

AWS VPC with Variable-Size Subnets Setup (Without NAT Gateway)

1. VPC Creation: "asymmetric-vpc"

Objective

Create a new Virtual Private Cloud (VPC) with a /16 CIDR block, enabling DNS resolution and DNS hostnames for a production environment.

VPC Configuration

- **VPC Name:** asymmetric-vpc
- **CIDR Block:** 10.0.0.0/16
- **DNS Resolution:** Enabled
- **DNS Hostnames:** Enabled
- **Tags:**
 - Environment = "production"
 - Owner = "network-team"
 - Project = "asymmetric-vpc-build"
 - CostCenter = "AWS-Networking"

Steps Taken

1. **Navigate to:** VPC Dashboard → Create VPC.
2. **Input VPC CIDR Block:** 10.0.0.0/16.
3. **Enable DNS Settings:** DNS resolution and DNS hostnames were enabled.

4. Tag the VPC: Tags were added as per the requirement.

The screenshot shows the 'Create VPC' settings page in the AWS VPC console. The 'VPC only' option is selected under 'Resources to create'. A name tag 'asymmetric-vpc' is specified. The IPv4 CIDR block is set to '10.0.0.0/16'. The IPv6 CIDR block section indicates 'No IPv6 CIDR block'.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only **VPC and more**

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
asymmetric-vpc

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the 'Your VPCs' page in the AWS VPC console. It displays two VPCs: 'vpc-04cf58a007b96cc98' and 'vpc-01041cfa5e84bb502', both marked as 'Available'. A sidebar on the left provides navigation for the VPC dashboard and virtual private cloud components.

Your VPCs

VPCs | [VPC encryption controls - new](#)

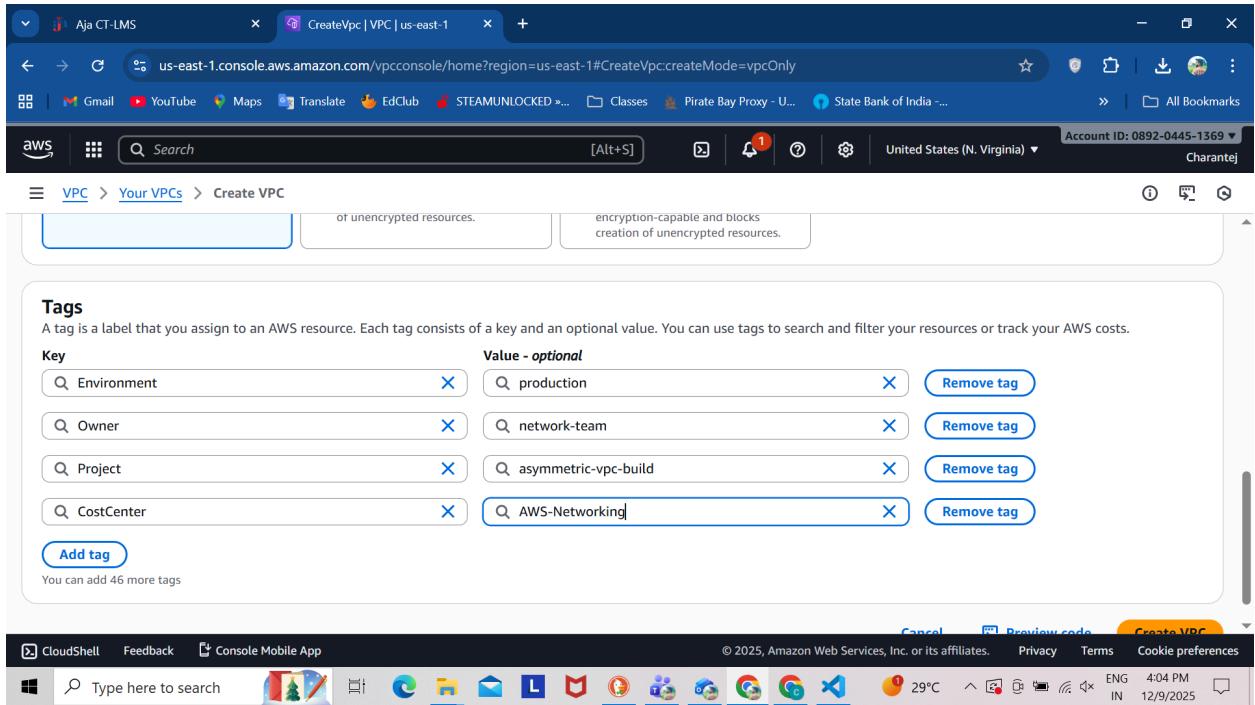
Your VPCs (2) [Info](#)

