Enterprise AWS VPC Design & Implementation Document

Project Objective

Design and implement a **scalable, production-ready AWS VPC** that:

- Uses **multiple subnet sizes** based on workload demand
- Implements **correct routing and controlled internet access**
- Follows **enterprise CIDR planning best practices**
- Is **secure, expandable, auditable**, and suitable for long-term growth

1. Business Scenario

The organization is building a **shared cloud network platform** to host:

- Admin & operational services (bastion, ops tooling)
- Internet-facing edge and load balancers
- Web application tiers
- Backend application services
- Internal platforms and container workloads
- Large shared internal services

The network **must be designed once** and support **years of growth** without re-CIDR or re-architecture.

2. CIDR & Capacity Planning Strategy

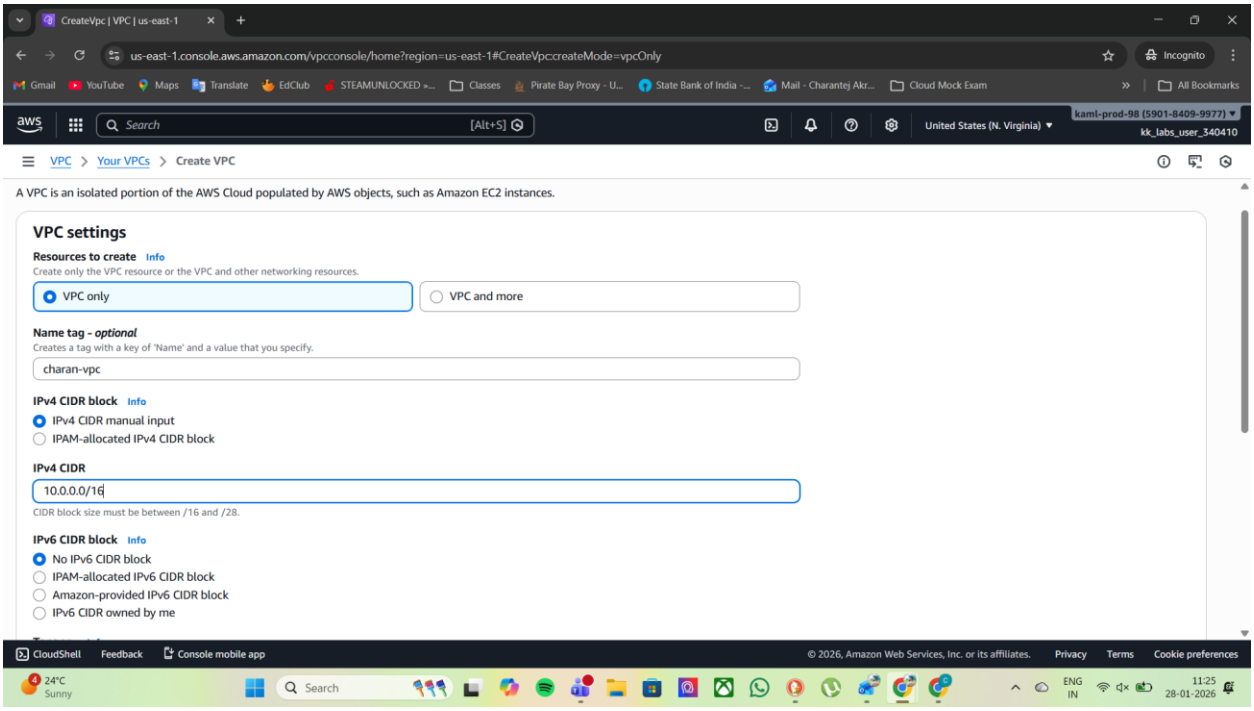
2.1 Why a /16 VPC CIDR

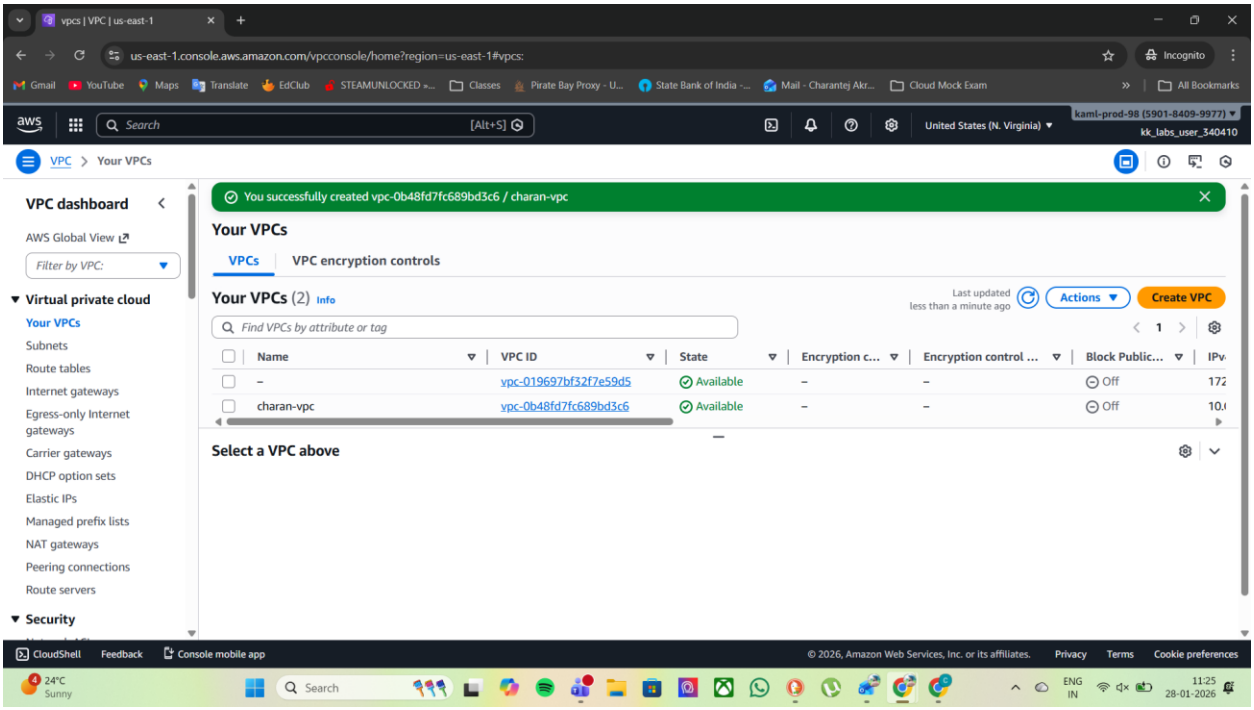
- Provides **65,536 IP addresses**
- Supports **large uneven subnet allocations**
- Allows **future subnet additions** without redesign
- Aligns with **AWS enterprise best practices**

Selected VPC CIDR

`10.0.0.0/16`

This CIDR provides a clean, private RFC1918 address space with predictable subnet boundaries.





3. Subnet Design Principles

Key Rules Applied

- Allocate **largest subnets first**
- Respect **binary CIDR boundaries**
- Ensure **no overlaps**
- Keep design **human-readable and auditable**

Failure to follow these rules results in:

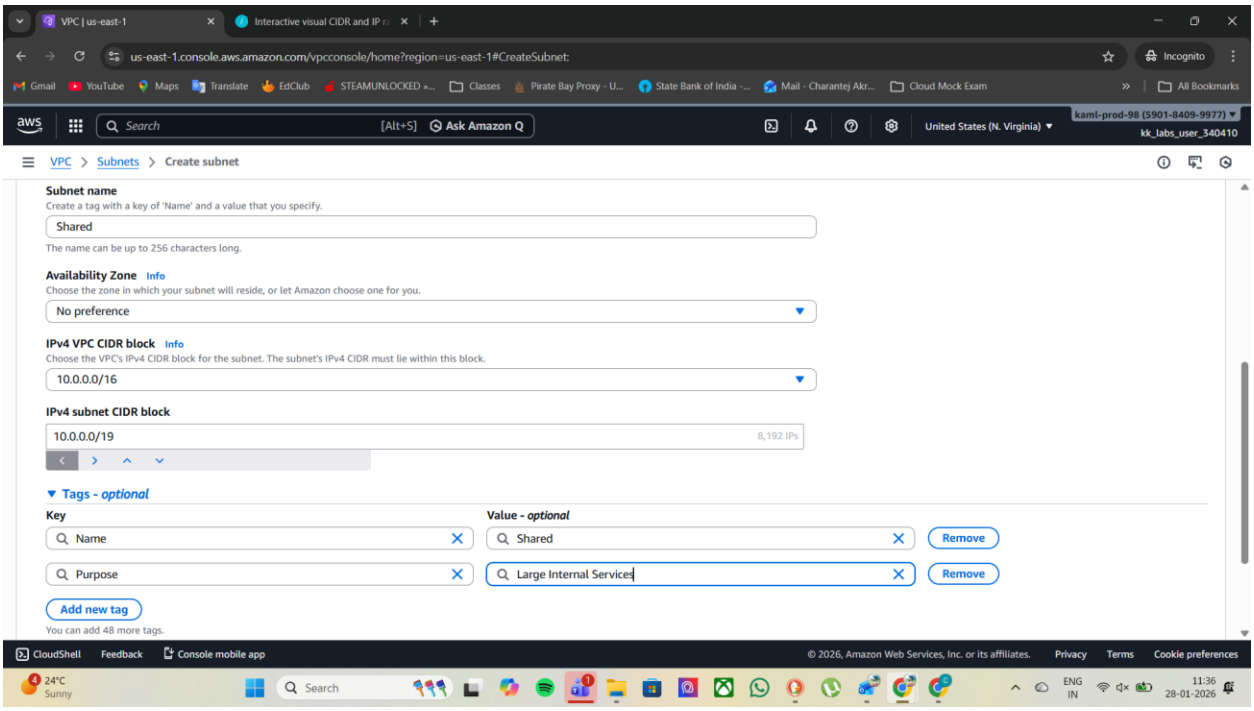
- Invalid CIDR blocks
- AWS rejection
- Broken routing and expansion limits

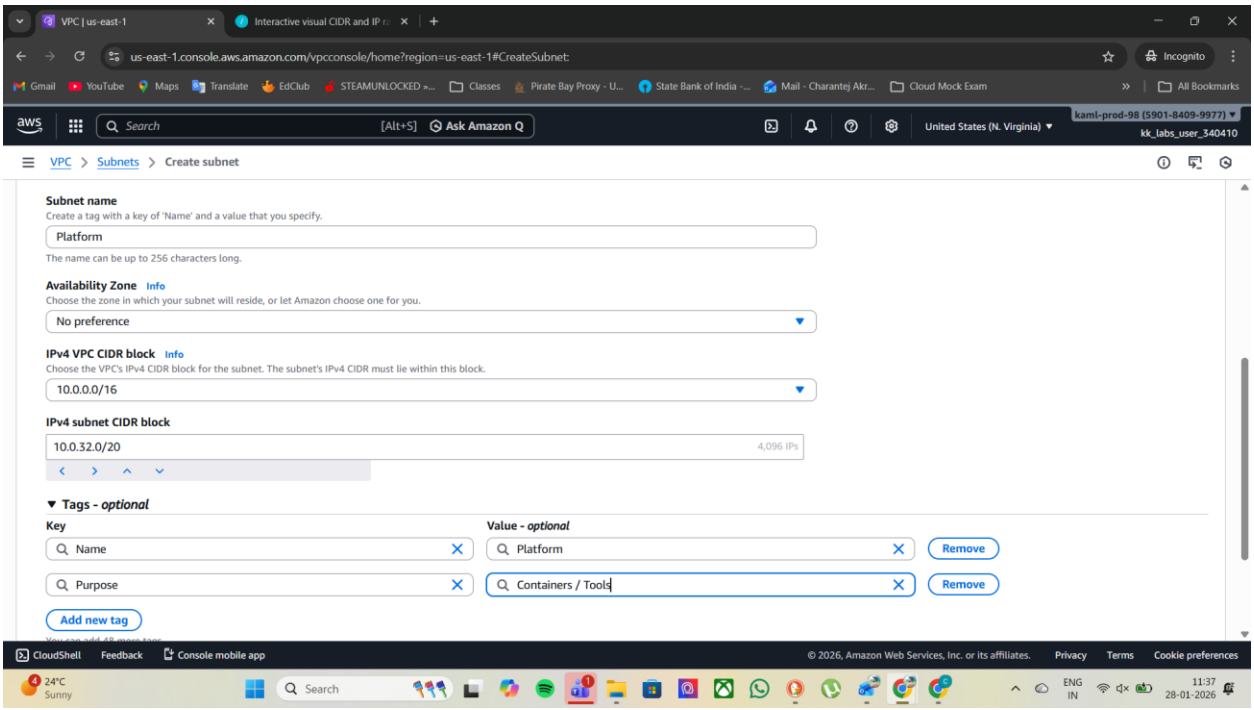
4. Subnet CIDR Allocation (6 Unequal Subnets)

