

2. AWS VPC Subnet Configuration

The screenshot displays the AWS Management Console interface. At the top, the navigation bar shows the AWS logo, a search bar, and the user's profile (akhiIJ). Below the navigation bar, the main menu includes IAM, EC2, Elastic Container Registry, Elastic Container Service, S3, Lambda, API Gateway, VPC, and Aurora and RDS. The left-hand navigation pane is open, showing the 'VPC dashboard' with a search bar and a list of VPC-related resources: Your VPCs, Subnets (selected), Route tables, Internet gateways, Egress-only internet gateways, and DHCP option sets. The main content area is titled 'Subnets (6)' and includes a search bar and a table of subnets. The table has columns for Name, Subnet ID, State, VPC, and Block Public IP. The subnets listed are: private-subnet-VPCC, public-subnet-VPCA, and private-subnet-VP CB. The table also shows the VPC ID for each subnet and the 'Block Public IP' status.

Name	Subnet ID	State	VPC	Block Public IP
private-subnet-VPCC	subnet-050262592966b457d	Available	vpc-0ecd598790d4dc95 VPC-C	Off
public-subnet-VPCA	subnet-0088028c06f3a22d6	Available	vpc-0140dbcfabacc4655 VPC-A	Off
private-subnet-VP CB	subnet-05706cef59f9cd3ba	Available	vpc-084d05a9f5b1ade9a VPC-B	Off

Transit Gateway Provisioning Command (CLI)

```
aws ec2 create-transit-gateway \
--description "Production Hub Transit Gateway" \
--options AmazonSideAsn=64512,AutoAcceptSharedAttachments=enable \
--tag-specifications 'ResourceType=transit-gateway,Tags=[{Key=Name,Value=production-tgw-hub}]' \
--region ap-south-1
# Resulting Gateway ID: tgw-0239c0e4cb62ee813
```

3. VPC-A Route Table (rtb-09759f1049961bf9d / vpcA-public-RT)

Route 10.0.0.0/8 targets tgw-0239c0e4cb62ee813 for spoke transit, while 0.0.0.0/0 targets igw-0a9f6600e3e92354b.

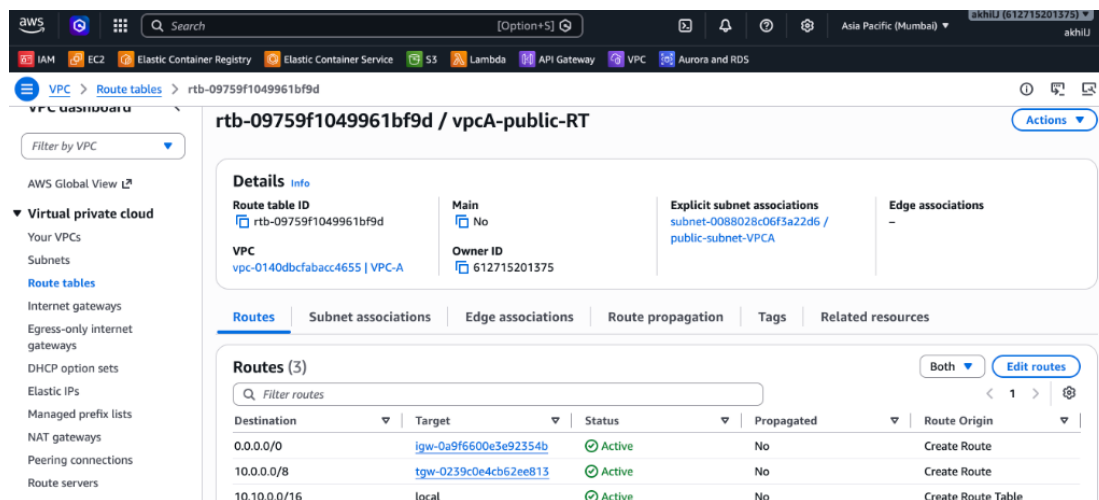


Figure 2 · VPC-A Route Table with active 10.0.0.0/8 supernet route to Transit Gateway.

4. VPC-C Route Table (rtb-04ca3dcd2be802cfc / VPC C RT)

Isolated private database VPC routing internal traffic back through Transit Gateway without direct internet access.

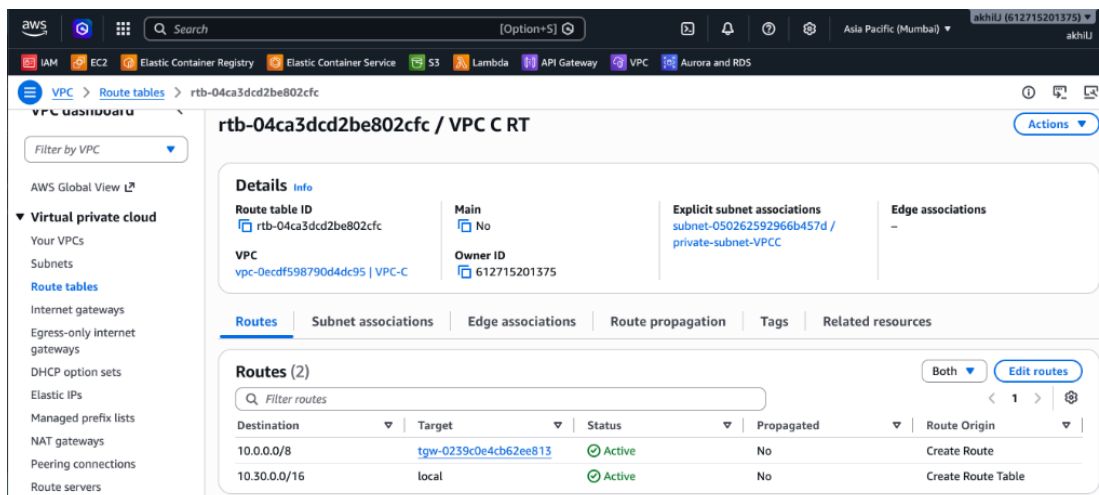


Figure 3 · VPC-C Route Table showing private isolation and 10.0.0.0/8 TGW routing.