Last updated less than a minute ago

<input type="checkbox"/>	Name	VPC ID	State	Encryption c...	Encryption contrc
<input type="checkbox"/>	-	vpc-04cf58a007b96cc98	Available	-	-
<input type="checkbox"/>	asymmetric-vpc	vpc-01041cfa5e84bb502	Available	-	-

Select a VPC above

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



2. Subnet Creation: Variable IP Sizes

Objective

Create six subnets in multiple Availability Zones (AZs) with varying IP capacities to represent different production workloads. Three public subnets and three private subnets are created.

Public Subnets

1. Public Subnet A:

- **CIDR:** 10.0.0.0/24 (~256 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Enabled
- **Tags:**
 - Tier = "public"

The screenshot shows the 'Create subnet' step in the AWS VPC console. The subnet is named 'Public Subnet A'. It is assigned to the 'United States (N. Virginia) / use1-az2 (us-east-1a)' availability zone. The IPv4 CIDR block is set to '10.0.0.0/16'. The IPv4 subnet CIDR block is specified as '10.0.0.0/24', which provides 256 IP addresses. There are no tags added to this subnet.

2. Public Subnet B:

- **CIDR:** 10.0.16.0/20 (~4,096 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Enabled
- **Tags:**

■ Tier = "public"

The screenshot shows the 'Create subnet' step in the AWS VPC console. The subnet is named 'Public Subnet B'. It is assigned to the 'United States (N. Virginia) / use1-az4 (us-east-1b)' availability zone. The IPv4 CIDR block is set to '10.0.16.0/20', which provides 4,096 IP addresses. There is one tag named 'Name' associated with this subnet.

3. Public Subnet C:

- **CIDR:** **10.0.32.0/19** (~8,192 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Enabled
- **Tags:**
 - Tier = "public"

The screenshot shows the AWS VPC console interface for creating a new subnet. The page title is 'Create subnet' under 'Subnets'. The subnet is named 'Public Subnet C'. The CIDR block is set to '10.0.32.0/19', which is highlighted with a blue border. The availability zone is 'United States (N. Virginia) / us-east-1a2 (us-east-1c)'. The IPv4 subnet CIDR block dropdown also shows '10.0.32.0/19'. The page includes standard AWS navigation and status bars at the top and bottom.

Private Subnets

1. Private Subnet A:

- **CIDR:** **10.0.4.0/22** (~1,024 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Disabled
- **Tags:**
 - Tier = "private"

The screenshot shows a browser window with multiple tabs open, including 'Aja CT-LMS', 'VPC | us-east-1', 'Interactive visual CIDR calculator', 'Create VPC Subnets - Go', and 'Subnet Allocation Overlay'. The main content area is titled 'Subnet 1 of 1' under 'VPC > Subnets > Create subnet'. It contains fields for 'Subnet name' (Private Subnet A), 'Availability Zone' (United States (N. Virginia) / use1-az1 (us-east-1d)), 'IPv4 VPC CIDR block' (10.0.0.0/16), and 'IPv4 subnet CIDR block' (10.0.4.0/22). The interface includes a sidebar with 'Next Step' and 'Cancel' buttons, and a bottom navigation bar with links like CloudShell, Feedback, Console Mobile App, and various icons.

