

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**.

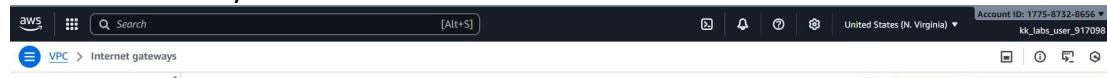
Enable **DNS resolution** and **DNS hostnames**.

Tag all resources with:

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

2. Internet Gateway:

Internet Gateway Creation



Name	Internet gateway ID	State	VPC ID	Owner
asym-igw	igw-0c720074afc1b4b65	Attached	vpc-0f24744540817593c asymmetric...	177587328656
-	igw-0d5ccf09e9be62421	Attached	vpc-07c030016e4ee46ba	177587328656

Attachment to VPC.

Attach to VPC (igw-0c720074afc1b4b65) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the Internet gateway to this VPC.

[X](#)

▶ AWS Command Line Interface command

[Cancel](#) [Attach internet gateway](#)

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:

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.
vpc-0f24744540817593c (asymmetric-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public Subnet A

Select cidr range

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

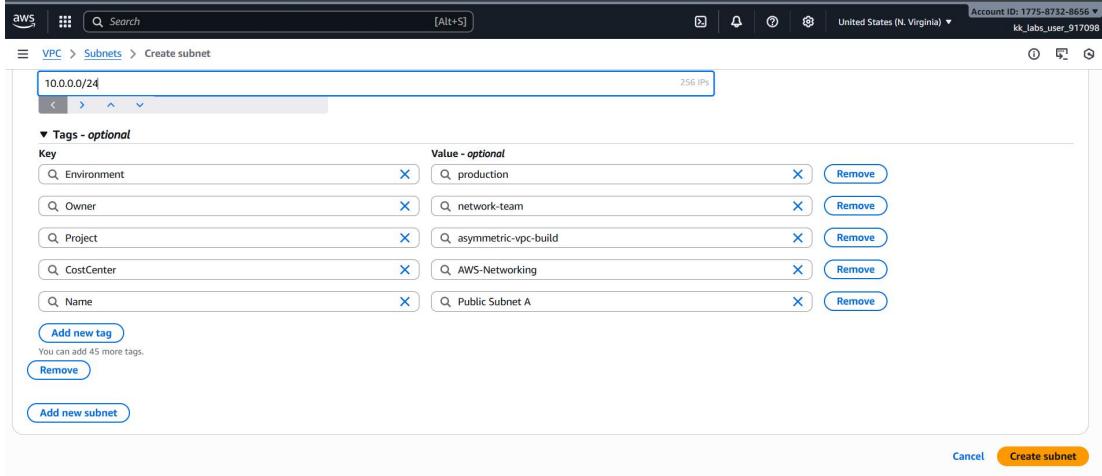
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public Subnet A
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.0/24 256 IPs
< > ^ v

Give tags



Create six subnets with above CIDR values;

Route tables (8) <small>Info</small>						
Last updated <small>25 minutes ago</small> Actions Create route table						
	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<input type="checkbox"/>	Private rt B	rtb-0e240eca39c70b7b3	subnet-005cc0d4d982b9...	-	No	vpc-0f24744540817593c asym...
<input type="checkbox"/>	-	rtb-0eb19a5ed7359ebe5	-	-	Yes	vpc-0f24744540817593c asym...
<input type="checkbox"/>	Public rt C	rtb-0e01ff1b3fc8fa500	subnet-09033a1bb242ee...	-	No	vpc-0f24744540817593c asym...
<input type="checkbox"/>	Public rt A	rtb-094e6119ae4f71746	subnet-0bf643023f02f56...	-	No	vpc-0f24744540817593c asym...
<input type="checkbox"/>	Private rt C	rtb-0e3ff70c8ea0a27c1	subnet-02f40c5c9e0908...	-	No	vpc-0f24744540817593c asym...
<input type="checkbox"/>	-	rtb-044ef19c9340c3946	-	-	Yes	vpc-0f24744540817593c asym...
<input type="checkbox"/>	Public rt b	rtb-07a4be83645941eb7	subnet-0029056b321110...	-	No	vpc-0f24744540817593c asym...
<input type="checkbox"/>	Private rt A	rtb-08198719eecde07a6	subnet-05876d69e92c8f...	-	No	vpc-0f24744540817593c asym...

