

# 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.

The screenshot shows two stacked screenshots of the AWS VPC creation interface and the resulting VPC dashboard.

**Top Screenshot (Create VPC):**

- The URL is [us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpc:createMode=vpcOnly](https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpc:createMode=vpcOnly).
- The "VPC settings" section shows "Resources to create": **VPC only** (selected) and **VPC and more**.
- "Name tag - optional": charan-vpc
- "IPv4 CIDR block": 10.0.0.0/16 (selected)
- "IPv6 CIDR block": No IPv6 CIDR block selected.

**Bottom Screenshot (VPC Dashboard):**

- The URL is [us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#vpcs](https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#vpcs).
- A success message: "You successfully created vpc-0b48fd7fc689bd3c6 / charan-vpc".
- The "Your VPCs" table lists two VPCs:

Name	VPC ID	State	Encryption c...	Encryption control...	Block Public...	IPv4 CIDR
-	vpc-019697bf32f7e59d5	Available	-	-	Off	172.31.0.0/16
charan-vpc	vpc-0b48fd7fc689bd3c6	Available	-	-	Off	10.0.0.0/16

## 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 range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED Classes Pirate Bay Proxy - U... State Bank of India Mail - Charanjeet Akr... Cloud Mock Exam

aws Search [Alt+S] Ask Amazon Q United States (N. Virginia) kami-prod-98 (5901-8409-9977) kk\_labs\_user\_340410

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

**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.

**IPv4 subnet CIDR block**  
 8,192 IPs  
< > ^ v

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> <input type="text" value="Shared"/>	<input type="button" value="Remove"/>
<input type="text" value="Purpose"/> <input type="text" value="Large Internal Service"/>	<input type="button" value="Remove"/>

You can add 48 more tags.

CloudShell Feedback Console mobile app 24°C Sunny 11:36 28-01-2026 ENG IN © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED Classes Pirate Bay Proxy - U... State Bank of India Mail - Charanjeet Akr... Cloud Mock Exam

aws Search [Alt+S] Ask Amazon Q United States (N. Virginia) kami-prod-98 (5901-8409-9977) kk\_labs\_user\_340410

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

**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.

**IPv4 subnet CIDR block**  
 4,096 IPs  
< > ^ v

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> <input type="text" value="Platform"/>	<input type="button" value="Remove"/>
<input type="text" value="Purpose"/> <input type="text" value="Containers / Tools"/>	<input type="button" value="Remove"/>

You can add 48 more tags.

CloudShell Feedback Console mobile app 24°C Sunny 11:37 28-01-2026 ENG IN © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED Classes Pirate Bay Proxy - U... State Bank of India Mail - Charantej Akr... Cloud Mock Exam

aws Search [Alt+S] Ask Amazon Q

United States (N. Virginia) kami-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.  
 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.

**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.

**IPv4 subnet CIDR block**  
 2,048 IPs  
< > ^ v

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="App"/> <a href="#">Remove</a>
<input type="text" value="Purpose"/>	<input type="text" value="App Tier"/> <a href="#">Remove</a>

CloudShell Feedback Console mobile app News for you Vivo X200T deb... Search ENG IN 11:39 28-01-2026 © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED Classes Pirate Bay Proxy - U... State Bank of India Mail - Charantej Akr... Cloud Mock Exam

aws Search [Alt+S] Ask Amazon Q

United States (N. Virginia) kami-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.  
 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.

**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.

**IPv4 subnet CIDR block**  
 1,024 IPs  
< > ^ v

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="Web"/> <a href="#">Remove</a>
<input type="text" value="Purpose"/>	<input type="text" value="Web Tier"/> <a href="#">Remove</a>

CloudShell Feedback Console mobile app News for you Vivo X200T deb... Search ENG IN 11:40 28-01-2026 © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED... Classes Pirate Bay Proxy - U... State Bank of India ... Mail - Charanjeet Akr... Cloud Mock Exam

aws 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.  
  
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.