2. Private Subnet B:

- **CIDR:** 10.0.2.0/23 (~512 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Disabled
- **Tags:**
 - Tier = "private"

The screenshot shows a browser window with multiple tabs open, including 'VPC | us-east-1' which is the active tab. The main content area displays the 'Create subnet' configuration page. The steps are as follows:

- Subnet name:** A text input field containing 'Private Subnet B'. A note below says 'The name can be up to 256 characters long.'
- Availability Zone:** A dropdown menu set to 'United States (N. Virginia) / use1-az3 (us-east-1e)'.
- IPv4 VPC CIDR block:** A dropdown menu set to '10.0.0.0/16'.
- IPv4 subnet CIDR block:** A dropdown menu set to '10.0.2.0/23'.
- Tags - optional:** A section where users can add tags. One tag is visible: 'Tier = "private"'.

The AWS navigation bar at the top includes links for CloudShell, Feedback, Console Mobile App, and various AWS services like Lambda, S3, and CloudWatch. The bottom status bar shows the date and time as '12/9/2025 4:45 PM'.

3. Private Subnet C:

- **CIDR:** 10.0.128.0/19 (~8,192 IPs)
- **AZ:** [Insert AZ Name]
- **Public IP Assignment:** Disabled
- **Tags:**
 - Tier = "private"

The screenshot shows the AWS VPC Subnet creation interface. The 'Subnet name' field contains 'Private Subnet C'. The 'Availability Zone' dropdown shows 'United States (N. Virginia) / us-east-1f'. The 'IPv4 CIDR block' dropdown shows '10.0.0.0/16'. The 'IPv4 subnet CIDR block' input field contains '10.0.128.0/19', which is highlighted with a blue border and shows '8,192 IPs' below it. The 'Tags - optional' section is collapsed. The bottom navigation bar includes CloudShell, Feedback, Console Mobile App, a search bar, and various AWS service icons.

Steps Taken

1. **Navigate to:** VPC Dashboard → Subnets → Create Subnet.
2. **Input Subnet Details:** Choose the VPC, AZ, CIDR block, and enable/disable public IP assignment.
3. **Add Tags:** Each subnet is tagged with "Tier" (either "public" or "private").

You have successfully created 3 subnets: subnet-0ba404c4b8a42e264, subnet-010c8f8c50f63cbf7, subnet-04b63502c7f3f126c

Subnets (9) Info

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
Public Subnet C	subnet-04b63502c7f3f126c	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.32.0/1
Public Subnet B	subnet-010c8f8c50f63cbf7	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.16.0/2
Public Subnet A	subnet-0ba404c4b8a42e264	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.0.0/24

Select a subnet

You have successfully created 3 subnets: subnet-083045bc5258e20f6, subnet-02de7ef7692a15d30, subnet-01e3a5cf1ce8fcf

Subnets (12) Info

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
Private Subnet B	subnet-02de7ef7692a15d30	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.2.0/23
Private Subnet A	subnet-083045bc5258e20f6	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.4.0/22
Private Subnet C	subnet-01e3a5cf1ce8fcf	Available	vpc-04c174d4b9de719d0 asym...	Off	10.0.128.0/