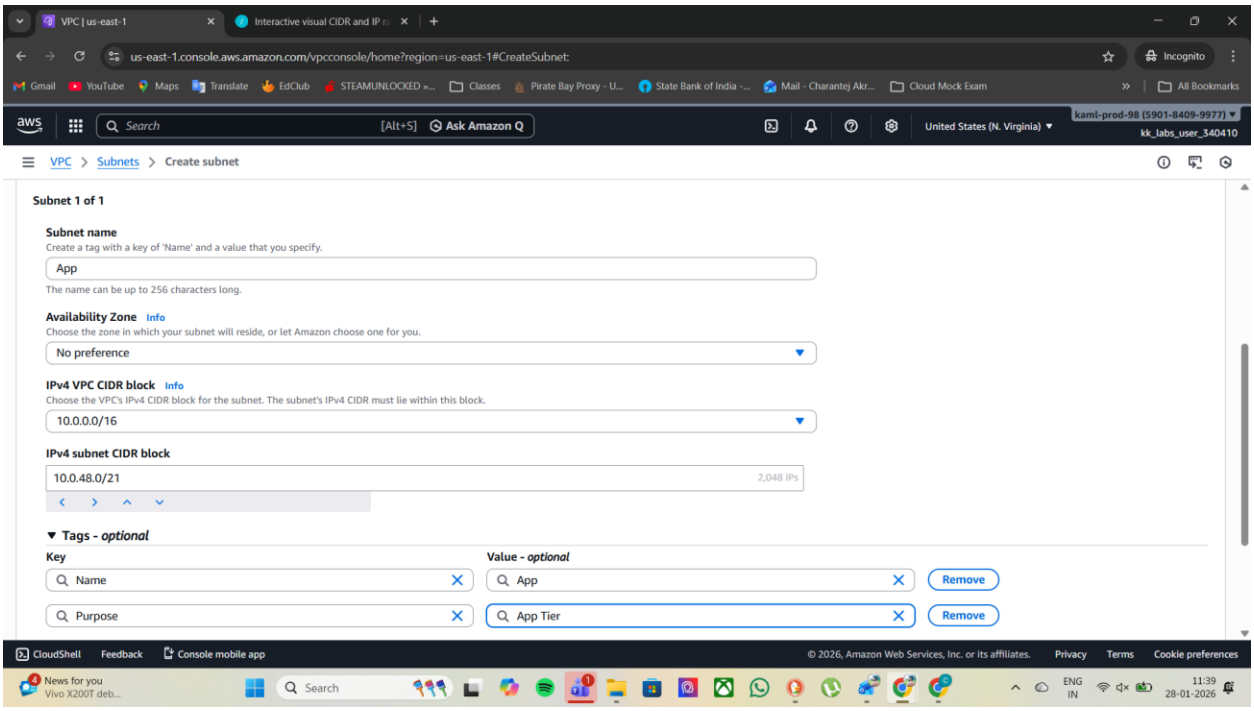
4.1 Subnet Allocation Table

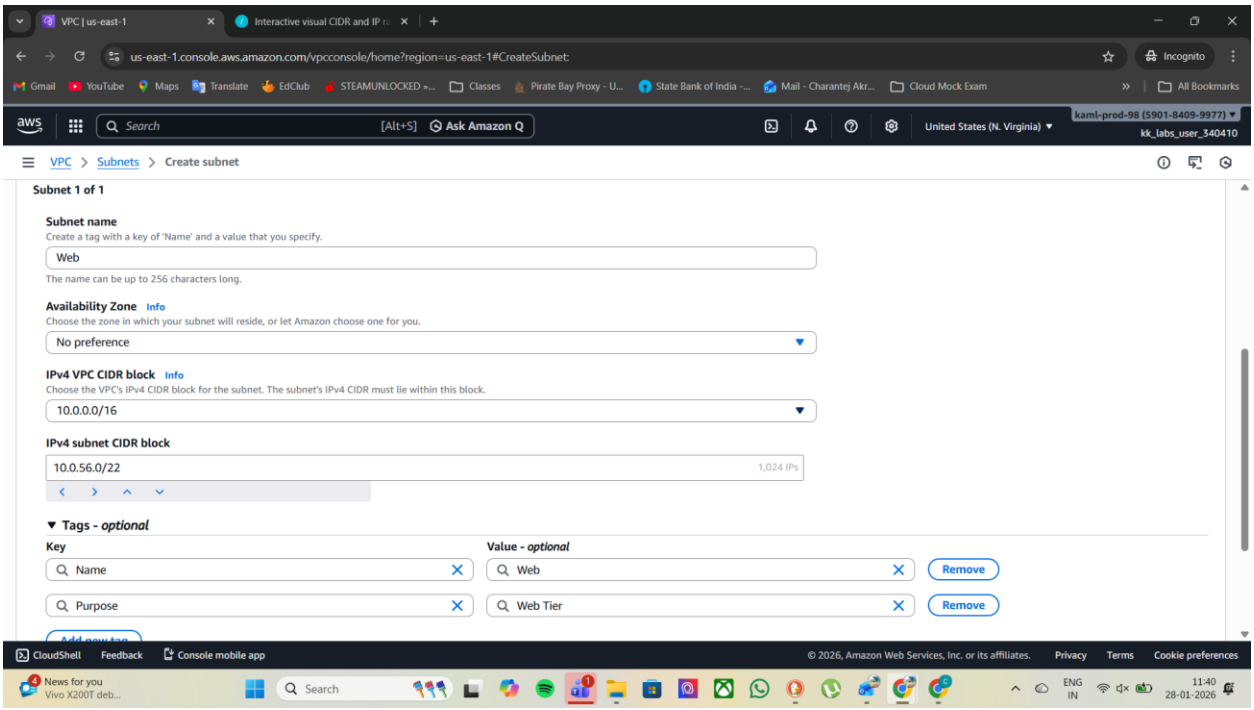
Subnet Name	Purpose	Required IPs	CIDR	Address Range
Shared	Large Internal Services	~8,192	/19	10.0.0.0 – 10.0.31.255
Platform	Containers / Tools	~4,096	/20	10.0.32.0 – 10.0.47.255
App	Application Tier	~2,048	/21	10.0.48.0 – 10.0.55.255
Web	Web Tier	~1,024	/22	10.0.56.0 – 10.0.59.255
Edge	Ingress / Load Balancers	~512	/23	10.0.60.0 – 10.0.61.255
Admin	Bastion / Ops	~256	/24	10.0.62.0 – 10.0.62.255

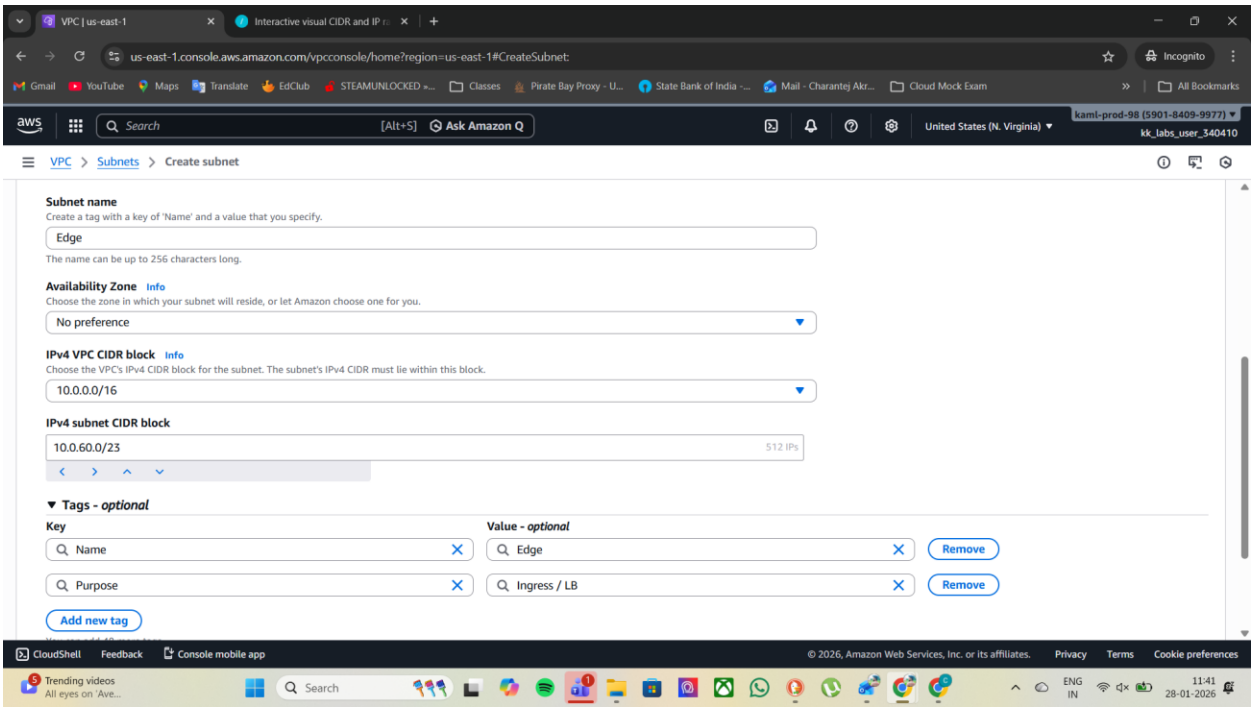
Remaining space (10.0.63.0 – 10.0.255.255) is **reserved for future growth**.