**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.

**IPv4 subnet CIDR block**  
 512 IPs

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> Name	<input type="text" value="Edge"/> Edge
<input type="text" value="Purpose"/> Purpose	<input type="text" value="Ingress / LB"/> Ingress / LB

CloudShell Feedback Console mobile app Trending videos All eyes on 'Ave... © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 11:41 28-01-2026

VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets:sort=tag:Name

Gmail YouTube Maps Translate EdClub STEAMUNLOCKED... Classes Pirate Bay Proxy - U... State Bank of India ... Mail - Charanjeet Akr... Cloud Mock Exam

aws Search [Alt+S] Ask Amazon Q

United States (N. Virginia) **kaml-prod-98 (5901-8409-9977)** kk\_labs\_user\_340410

**VPC dashboard** < **Subnets**

**Subnets (12) Info**

Last updated less than a minute ago

Name	Subnet ID	State	VPC	Block Public...	IPv4
-	subnet-0c6ac3e40d994987f	Available	vpc-019697bf32f7e59d5	Off	172.0.0.0/16
Admin	subnet-0ef8672b8020e89e8	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16
App	subnet-0adae62f54d5fbf00	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16
Edge	subnet-0cbf35bf34ecb758f	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16
Platform	subnet-04cfb6939d5037279	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16
Shared	subnet-035chae781a99a04	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16
Web	subnet-0d793da5df7eee300	Available	vpc-0b48fd7fc689bd3c6   charan-vpc	Off	10.0.0.0/16

Select a subnet

CloudShell Feedback Console mobile app © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 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

The screenshot shows the 'Create internet gateway' wizard in the AWS VPC console. The first step, 'Internet gateway settings', is displayed. It includes a 'Name tag' section where 'charan-IGW' is entered into a text input field. Below it is a 'Tags - optional' section with a single tag 'Name: charan-IGW'. At the bottom right are 'Cancel' and 'Create internet gateway' buttons.

The screenshot shows the 'Internet gateways' list in the AWS VPC console. The table displays two entries:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0530e446f96e33bcc	Attached	vpc-019697bf32f7e59d5	590184099977
charan-IGW	igw-0480f57aa00846066	Detached	-	590184099977

A message at the bottom says 'Select an internet gateway above'.

The screenshot shows the AWS VPC console interface. The user is performing a search for a VPC to attach an Internet Gateway to. The search bar contains the identifier "vpc-0b48fd7fc689bd3c6". Below the search bar, there is a section titled "AWS Command Line Interface command" which includes a "Cancel" button and an "Attach internet gateway" button.

The screenshot shows the AWS VPC console interface. The user is editing the routes for a specific route table. In the "Edit routes" section, there is a table with the following data:

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway	-	No	CreateRoute
0.0.0.0/0	igw-0480f57aa00846066	-	-	-

At the bottom of the "Edit routes" section, there are "Add route", "Cancel", "Preview", and "Save changes" buttons.



## 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 → local 0.0.0.0/0 → IGW
Private-RT	Web, App, Platform, Shared	10.0.0.0/16 → local

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

The screenshot shows the AWS VPC Route Tables console. On the left, there's a navigation sidebar with options like 'VPC dashboard', 'Virtual private cloud', 'Route tables', and 'Security'. The main area displays a table titled 'Route tables (1/4) Info' with one item: 'rtb-0972d715863cfa61f / Private-RT'. Below this, there are tabs for 'Details', 'Routes', 'Subnet associations' (which is selected), 'Edge associations', 'Route propagation', and 'Tags'. Under 'Subnet associations', it says 'Explicit subnet associations (0)' and 'No subnet associations'. You do not have any subnet associations.' At the bottom, there are standard browser controls and a status bar indicating '24°C Sunny'.

This screenshot is identical to the one above, showing the AWS VPC Route Tables console. It displays the same route table list and the detailed view for the 'Private-RT' route table. The 'Subnet associations' tab is selected, showing 'Explicit subnet associations (0)' and 'No subnet associations'. The browser status bar at the bottom indicates '24°C Sunny'.