Select a subnet

3. Internet Gateway Creation: "asym-igw"

Objective

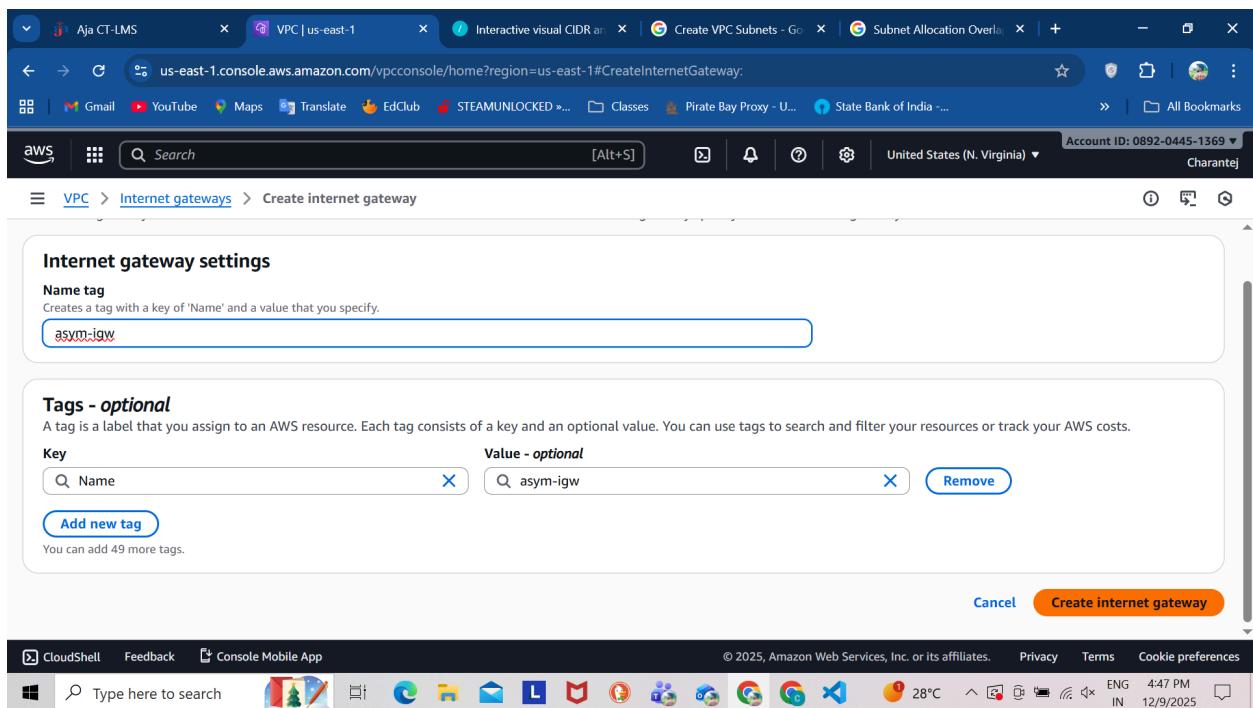
Create an Internet Gateway and attach it to the VPC, allowing public subnets to communicate with the internet.

Internet Gateway Configuration

- **IGW Name:** asym-igw
- **Attachment:** Attached to the asymmetric-vpc VPC.

Steps Taken

1. **Navigate to:** VPC Dashboard → Internet Gateways → Create Internet Gateway.
2. **Name the IGW:** Set the name to "asym-igw".
3. **Attach IGW:** Attach the IGW to the asymmetric-vpc.



The screenshot shows the AWS VPC console with the URL us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#igws. The page displays a list of two internet gateways:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-018a03d1e2db5204e	Attached	vpc-04cf58a007b96cc98	089204451369
asym-igw	igw-098248cba44356539	Detached	-	089204451369

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

The screenshot shows the Windows taskbar with several pinned icons, including CloudShell, Feedback, Console Mobile App, Gmail, YouTube, Maps, Translate, EdClub, STEAMUNLOCKED, Classes, Pirate Bay Proxy, State Bank of India, and All Bookmarks.

The screenshot shows the AWS VPC console with the URL us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#igws. The "asym-igw" internet gateway is selected. A context menu is open over the "Actions" button, with "Attach to VPC" highlighted.

The screenshot shows the Windows taskbar with several pinned icons, including CloudShell, Feedback, Console Mobile App, Gmail, YouTube, Maps, Translate, EdClub, STEAMUNLOCKED, Classes, Pirate Bay Proxy, State Bank of India, and All Bookmarks.