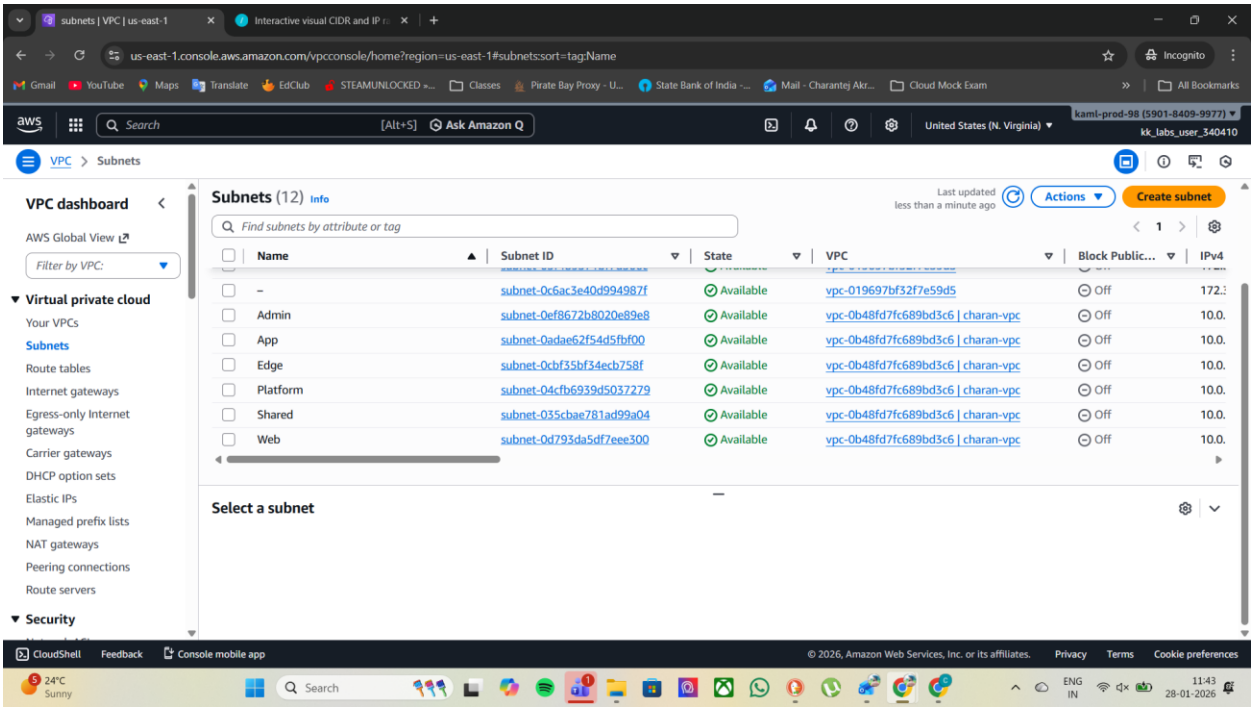

VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
Incognito
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets > Create subnet
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Shared
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.
No preference
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
10.0.0.0/19
8,192 IPs
Tags - optional
Key
Value - optional
Name
Shared
Remove
Purpose
Large Internal Services
Remove
Add new tag
You can add 48 more tags.
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
Search
ENG
IN
11:36
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
Incognito
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets > Create subnet
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Platform
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.
No preference
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
10.0.32.0/20
4,096 IPs
Tags - optional
Key
Value - optional
Name
Platform
Remove
Purpose
Containers / Tools
Remove
Add new tag
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
Search
ENG
IN
11:37
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
Incognito
All Bookmarks
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets > Create subnet
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
App
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.
No preference
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
10.0.48.0/21
2,048 IPs
Tags - optional
Key
Value - optional
Name
App
Remove
Purpose
App Tier
Remove
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
News for you
Vivo X200T deb...
Search
ENG
IN
11:39
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
Incognito
All Bookmarks
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets > Create subnet
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Web
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.
No preference
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
10.0.56.0/22
1,024 IPs
Tags - optional
Key
Value - optional
Name
Web
Remove
Purpose
Web Tier
Remove
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
News for you
Vivo X200T deb...
Search
ENG
IN
11:40
28-01-2026

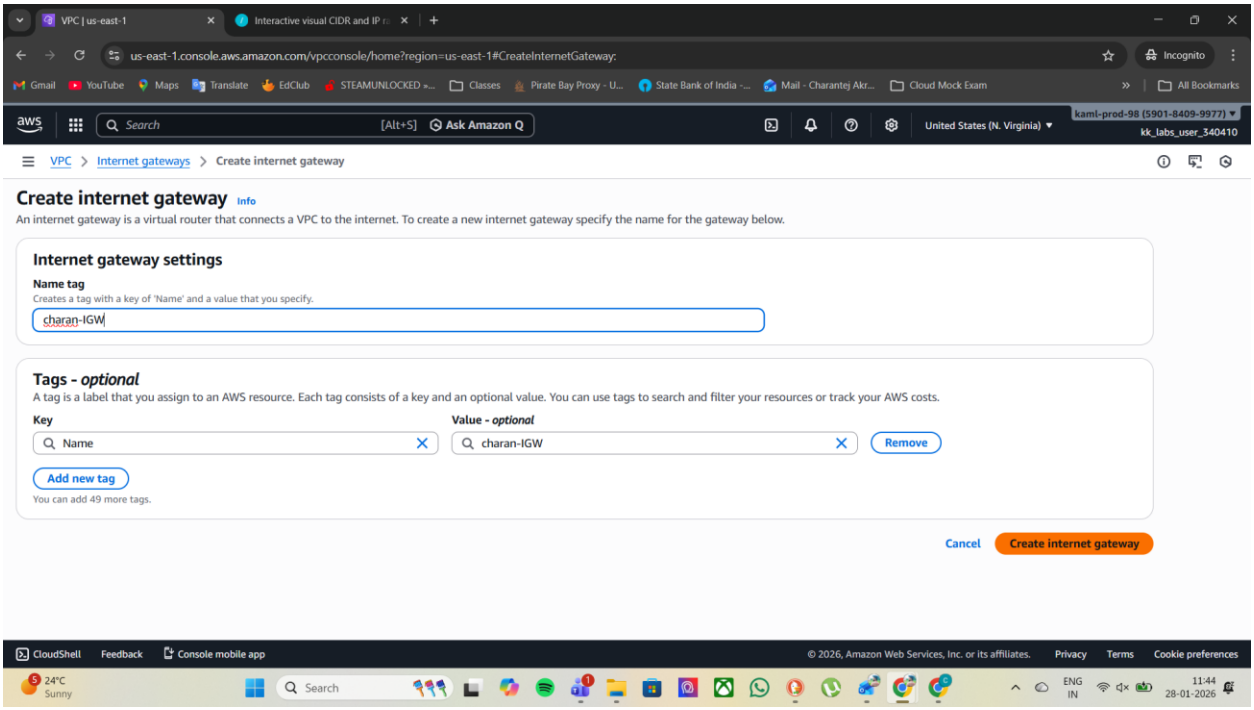

VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:
Incognito
All Bookmarks
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets > Create subnet
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Edge
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.
No preference
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
10.0.60.0/23
512 IPs
Tags - optional
Key
Value - optional
Name
Edge
Remove
Purpose
Ingress / LB
Remove
Add new tag
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Trending videos
All eyes on 'Ave...
Search
ENG
IN
11:41
28-01-2026

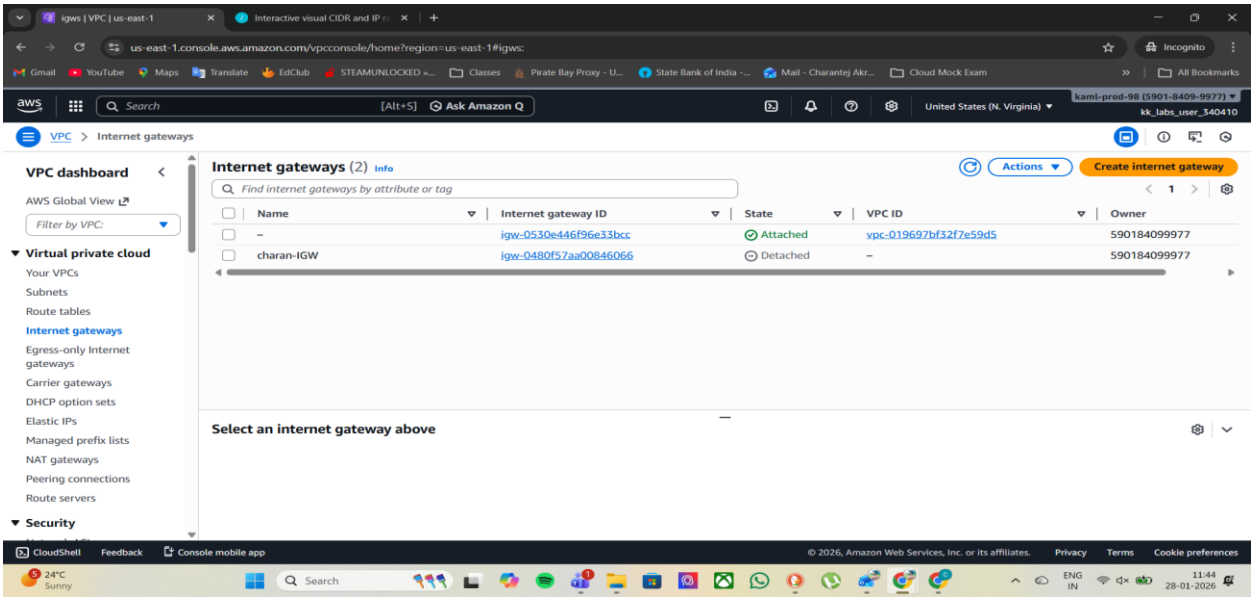

subnets | VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets:sort=tag:Name
Incognito
All Bookmarks
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Subnets
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Subnets (12) Info
Last updated less than a minute ago
Actions
Create subnet
Find subnets by attribute or tag
Name
Subnet ID
State
VPC
Block Public...
IPv4
– subnet-0c6ac3e40d994987f Available vpc-019697bf32f7e59d5 Off 172.
Admin subnet-0ef8672b8020e89e8 Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
App subnet-0adae62f54d5fbf00 Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
Edge subnet-0cbf35bf34ecb758f Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
Platform subnet-04cfb6939d5037279 Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
Shared subnet-035cbae781ad99a04 Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
Web subnet-0d793da5df7eee300 Available vpc-0b48fd7fc689bd3c6 | charan-vpc Off 10.0.
Select a subnet
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
Search
ENG
IN
11:43
28-01-2026