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.

Name	Route table ID	Explicit subnet association	Main	VPC
Private rt B	rtb-0e240eca39c70b7b3	subnet-005cc0d4d982b9...	No	vpc-0f24744540817593c asy...
-	rtb-0eb19a5ed7339ebe5	-	Yes	vpc-0f24744540817593c asy...
Public rt C	rtb-0e01ff1b3fc8fa500	subnet-09033a1bb242ee...	No	vpc-0f24744540817593c asy...
Public rt A	rtb-094e6119aeaf471746	subnet-0fb643023f02f56...	No	vpc-0f24744540817593c asy...
Private rt C	rtb-0e3ff70c8ea0a27c1	subnet-02f40c5c9e0908...	No	vpc-0f24744540817593c asy...
-	rtb-044ef9c9340c3946	-	Yes	vpc-07c030164eee46b...
Public rt b	rtb-07a4be83645941eb7	subnet-0029056b321110...	No	vpc-0f24744540817593c asy...
Private rt A	rtb-08198719eecde07a6	subnet-05876d69e92c8f...	No	vpc-0f24744540817593c asy...

Add Routes to all the route tables

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

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway	-	No	CreateRoute

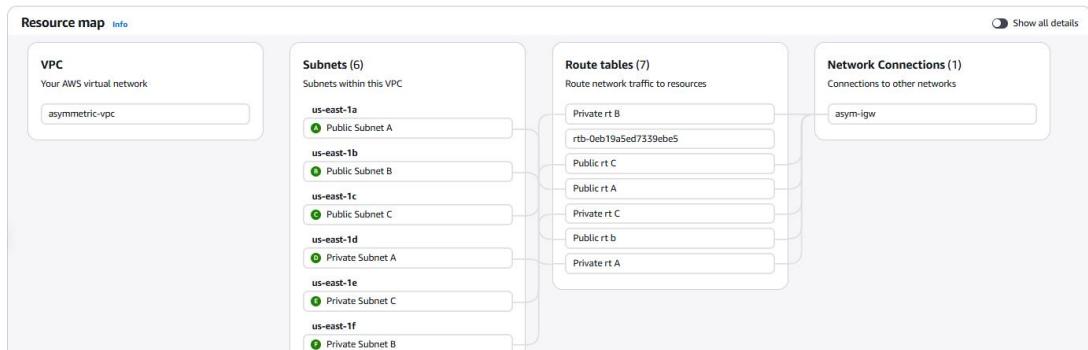
5.Edit Subnet Associations

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.

The screenshot shows the AWS VPC Route Tables page. On the left, there's a navigation sidebar with options like 'VPC dashboard', 'AWS Global View', 'Virtual private cloud', 'Route tables' (which is selected), and 'Security'. The main area displays a table titled 'Route tables (1/8)'. It lists four route tables: 'Private rt B', 'Public rt C', and 'Public rt A' (selected). Each row includes columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. Below the table, a specific route table ('rtb-094e6119aef471746 / Public rt A') is selected, showing its details: 'Details', 'Routes', 'Subnet associations' (which is selected), 'Edge associations', 'Route propagation', and 'Tags'. Under 'Subnet associations', it shows 'Explicit subnet associations (1)' with one entry: 'Public Subnet A' associated with 'subnet-0bf643023f02f567' and 'IPv4 CIDR 10.0.0.0/24'. There's also a section for 'Subnets without explicit associations (0)'.

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.