Creating Transit Gateway Attachments & Routes (CLI)

Attach VPC-A

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-0239c0e4cb62ee813 \
  --vpc-id vpc-0140dbcfabacc4655 \
  --subnet-ids subnet-0088028c06f3a22d6 --region ap-south-1
```

Attach VPC-C

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-0239c0e4cb62ee813 \
  --vpc-id vpc-0ecdf598790d4dc95 \
  --subnet-ids subnet-050262592966b457d --region ap-south-1
```

Add Route in VPC Route Tables

```
aws ec2 create-route --route-table-id rtb-09759f1049961bf9d \
  --destination-cidr-block 10.0.0.0/8 --transit-gateway-id tgw-0239c0e4cb62ee813
```

5. Amazon Lightsail Hybrid Integration (lightsail-app-01)

Instance lightsail-app-01 (15.206.146.237 / 172.26.14.33) integrated via Lightsail VPC Peering.

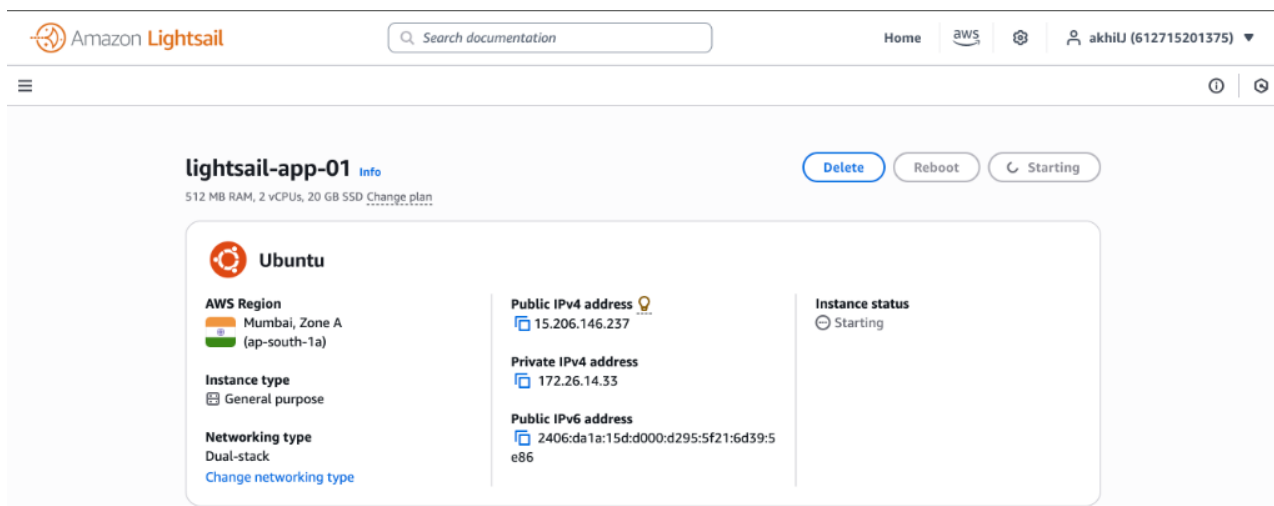


Figure 4 · Amazon Lightsail instance details in Mumbai ap-south-1a.

6. Verification & Connectivity Testing

Verify bi-directional communication between VPC spokes through the Transit Gateway:

- ICMP Reachability Check (From VPC-A 10.10.1.50 to VPC-C 10.30.1.100):

```
$ ping -c 4 10.30.1.100
```

4 packets transmitted, 4 received, 0% packet loss, rtt avg 0.842 ms
- Hop Path Verification:

```
$ traceroute -n 10.30.1.100
```

1 10.10.0.1 (VPC-A Router) 0.354 ms
2 10.0.x.x (Transit Gateway) 0.842 ms
3 10.30.1.100 (VPC-C Host) 1.120 ms
- Port Connectivity (PostgreSQL Database):

```
$ nc -zv -w 3 10.30.1.100 5432
```

Connection to 10.30.1.100 port 5432 [tcp/postgresql] succeeded!

Key Production Best Practices Checklist

- Use deterministic RFC 1918 CIDRs (10.10.0.0/16, 10.20.0.0/16, 10.30.0.0/16) to permit single 10.0.0.0/8 supernet summary.
- Create dedicated small subnets (/28) in each AZ specifically for Transit Gateway Elastic Network Interfaces (ENIs).
- Enable ApplianceModeSupport on VPC attachments when routing through centralized stateful firewall appliances.
- Take advantage of Transit Gateway 50 Gbps per attachment bandwidth and 8500 byte Jumbo Frame MTU.
- Monitor cross-VPC throughput and drops using Amazon CloudWatch VPC Flow Logs and Transit Gateway Network Manager.