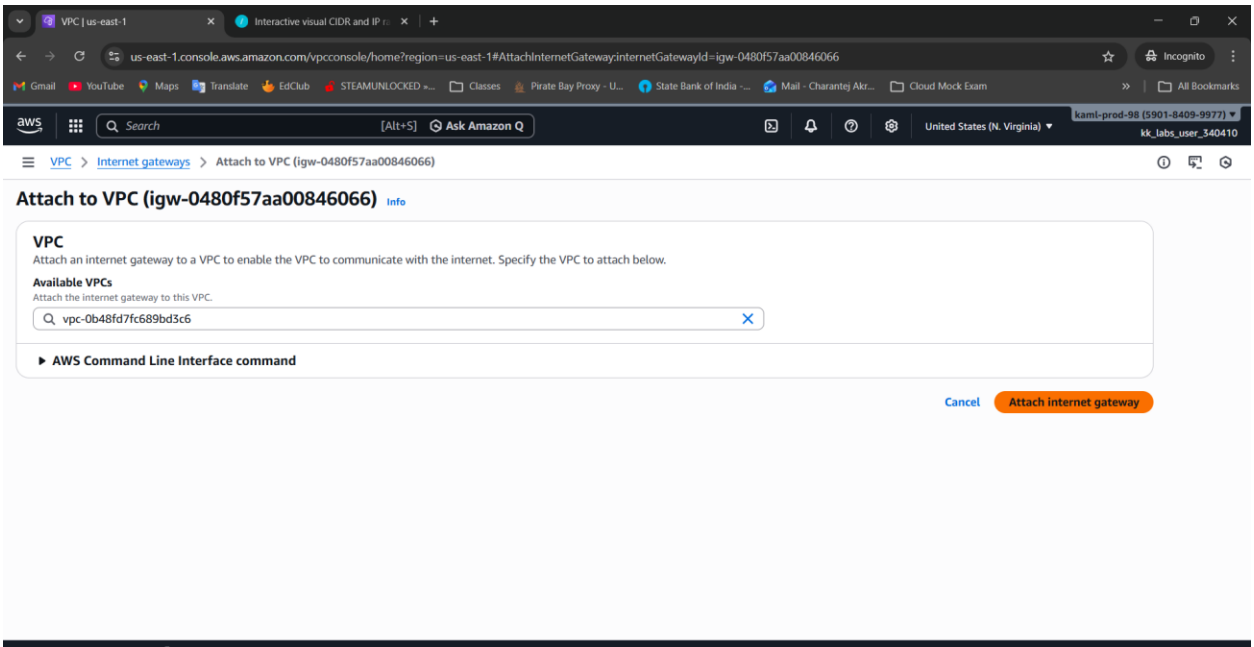
5. Internet Gateway Design

5.1 Internet Gateway (IGW)

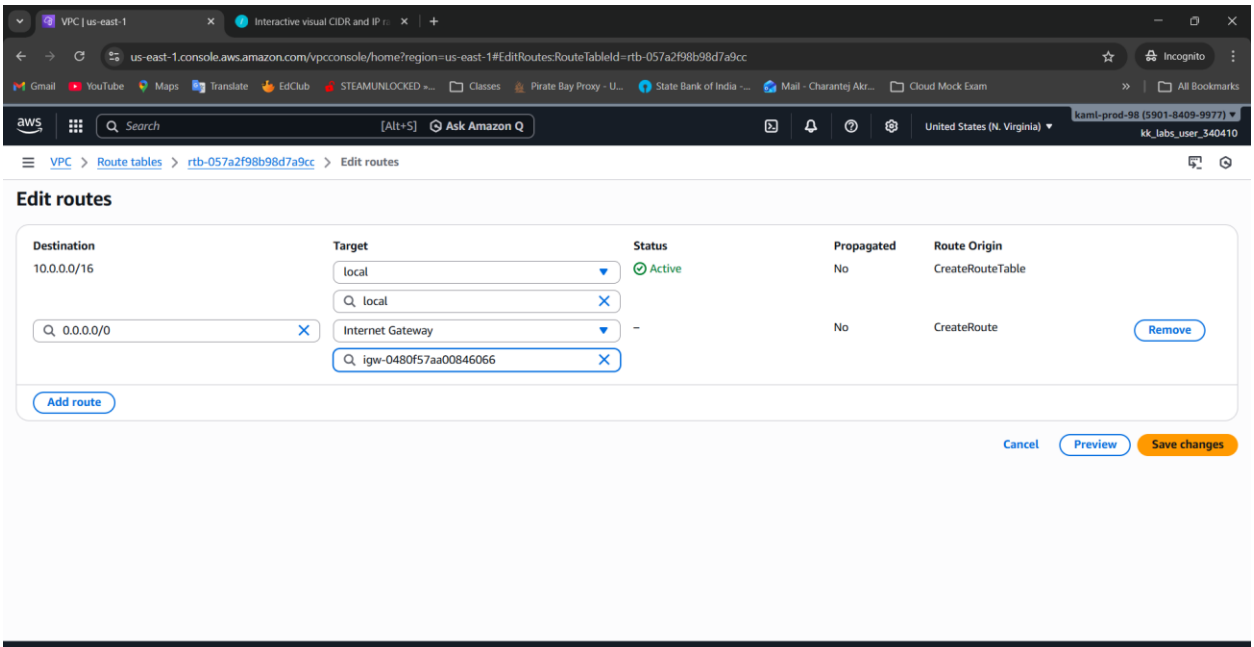
- A **single Internet Gateway** is created
- Attached directly to the VPC
- Enables internet routing **only where explicitly allowed**



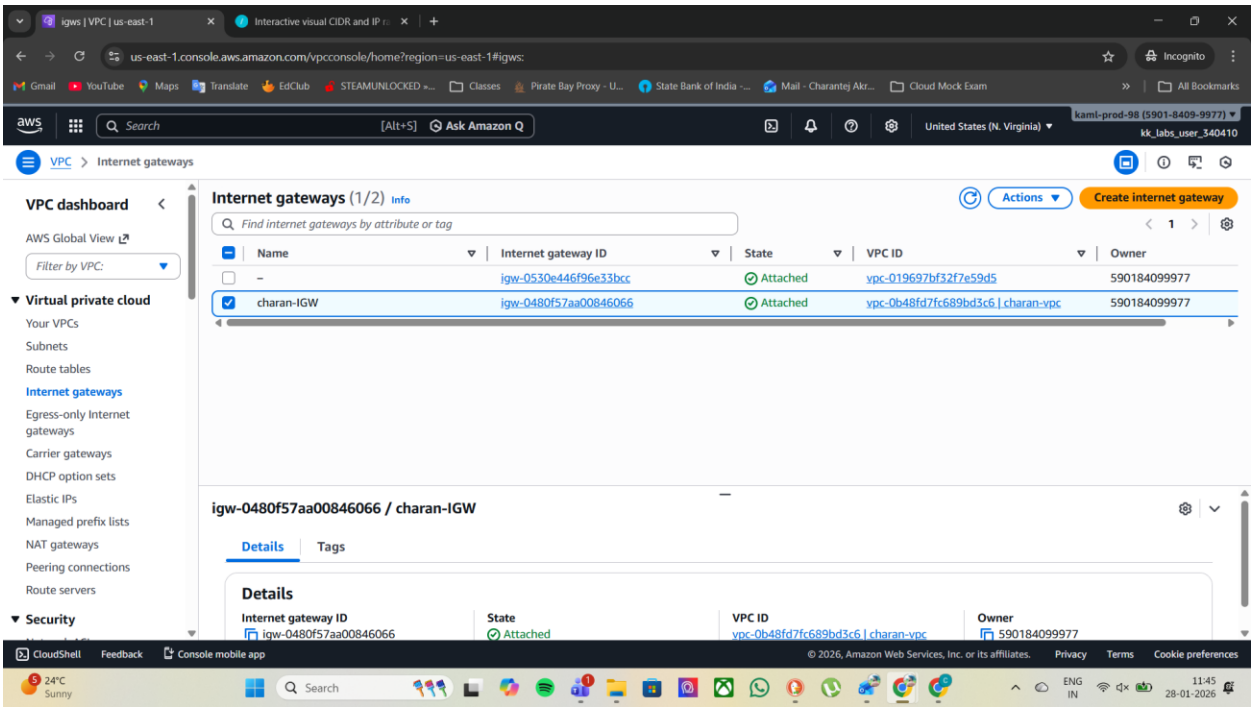



VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#AttachInternetGateway:internetGatewayId=igw-0480f57aa00846066
Incognito
Gmail
YouTube
Maps
Translate
EdClub
STEAMUNLOCKED »...
Classes
Pirate Bay Proxy - U...
State Bank of India -...
Mail - Charantej Akr...
Cloud Mock Exam
All Bookmarks
aws
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC
Internet gateways
Attach to VPC (igw-0480f57aa00846066)
Attach to VPC (igw-0480f57aa00846066) 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.
vpc-0b48fd7fc689bd3c6
AWS Command Line Interface command
Cancel
Attach internet gateway


CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
Search
ENG
IN
11:45
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:RouteTableId=rtb-057a2f98b98d7a9cc
Incognito
Gmail
YouTube
Maps
Translate
EdClub
STEAMUNLOCKED »...
Classes
Pirate Bay Proxy - U...
State Bank of India -...
Mail - Charantej Akr...
Cloud Mock Exam
All Bookmarks
aws
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC
Route tables
rtb-057a2f98b98d7a9cc
Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
–
No
CreateRoute
Remove
igw-0480f57aa00846066
Add route
Cancel
Preview
Save changes


CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
Search
ENG
IN
11:48
28-01-2026

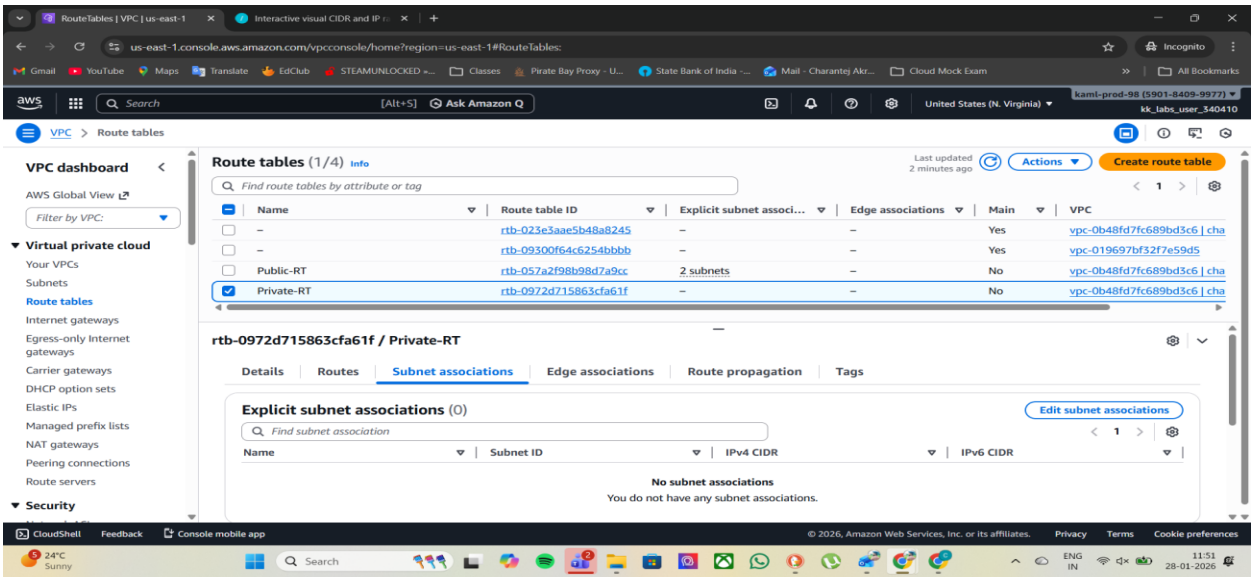


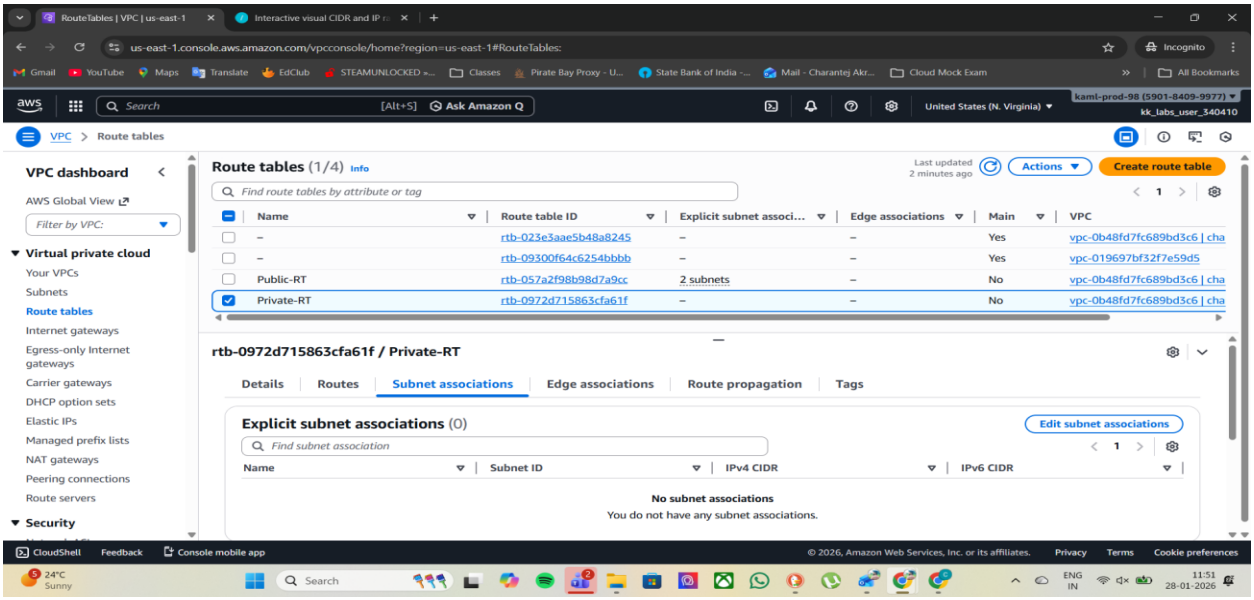
6. Route Table Architecture (Enterprise Model)

6.1 Route Tables Created

Route Table	Associated Subnets	Routes
Public-RT	Admin, Edge	10.0.0.0/16 → local0.0.0.0/0 → IGW
Private-RT	Web, App, Platform, Shared	10.0.0.0/16 → local

No NAT Gateway is used intentionally to **fully isolate private subnets**.