## 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**

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 (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), and Security. The main content area displays a table titled "Route tables (1/3) info". The table has columns for Name, Route table ID, Explicit subnet associ..., Edge associations, Main, and VPC. It lists three route tables: "rtb-023e3aae5b48a8245" (Main, VPC "vpc-0b48fd7fc689bd3c6 | chara."), "rtb-09300f64c6254bbb" (Yes, VPC "vpc-019697bf32f7e59d5"), and "Public-RT" (No, VPC "vpc-0b48fd7fc689bd3c6 | chara."). Below this, a specific route table "rtb-057a2f98b98d7a9cc / Public-RT" is selected. The "Subnet associations" tab is active, showing a table with columns for Name, Subnet ID, IPv4 CIDR, and IPv6 CIDR. A message indicates "No subnet associations" and "You do not have any subnet associations.".

The screenshot then transitions to the "Edit subnet associations" page for the selected route table. At the top, it says "Edit subnet associations" and "Change which subnets are associated with this route table." Below this is a table titled "Available subnets (2/6)" with columns for Name, Subnet ID, IPv4 CIDR, IPv6 CIDR, and Route table ID. It lists several subnets: "Shared" (subnet-035cbae781ad99a04, 10.0.0.0/19, Main (rtb-023e3aae5b48a8245)), "Platform" (subnet-04cfb6939d5037279, 10.0.32.0/20, Main (rtb-023e3aae5b48a8245)), "App" (subnet-0adae62f54d5fb00, 10.0.48.0/21, Main (rtb-023e3aae5b48a8245)), "Web" (subnet-0d793da5df7eee300, 10.0.56.0/22, Main (rtb-023e3aae5b48a8245)), "Edge" (subnet-0cbf35bf34ecb758f, 10.0.60.0/23, Main (rtb-023e3aae5b48a8245)), and "Admin" (subnet-0ef8672b8020e89e8, 10.0.62.0/24, Main (rtb-023e3aae5b48a8245)).

At the bottom of this page, under "Selected subnets", two subnets are listed: "subnet-0cbf35bf34ecb758f / Edge" and "subnet-0ef8672b8020e89e8 / Admin". There are "Cancel" and "Save associations" buttons at the bottom right.

This screenshot shows the same "Route tables (1/3) info" page as the first one, but with the "Public-RT" route table selected. The "Subnet associations" tab is active, showing the "Explicit subnet associations (0)" table. A message says "No subnet associations" and "You do not have any subnet associations.".

This screenshot shows the "Edit subnet associations" page again, but this time the "Edge" subnet is selected in the "Available subnets" table. The "Selected subnets" section now contains "subnet-0cbf35bf34ecb758f / Edge". The "Save associations" button is visible at the bottom right.

Screenshot of the AWS VPC Route Tables console page.

**Route tables (1/3) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-023e3aae5b48a8245	-	-	Yes	vpc-0b48fd7fc689bd3c6   chara.
-	rtb-09300f64c6254bb5	-	-	Yes	vpc-019697bf32f7e59d5
<b>Public-RT</b>	<b>rtb-057a2f98b98d7a9cc</b>	<b>2 subnets</b>	-	No	vpc-0b48fd7fc689bd3c6   chara.

**rtb-057a2f98b98d7a9cc / Public-RT**

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

**Routes (1)**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

**Route tables (1/3) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-023e3aae5b48a8245	-	-	Yes	vpc-0b48fd7fc689bd3c6   chara.
-	rtb-09300f64c6254bb5	-	-	Yes	vpc-019697bf32f7e59d5
<b>Public-RT</b>	<b>rtb-057a2f98b98d7a9cc</b>	<b>2 subnets</b>	-	No	vpc-0b48fd7fc689bd3c6   chara.

