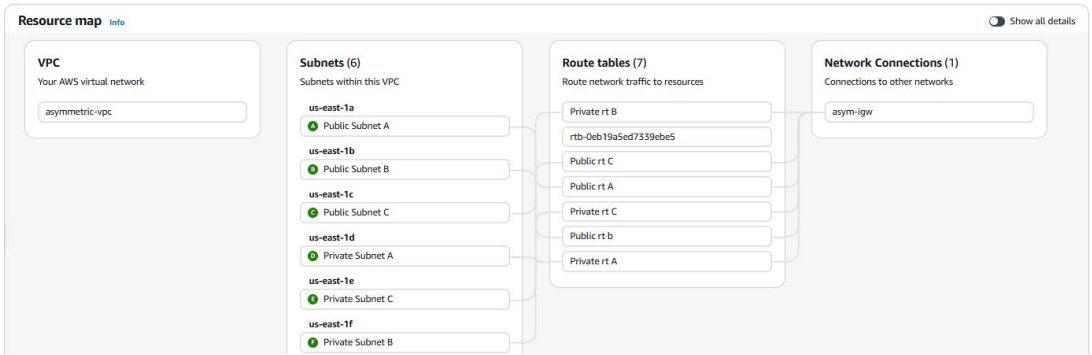
5.Edit Subnet Associations

Select the route table -----> scroll down----->goto subnet associations----->edit subnet association-----> selec the subnet you want to associate with the route table. Associate all the respective Route tables with the respective subnets accordingly.



6.ResourceMap of VPC:

Following is the ResourceMap of the VPC created.



7. **Conclusion:**

This asymmetric VPC architecture sets the stage for:

- Multi-tier application deployments
- Landing zone onboarding
- NAT / Transit Gateway expansion
- Cloud security posture alignment
- Hybrid network peering

Future Enhancements May Include:

- NAT Gateway for private outbound internet
- VPC Endpoints for S3 / DynamoDB
- Transit Gateway for multi-VPC communication

The network is primed for elastic scaling, security compliance, and production workload enablement.