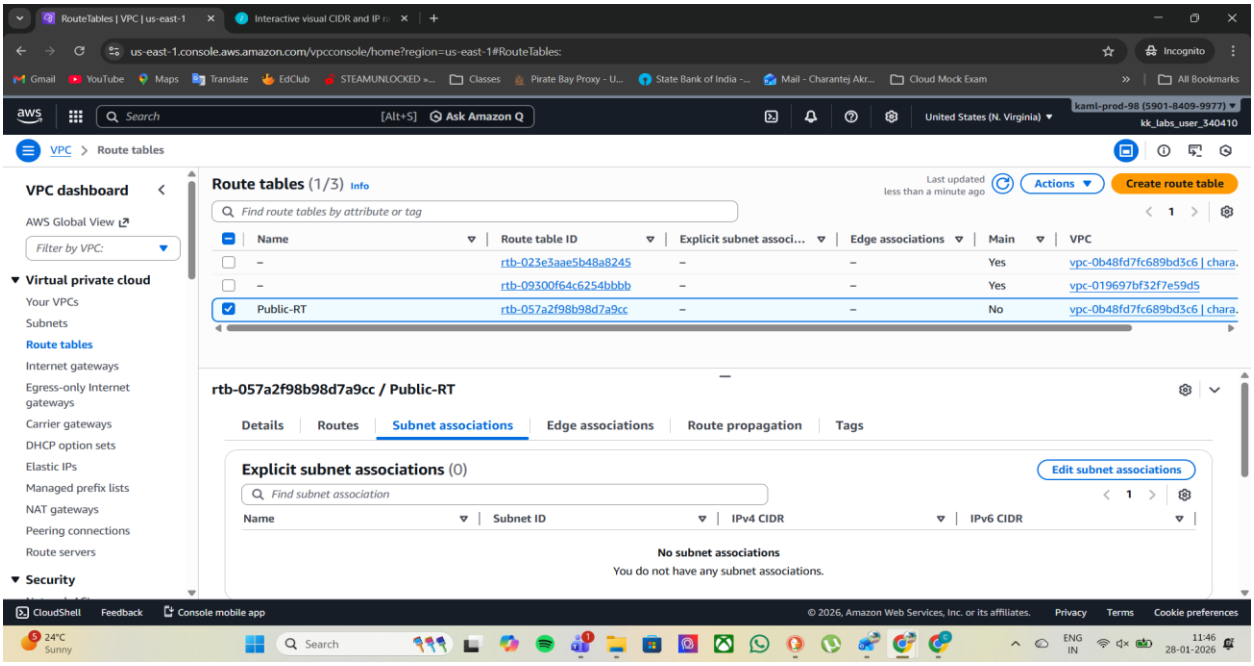
7. Route Table Associations

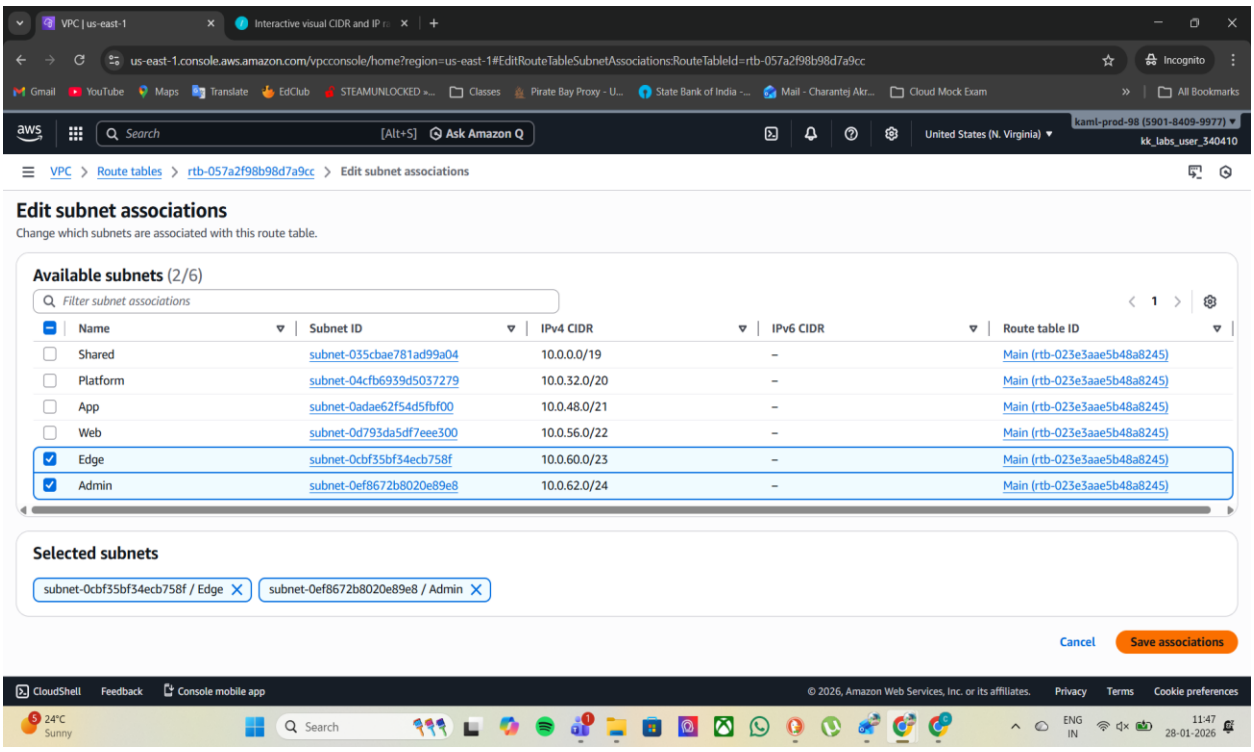
Explicit Associations

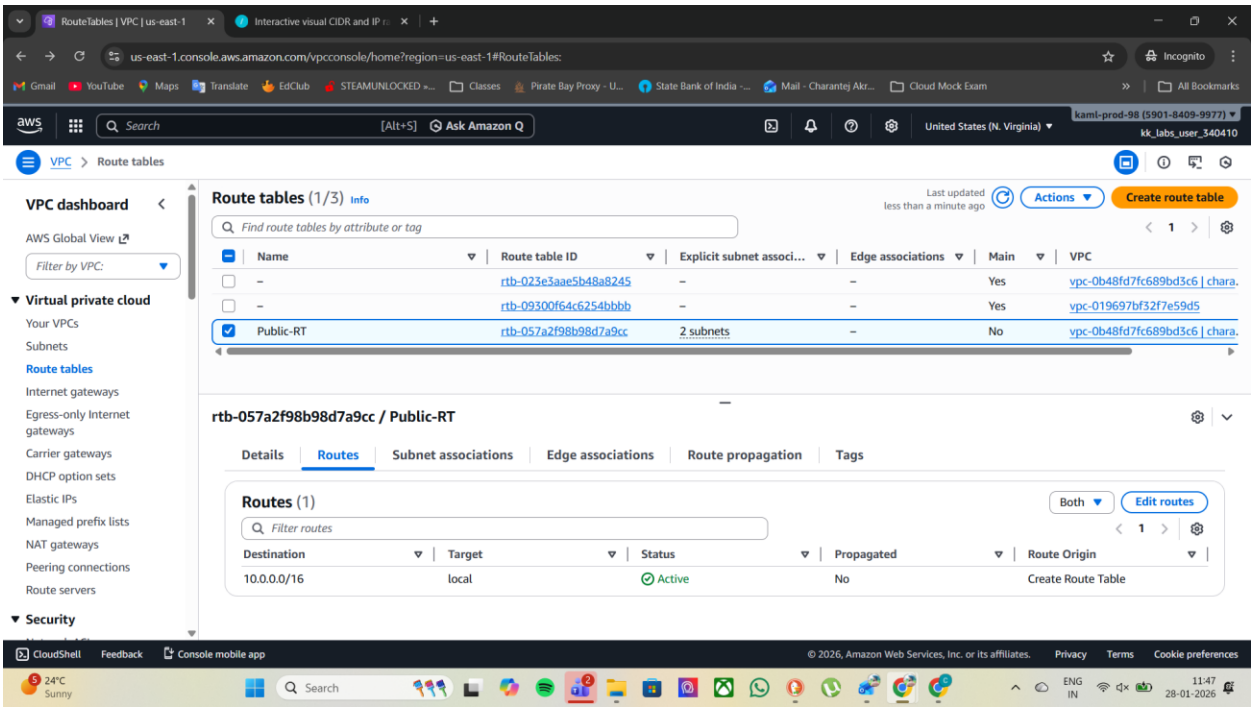
- **Admin subnet → Public-RT**
- **Edge subnet → Public-RT**
- **Web, App, Platform, Shared → Private-RT**

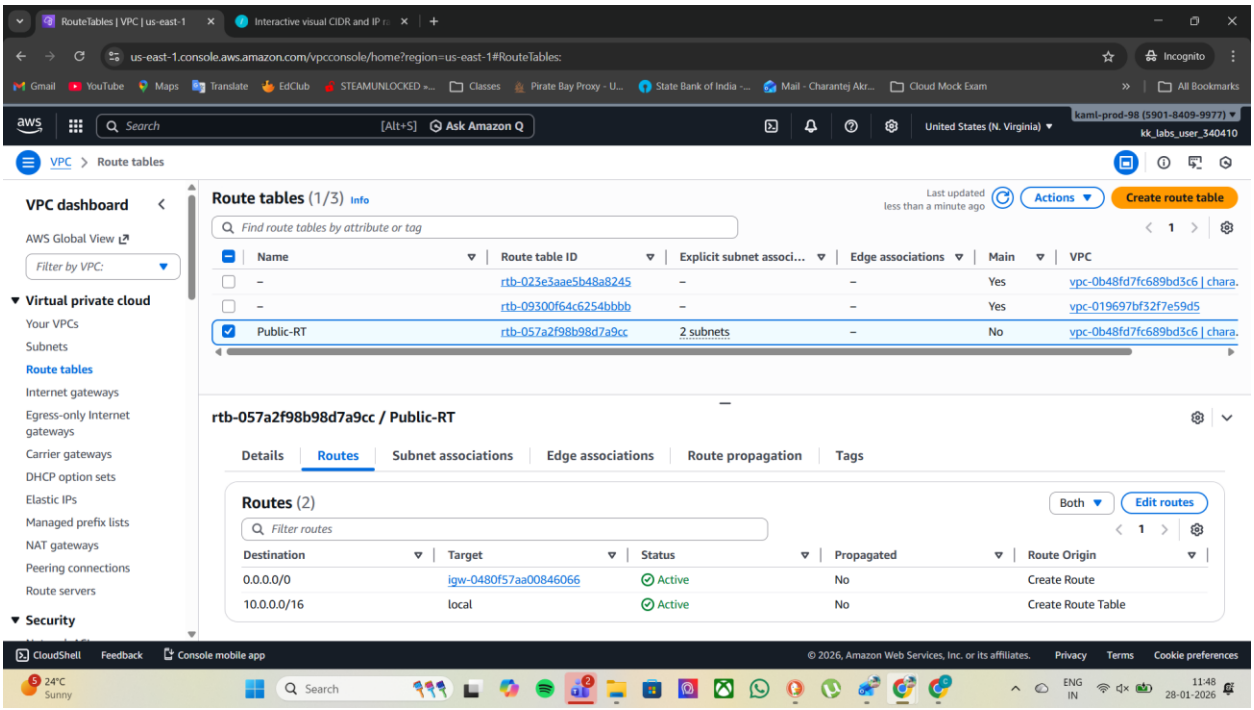
Validation Rule

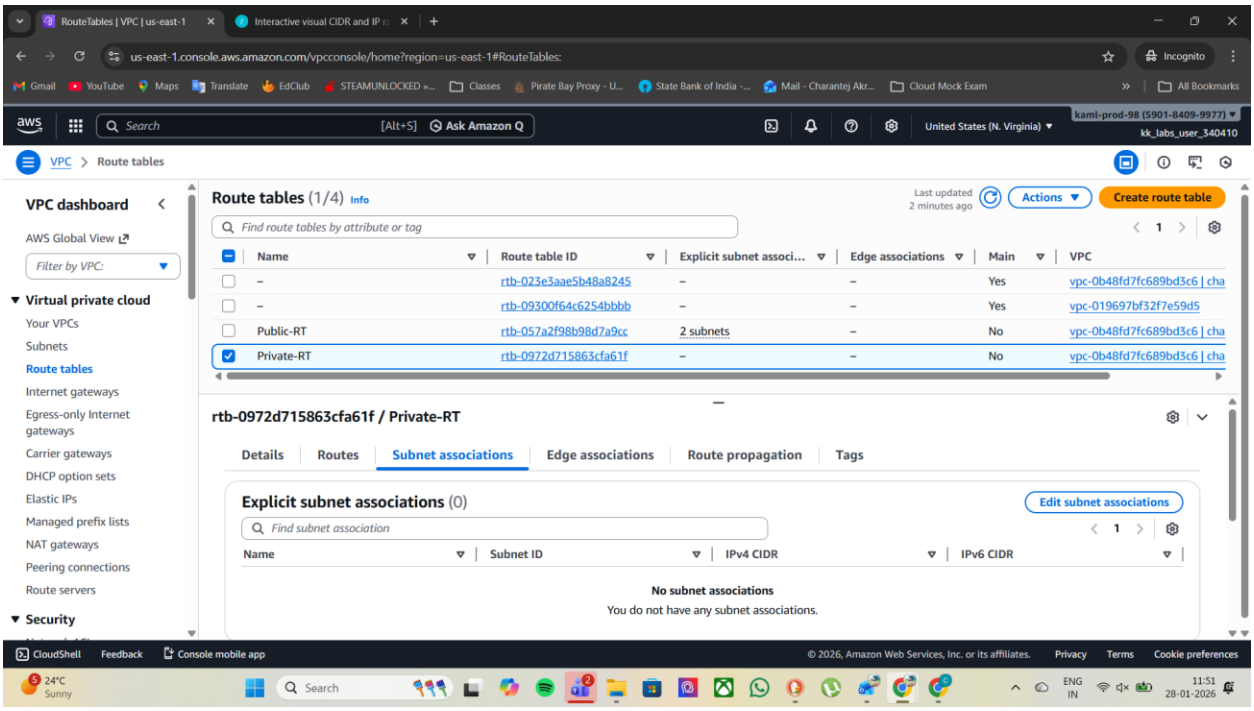
- No subnet uses the **main route table unintentionally**