**rtb-057a2f98b98d7a9cc / Public-RT**

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

**Routes (2)**

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

Screenshot of the AWS VPC Route Tables console page:

**Route tables (1/4) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-023e3aae5b48a8245	-	-	Yes	vpc-0b48fd7fc689bd3c6   cha
-	rtb-09300f64c6254bb	-	-	Yes	vpc-019697bf32f7e59d5
Public-RT	rtb-057a2f98b98d7a9cc	2 subnets	-	No	vpc-0b48fd7fc689bd3c6   cha
<b>Private-RT</b>	<b>rtb-0972d715863cfa61f</b>	-	-	No	<b>vpc-0b48fd7fc689bd3c6   cha</b>

**rtb-0972d715863cfa61f / Private-RT**

**Subnet associations**

No subnet associations

**Edit subnet associations**

**Available subnets (4/6)**

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	-	Main (rtb-023e3aae5b48a8245)
App	subnet-0adae62f54d5fb00	10.0.48.0/21	-	Main (rtb-023e3aae5b48a8245)
Web	subnet-0d793da5df7eee500	10.0.56.0/22	-	Main (rtb-023e3aae5b48a8245)
Edge	subnet-0cfb35bf34ecb758f	10.0.60.0/23	-	rtb-057a2f98b98d7a9cc / Public-RT
Admin	subnet-0ef8672b8020e89e8	10.0.62.0/24	-	rtb-057a2f98b98d7a9cc / Public-RT

**Selected subnets**

- subnet-04cfb6939d5037279 / Platform
- subnet-035cbae781ad99a04 / Shared
- subnet-0adae62f54d5fb00 / App
- subnet-0d793da5df7eee500 / Web

**Save associations**

**VPC | us-east-1**    **Interactive visual CIDR and IP range calculator**

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables

AWS Search [Alt+S] Ask Amazon Q

United States (N. Virginia)    kami-prod-98 (5901-8409-9977)    kk\_labs\_user\_340410

**VPC** > Route tables

You have successfully updated subnet associations for rtb-0972d715863cfa61f / Private-RT.

Last updated less than a minute ago

**Route tables (1/4) Info**

Name	Route table ID	Explicit subnet associations	Main	VPC
Public-RT	rtb-057a2f98b98d7a9cc	2 subnets	-	vpc-0b48fd7fc689bd3c6   cha
<b>Private-RT</b>	<b>rtb-0972d715863cfa61f</b>	<b>4 subnets</b>	-	<b>vpc-0b48fd7fc689bd3c6   cha</b>

**rtb-0972d715863cfa61f / Private-RT**

Details    **Routes**    Subnet associations    Edge associations    Route propagation    Tags

**Routes (1)**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Console mobile app

24°C Sunny

RouteTables | VPC | us-east-1    Interactive visual CIDR and IP range calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables

AWS Search [Alt+S] Ask Amazon Q

United States (N. Virginia)    kami-prod-98 (5901-8409-9977)    kk\_labs\_user\_340410

**VPC** > Route tables

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associations	Main	VPC
-	rtb-09300f64c6254bbb	-	-	vpc-019697bf32f7e59d5
Public-RT	rtb-057a2f98b98d7a9cc	2 subnets	-	vpc-0b48fd7fc689bd3c6   cha
<b>Private-RT</b>	<b>rtb-0972d715863cfa61f</b>	<b>4 subnets</b>	-	<b>vpc-0b48fd7fc689bd3c6   cha</b>

**rtb-0972d715863cfa61f / Private-RT**

Explicit subnet associations (4)

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-0adae62f54d5fb00	10.0.48.0/21	-
Web	subnet-0d793da5df7eee300	10.0.56.0/22	-

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Console mobile app

24°C Sunny

**Route tables (1/4) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-09300f64c6254bbb	-	-	Yes	vpc-019697bf32f7e59d5
<b>Public-RT</b>	<b>rtb-057a2f98b98d7a9cc</b>	<b>2 subnets</b>	-	No	vpc-0b48fd7fc689bd3c6   cha
Private-RT	rtb-0972d715863cfa61f	4 subnets	-	No	vpc-0b48fd7fc689bd3c6   cha

**rtb-057a2f98b98d7a9cc / Public-RT**

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

**Explicit subnet associations (2)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Edge	subnet-0cbf35bf34eb758f	10.0.60.0/23	-
Admin	subnet-0ef8672b8020e89e8	10.0.62.0/24	-