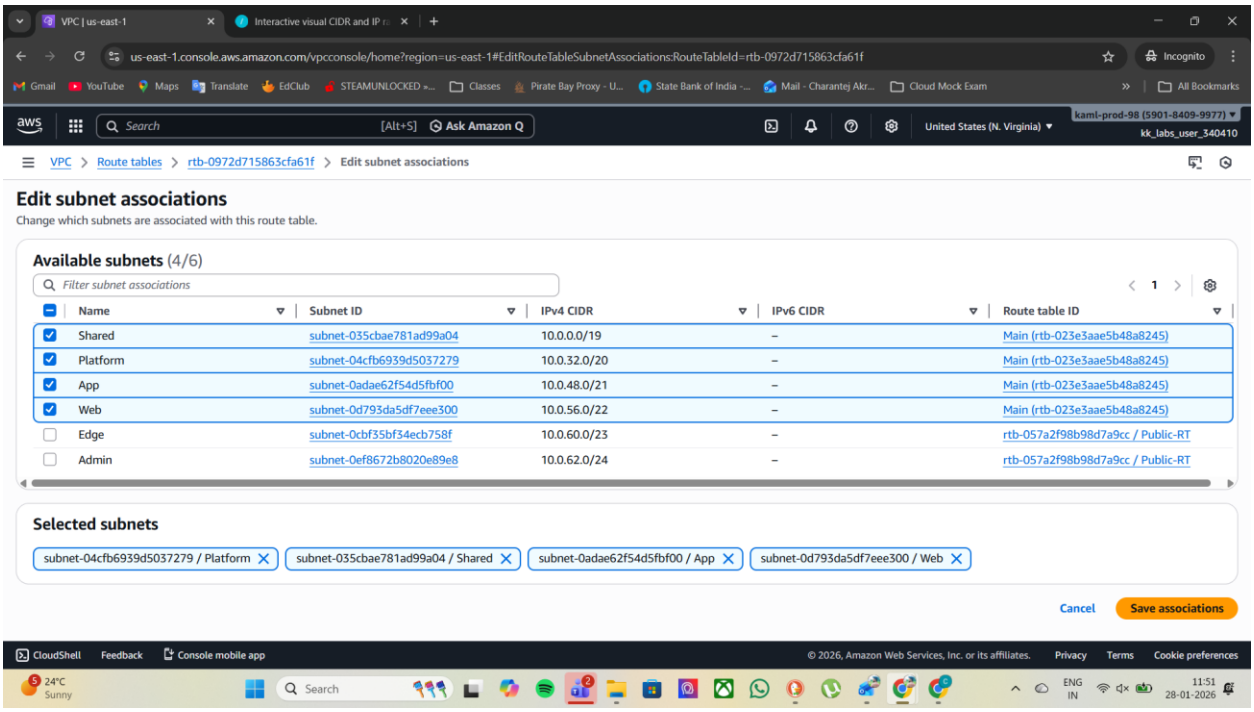


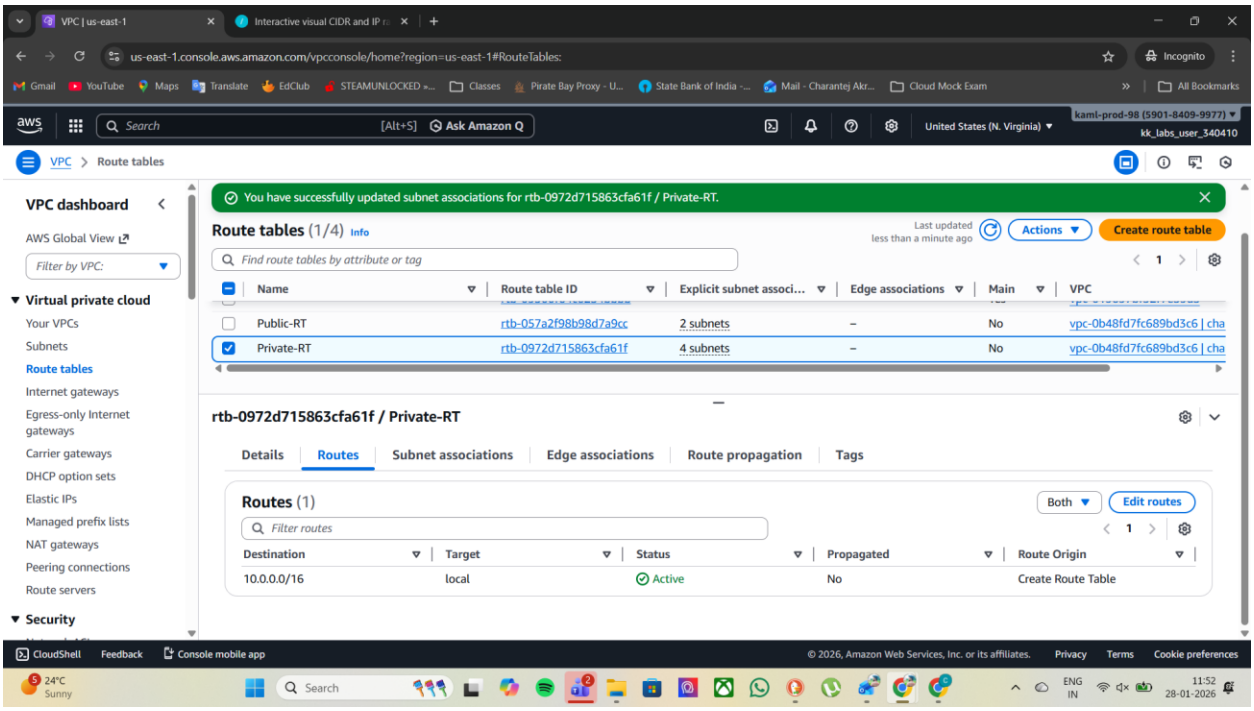


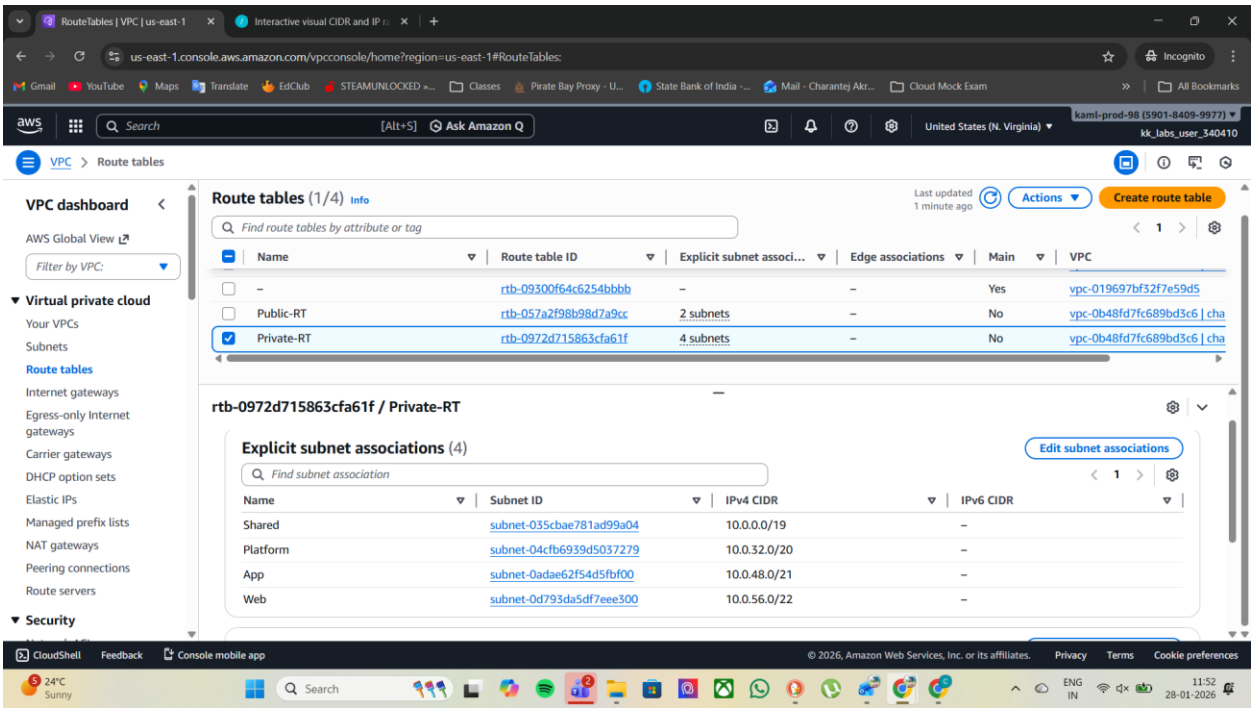

RouteTables | VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
Incognito
Gmail YouTube Maps Translate EdClub STEAMUNLOCKED »... Classes Pirate Bay Proxy - U... State Bank of India -... Mail - Charantej Akr... Cloud Mock Exam All Bookmarks
Search [Alt+S] Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Route tables (1/3) Info
Last updated less than a minute ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-023e3aae5b48a8245 – – Yes vpc-0b48fd7fc689bd3c6 | chara.
– rtb-09300f64c6254bbbb – – Yes vpc-019697bf32f7e59d5
Public-RT rtb-057a2f98b98d7a9cc 2 subnets – No vpc-0b48fd7fc689bd3c6 | chara.
rtb-057a2f98b98d7a9cc / Public-RT
Details Routes Subnet associations Edge associations Route propagation Tags
Routes (1)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16 local Active No Create Route Table
CloudShell Feedback Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
24°C Sunny
Search
ENG IN
11:47 28-01-2026

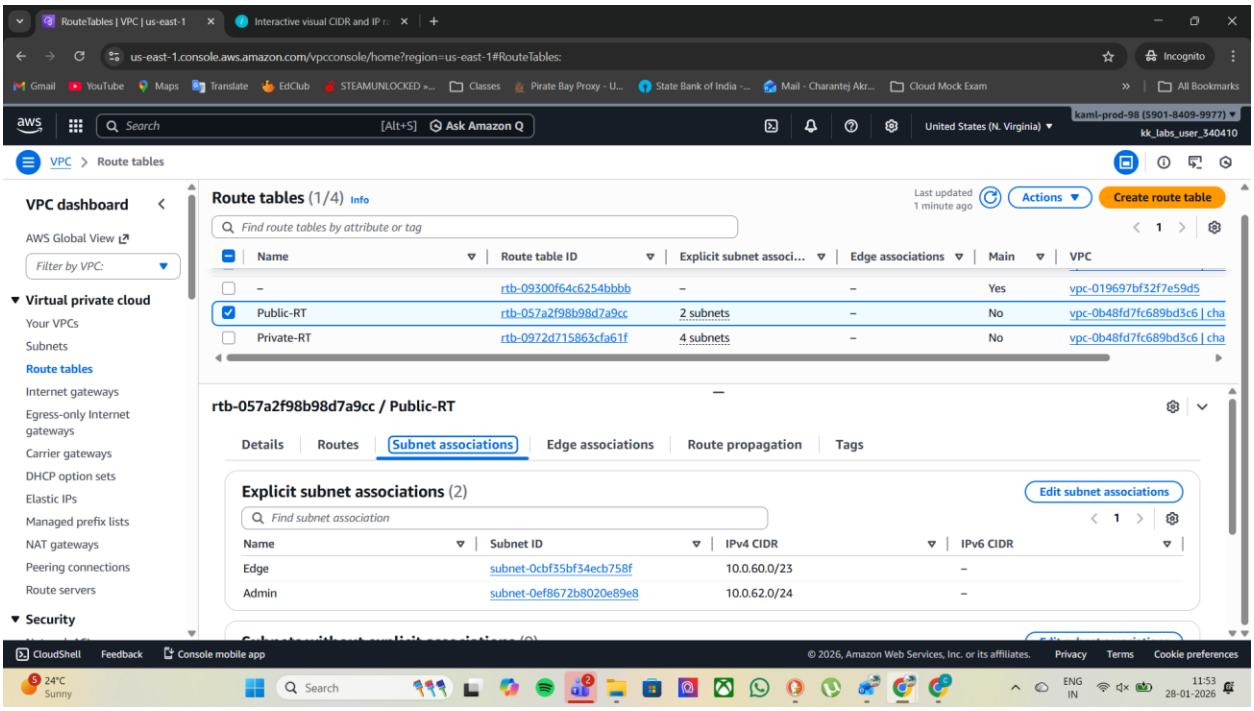

RouteTables | VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
Incognito
Gmail YouTube Maps Translate EdClub STEAMUNLOCKED »... Classes Pirate Bay Proxy - U... State Bank of India -... Mail - Charantej Akr... Cloud Mock Exam All Bookmarks
Search [Alt+S] Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Route tables (1/3) Info
Last updated less than a minute ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-023e3aae5b48a8245 – – Yes vpc-0b48fd7fc689bd3c6 | chara.
– rtb-09300f64c6254bbbb – – Yes vpc-019697bf32f7e59d5
Public-RT rtb-057a2f98b98d7a9cc 2 subnets – No vpc-0b48fd7fc689bd3c6 | chara.
rtb-057a2f98b98d7a9cc / Public-RT
Details Routes Subnet associations Edge associations Route propagation Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0 igw-0480f57aa00846066 Active No Create Route
10.0.0.0/16 local Active No Create Route Table
CloudShell Feedback Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
24°C Sunny
Search
ENG IN
11:48 28-01-2026

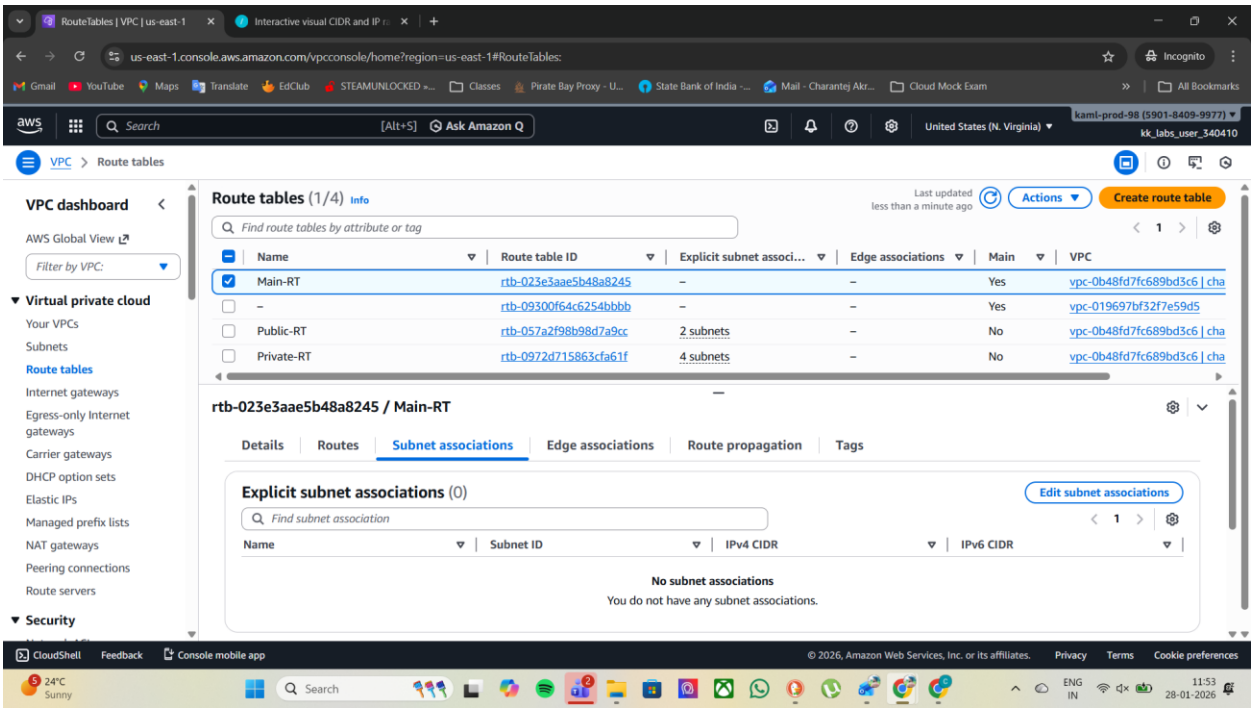

RouteTables | VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
Incognito
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Route tables (1/4) Info
Last updated 2 minutes ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
rtb-023e3aae5b48a8245
rtb-09300f64c6254bbbb
Public-RT
rtb-057a2f98b98d7a9cc
2 subnets
Private-RT
rtb-0972d715863cfa61f
rtb-0972d715863cfa61f / Private-RT
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnet associations
You do not have any subnet associations.
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
ENG
IN
11:51
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0972d715863cfa61f
Incognito
Search
[Alt+S]
Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables > rtb-0972d715863cfa61f > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (4/6)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
Shared
subnet-035cbae781ad99a04
10.0.0.0/19
Main (rtb-023e3aae5b48a8245)
Platform
subnet-04cfb6939d5037279
10.0.32.0/20
App
subnet-0adae62f54d5fbf00
10.0.48.0/21
Web
subnet-0d793da5df7eee300
10.0.56.0/22
Edge
subnet-0cbf35bf34ecb758f
10.0.60.0/23
rtb-057a2f98b98d7a9cc / Public-RT
Admin
subnet-0ef8672b8020e89e8
10.0.62.0/24
Selected subnets
subnet-04cfb6939d5037279 / Platform
subnet-035cbae781ad99a04 / Shared
subnet-0adae62f54d5fbf00 / App
subnet-0d793da5df7eee300 / Web
Cancel
Save associations
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Sunny
ENG
IN
11:51
28-01-2026


VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
Incognito
Gmail YouTube Maps Translate EdClub STEAMUNLOCKED »... Classes Pirate Bay Proxy - U... State Bank of India -... Mail - Charantej Akr... Cloud Mock Exam All Bookmarks
aws Search [Alt+S] Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
You have successfully updated subnet associations for rtb-0972d715863cfa61f / Private-RT.
Route tables (1/4) Info
Last updated less than a minute ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
Public-RT
rtb-057a2f98b98d7a9cc
2 subnets
–
No
vpc-0b48fd7fc689bd3c6 | cha
Private-RT
rtb-0972d715863cfa61f
4 subnets
–
No
vpc-0b48fd7fc689bd3c6 | cha
rtb-0972d715863cfa61f / Private-RT
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
Create Route Table
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C Sunny
Search
ENG IN
11:52 28-01-2026


RouteTables | VPC | us-east-1
Interactive visual CIDR and IP
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:
Incognito
Gmail YouTube Maps Translate EdClub STEAMUNLOCKED »... Classes Pirate Bay Proxy - U... State Bank of India -... Mail - Charantej Akr... Cloud Mock Exam All Bookmarks
aws Search [Alt+S] Ask Amazon Q
United States (N. Virginia)
kaml-prod-98 (5901-8409-9977)
kk_labs_user_340410
VPC > Route tables
VPC dashboard
AWS Global View
Filter by VPC:
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers
Security
Route tables (1/4) Info
Last updated 1 minute ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
–
rtb-09300f64c6254bbbb
–
–
Yes
vpc-019697bf32f7e59d5
Public-RT
rtb-057a2f98b98d7a9cc
2 subnets
–
No
vpc-0b48fd7fc689bd3c6 | cha
Private-RT
rtb-0972d715863cfa61f
4 subnets
–
No
vpc-0b48fd7fc689bd3c6 | cha
rtb-0972d715863cfa61f / Private-RT
Explicit subnet associations (4)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Shared
subnet-035cbae781ad99a04
10.0.0.0/19
–
Platform
subnet-04cfb6939d5037279
10.0.32.0/20
–
App
subnet-0adae62f54d5fbf00
10.0.48.0/21
–
Web
subnet-0d793da5df7eee300
10.0.56.0/22
–
CloudShell
Feedback
Console mobile app
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C Sunny
Search
ENG IN
11:52 28-01-2026





8. Security-Driven Network Behavior

Internet Access Rules

- Only **Admin & Edge** subnets have a default route to IGW

- Private subnets have **no path to the internet**

Internal Communication

- All subnets communicate via **implicit local VPC routing**
- No additional routes required

This design enforces **network-level security by default**.