**Route tables (1/4) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<b>Main-RT</b>	<b>rtb-023e3aae5b48a8245</b>	-	-	Yes	vpc-0b48fd7fc689bd3c6   cha
-	rtb-09300f64c6254bbb	-	-	Yes	vpc-019697bf32f7e59d5
Public-RT	rtb-057a2f98b98d7a9cc	2 subnets	-	No	vpc-0b48fd7fc689bd3c6   cha
Private-RT	rtb-0972d715863cfa61f	4 subnets	-	No	vpc-0b48fd7fc689bd3c6   cha

**rtb-023e3aae5b48a8245 / Main-RT**

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

**Explicit subnet associations (0)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
------	-----------	-----------	-----------

No subnet associations  
You do not have any subnet associations.

## 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

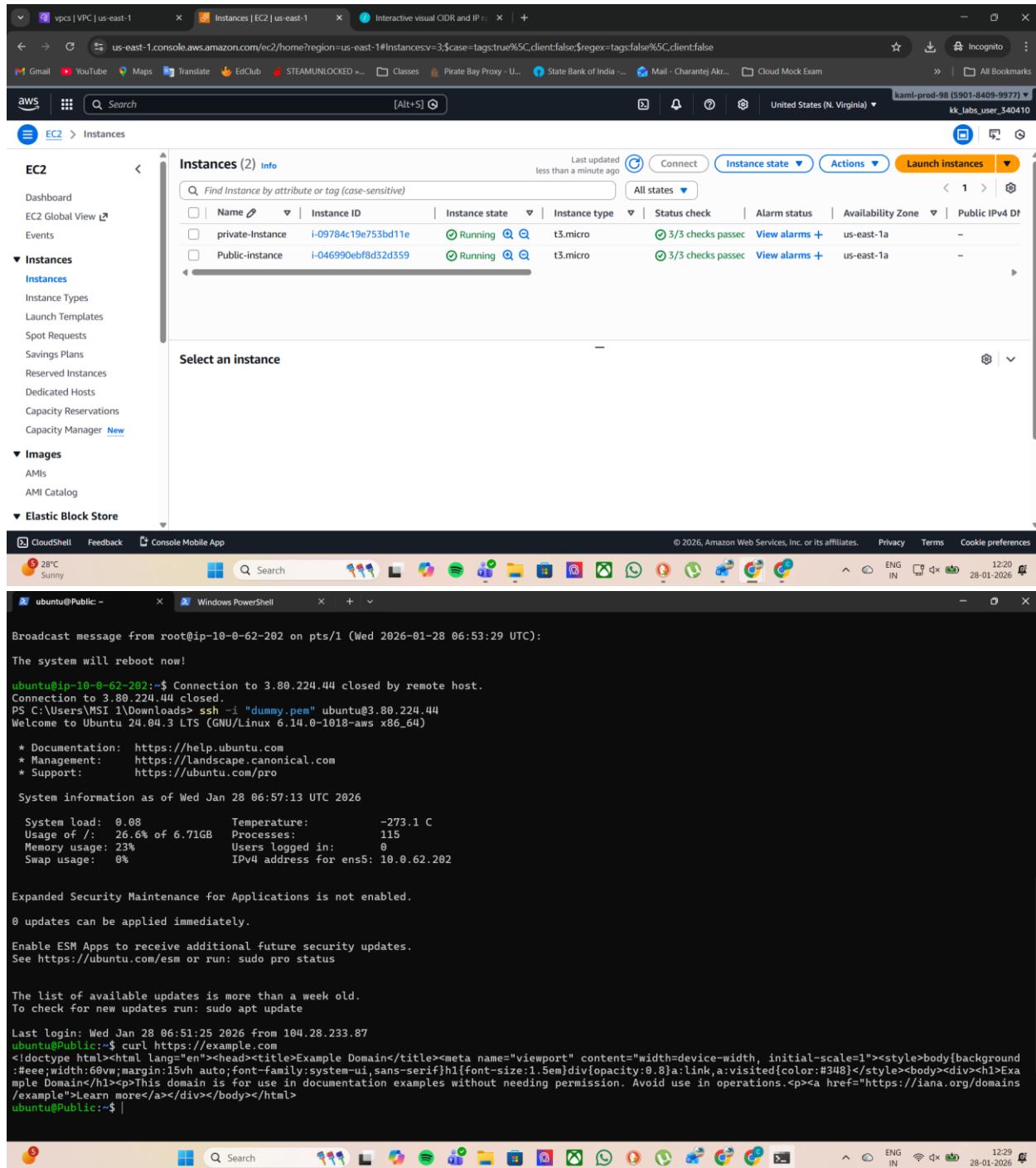
### 9.1 Public Subnet Test

#### 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



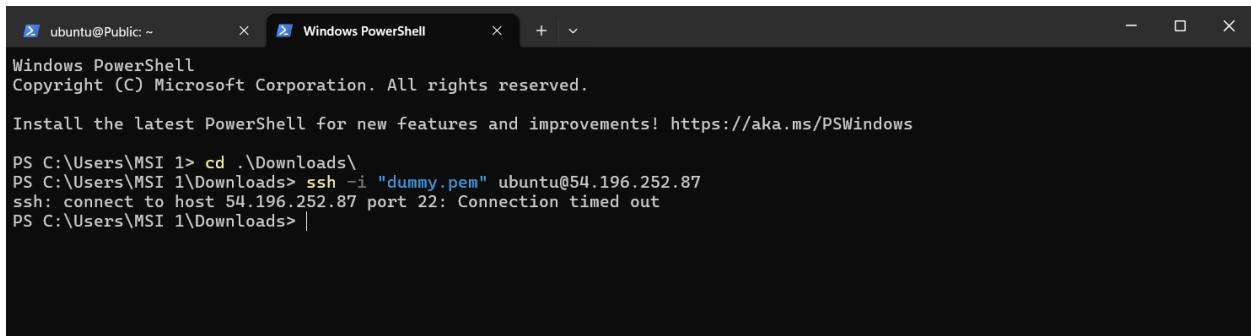
## 9.2 Private Subnet Test

## Expected Behavior:

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

## Reason:

- No 0.0.0.0/0 route
- IGW not reachable



```
ubuntu@Public: ~          Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\MSI 1> cd .\Downloads\
PS C:\Users\MSI 1\Downloads> ssh -i "dummy.pem" ubuntu@54.196.252.87
ssh: connect to host 54.196.252.87 port 22: Connection timed out
PS C:\Users\MSI 1\Downloads> |
```

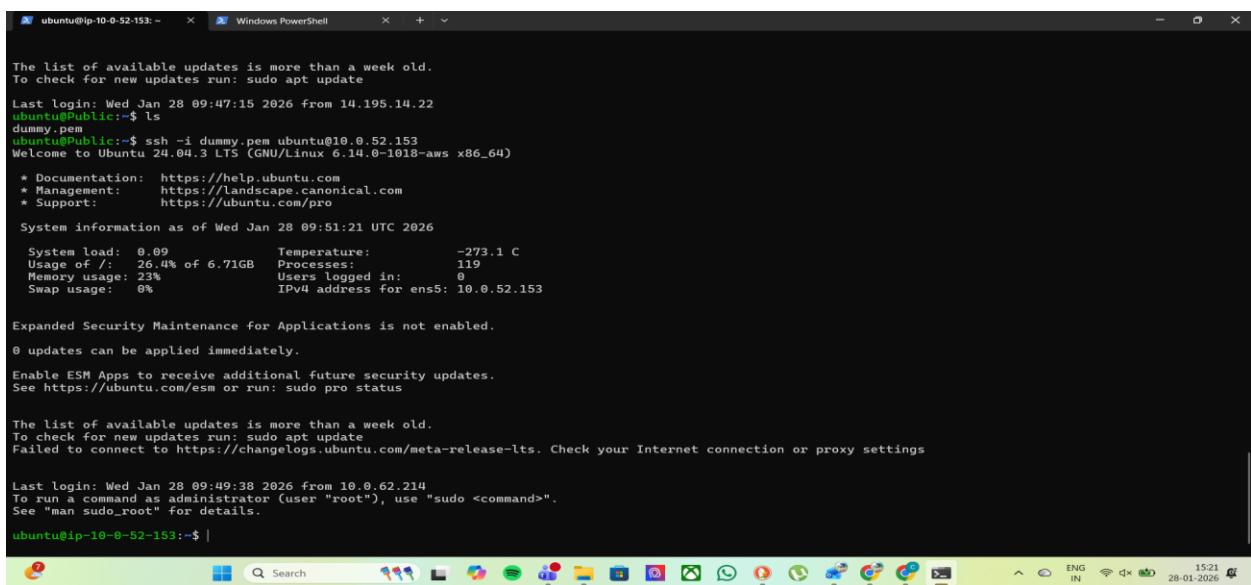
## 9.3 Internal Communication Test

### Expected Behavior:

- Instances across subnets can communicate internally

## Reason:

- Local VPC route automatically present



```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jan 28 09:47:15 2026 from 14.195.14.22
ubuntu@Public:~$ ls
dummy.pem
ubuntu@Public:~$ ssh -i dummy.pem ubuntu@10.0.52.153
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jan 28 09:51:21 UTC 2026

System load: 0.09      Temperature:      -273.1 C
Usage of /: 26.4% of 6.71GB  Processes:        119
Memory usage: 23%          Users logged in:   0
Swap usage:  0%           IPv4 address for ens5: 10.0.52.153

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Jan 28 09:49:38 2026 from 10.0.62.214
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-52-153:~$ |
```

```
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.
```

```
ubuntu@Private:~$ ls
ubuntu@Private:~$ |
```

## 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

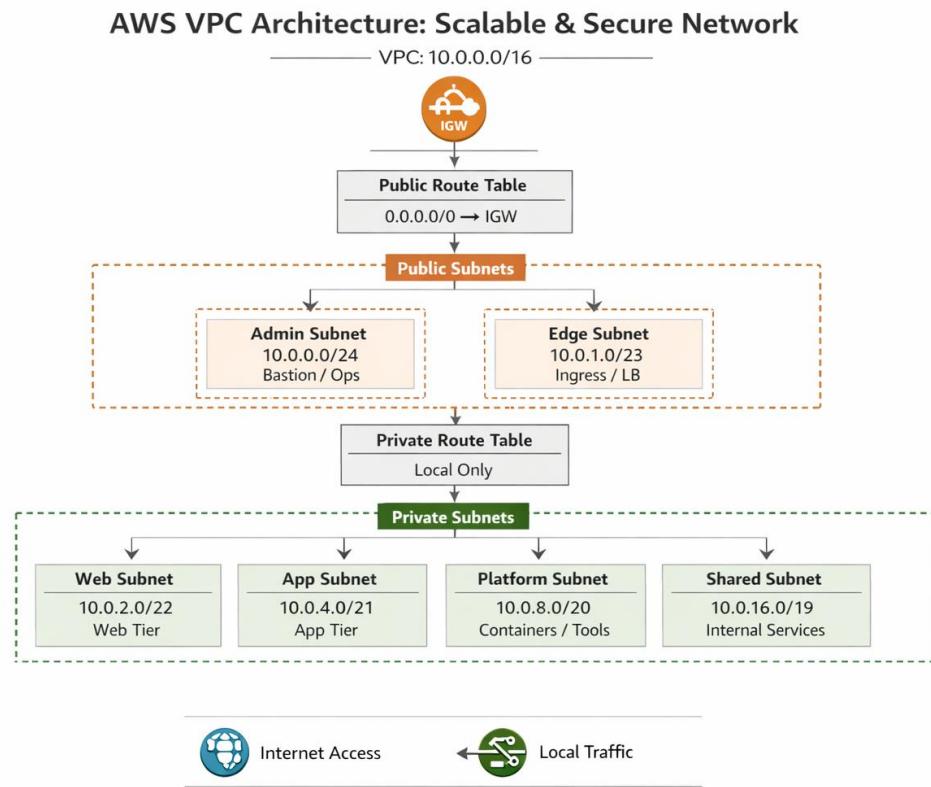
### 10.4 Future Growth Support

- 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