9. Validation & Testing

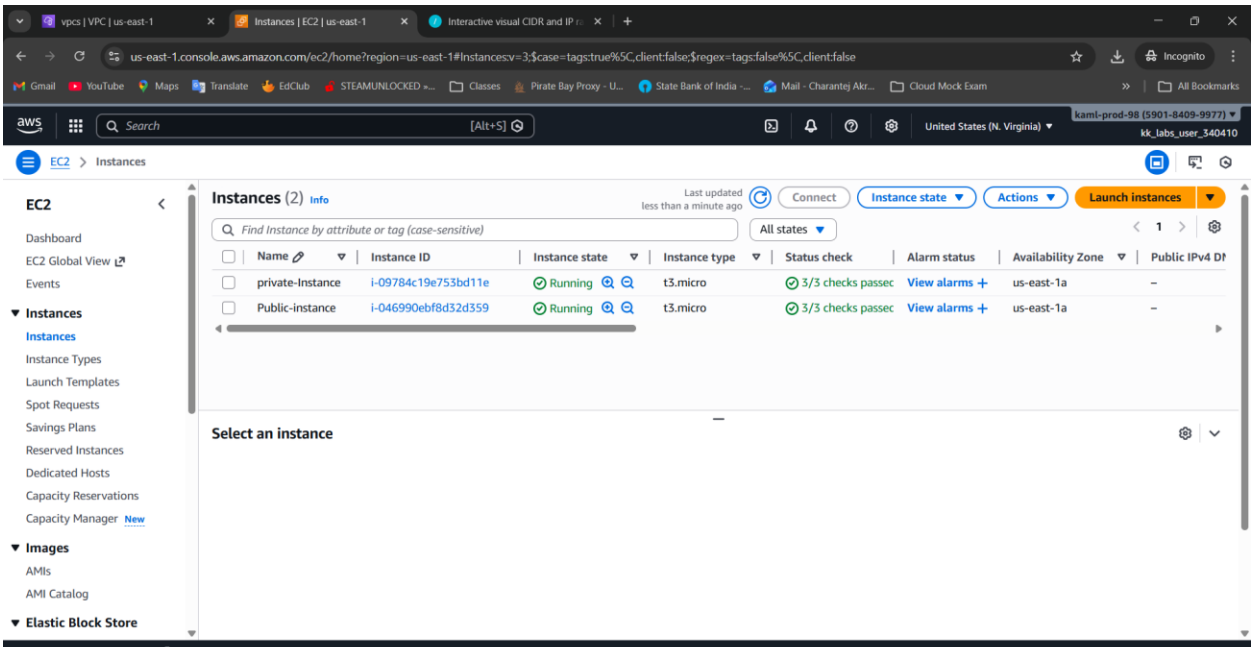
9.1 Public Subnet Test

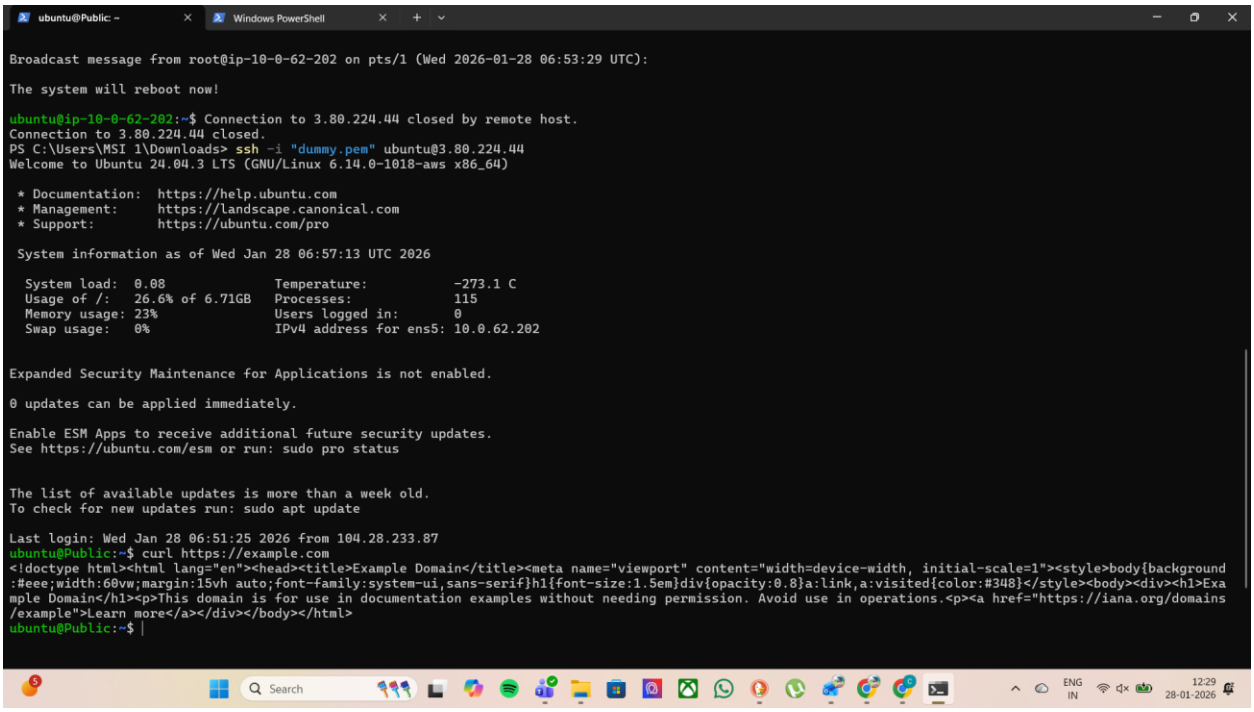
Expected Behavior:

- EC2 instance in Admin or Edge subnet
- Can reach the internet (ping, curl, yum update)

Reason:

- Route to IGW exists
- Public IP assigned





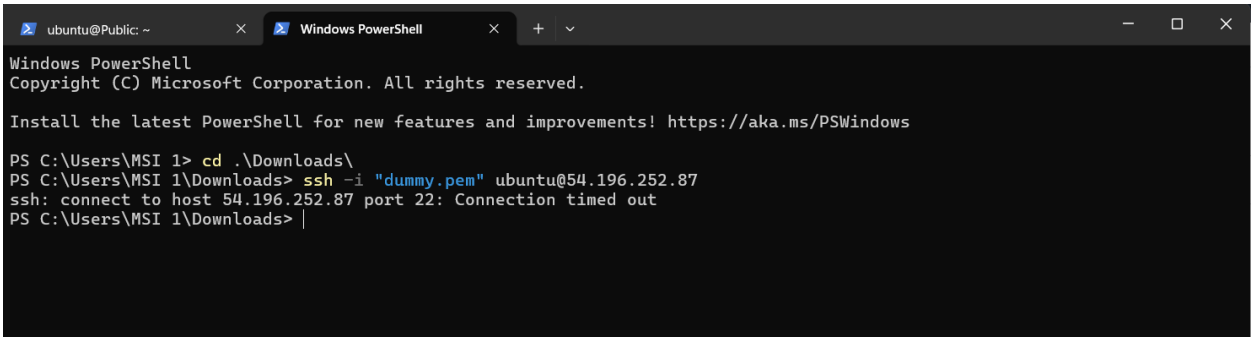
9.2 Private Subnet Test

Expected Behavior:

- EC2 instance in Web/App/Platform/Shared
- Cannot access the internet

Reason:

- No 0.0.0.0/0 route
- IGW not reachable



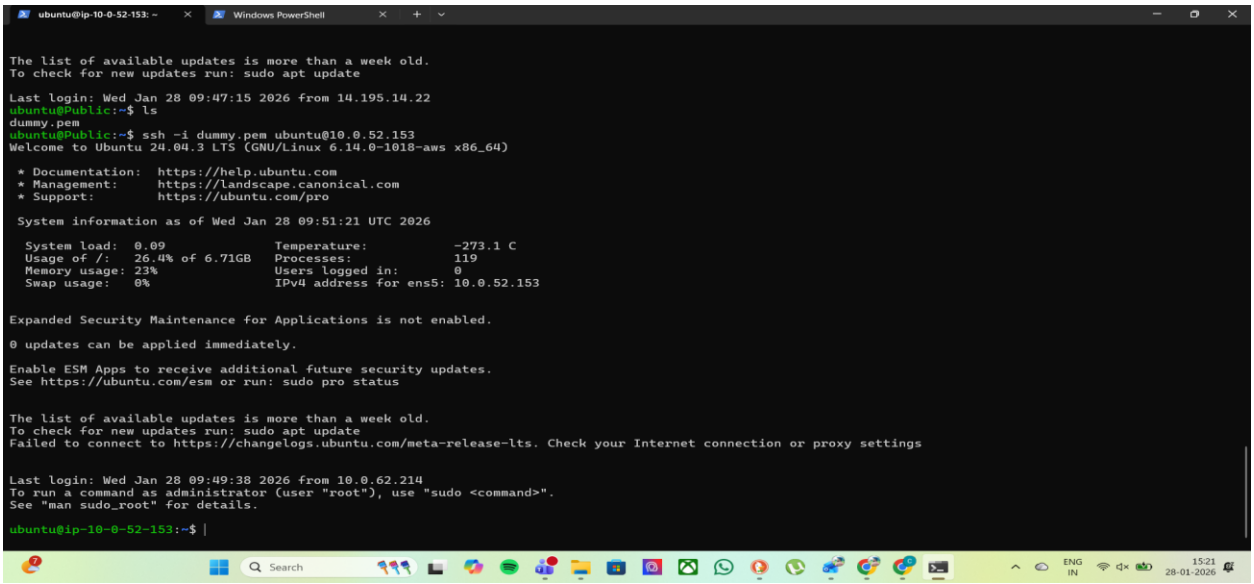
9.3 Internal Communication Test

Expected Behavior:

- Instances across subnets can communicate internally

Reason:

- Local VPC route automatically present



```
ubuntu@ip-10-0-52-153:~$ ls
ubuntu@ip-10-0-52-153:~$ sudo hostnamectl set-hostname Private
ubuntu@ip-10-0-52-153:~$ sudo init 6

Broadcast message from root@ip-10-0-52-153 on pts/1 (Wed 2026-01-28 09:51:54 UTC):

The system will reboot now!

ubuntu@ip-10-0-52-153:~$ Connection to 10.0.52.153 closed by remote host.
Connection to 10.0.52.153 closed.
```

10. Failure & Audit Scenarios

10.1 IGW Detached

- All internet access stops immediately
- No impact on internal communication

10.2 Private Subnet Associated with Public-RT

- Subnet becomes internet-reachable
- Violates security model
- Major audit finding

10.3 Incorrect /19 Starting Address

- CIDR misalignment
- Overlapping subnets
- AWS rejects configuration or routing breaks

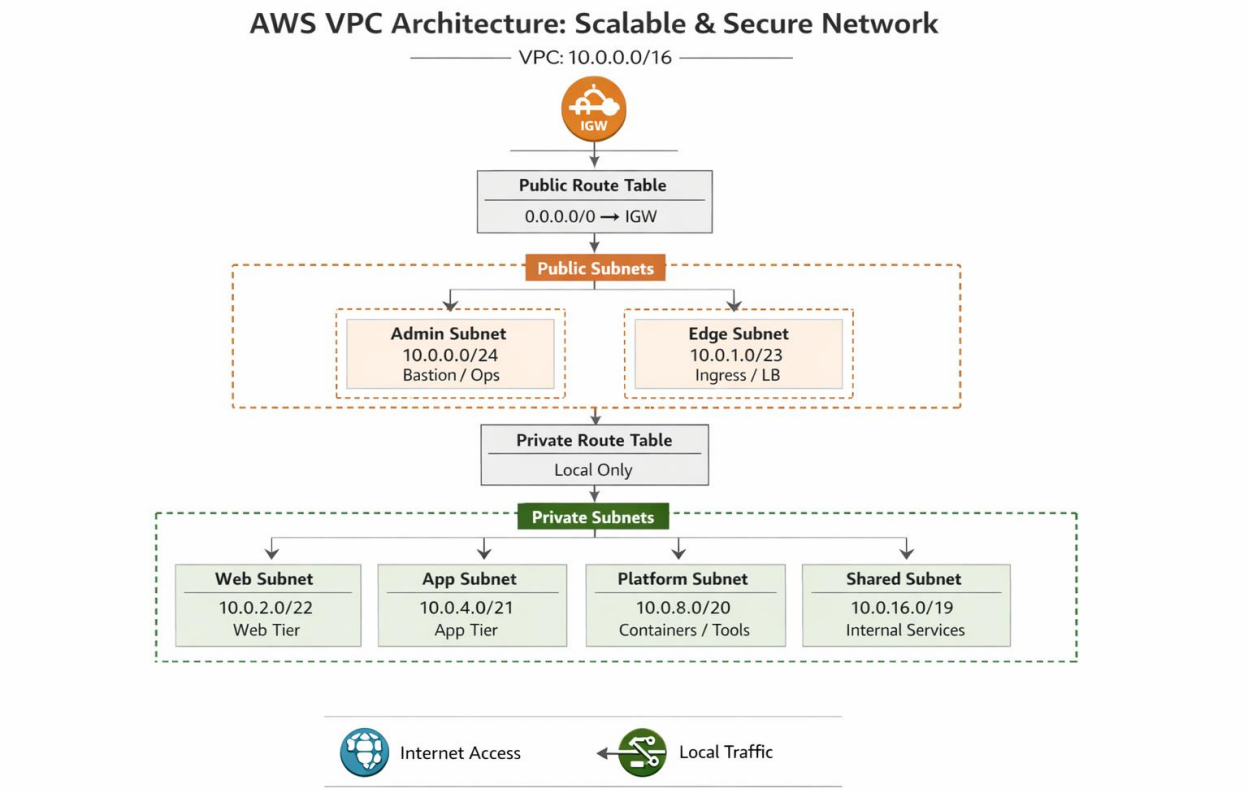
10.4 Future Growth Support

- Large unused CIDR space available
- New tiers can be added safely
- No subnet resizing required

11. Architecture Diagram

📐 Logical Network Diagram

- VPC boundary
- All 6 subnets
- Public vs Private route tables
- Internet Gateway



12. Conclusion

This VPC design:

- Meets enterprise scalability requirements
- Enforces security through routing
- Is simple to audit and reason about
- Supports long-term growth without redesign

✅ Production-ready ✅ Audit-friendly ✅ Scalable by design