The screenshot shows the AWS VPC console with the URL us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#AttachInternetGateway:internetGatewayId=igw-098248cba44356539. The page title is "Attach to VPC (igw-098248cba44356539)". The main content area is titled "VPC" and contains instructions to attach an internet gateway to a VPC. A search bar shows the query "vpc-04c174d4b9de719d0". Below the search bar is a section titled "AWS Command Line Interface command". At the bottom right are "Cancel" and "Attach internet gateway" buttons.

The screenshot shows the AWS VPC console with the URL us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#igws. The page title is "Internet gateways (1/2)". The main content area displays a table of internet gateways:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-018a03d1e2db5204e	Attached	vpc-04cf58a007b96cc98	089204451369
asym-igw	igw-098248cba44356539	Attached	vpc-04c174d4b9de719d0 asymmetric-vpc	089204451369

At the bottom, there is a detailed view for the internet gateway **igw-098248cba44356539 / asym-igw**, showing the "Details" tab selected. The details include:

- Internet gateway ID: igw-098248cba44356539
- State: Attached
- VPC ID: vpc-04c174d4b9de719d0 | asymmetric-vpc
- Owner: 089204451369

The browser status bar at the bottom indicates the date and time as 12/9/2025, 4:48 PM.

4. Route Tables Creation

Objective

Create route tables to control traffic flow within the VPC.

Public Route Tables

- **Route Table A (Public Subnet A):**
 - **Default Route:** 0.0.0.0/0 → Internet Gateway
- **Route Table B (Public Subnet B):**
 - **Default Route:** 0.0.0.0/0 → Internet Gateway
- **Route Table C (Public Subnet C):**
 - **Default Route:** 0.0.0.0/0 → Internet Gateway

Private Route Tables (Updated)

- **Route Table A (Private Subnet A):**
 - **Default Route:** 10.0.0.0/16
- **Route Table B (Private Subnet B):**
 - **Default Route:** 10.0.0.0/16
- **Route Table C (Private Subnet C):**
 - **Default Route:** 10.0.0.0/16

Steps Taken

1. **Navigate to:** VPC Dashboard → Route Tables → Create Route Table.
2. **Add Routes:**
 - For **public subnets**, the default route points to the **Internet Gateway**.
3. **Associate Route Tables:** Associate the correct route table with each subnet.

4.1 Subnet-to-Route Table Associations

Objective

Ensure proper routing between public and private subnets by associating each subnet with its dedicated route table.

Association Configuration

- **Public Subnets:** Each public subnet is associated with its corresponding public route table.
- **Private Subnets:** Each private subnet is associated with its corresponding private route table.

Steps Taken

1. **Navigate to:** VPC Dashboard → Subnet Associations.

Associate Subnets with Route Tables: Select each subnet and associate it with the correct route table.

The screenshot shows the AWS VPC Route Table creation interface. The top navigation bar includes tabs for 'VPC' and 'Route tables'. The main form is titled 'Create route table' and contains the following fields:

- Route table settings**:
 - Name - optional**: A text input field containing 'pub-rt-01'.
 - VPC**: A dropdown menu showing 'vpc-04c174d4b9de719d0 (asymmetric-vpc)'.
- Tags**: A section for assigning tags. It shows a key 'Name' with a value 'pub-rt-01'.

At the bottom of the page, there are standard AWS navigation links like CloudShell, Feedback, and Console Mobile App, along with system status indicators such as privacy terms, cookie preferences, and system metrics like temperature and battery level.

A screenshot of the AWS VPC console showing the details of a route table. The route table ID is rtb-072fe78af83db3732. It has one explicit subnet association and no edge associations. The routes section shows one route to the local target.

Details

Route table ID rtb-072fe78af83db3732	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-04c174d4b9de719d0 asymmetric-vpc	Owner ID 089204451369		

Routes

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

A screenshot of the AWS VPC console showing the 'Edit routes' page for the same route table. A new route is being added to an Internet Gateway.

Edit routes

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

Add route

Remove

Cancel **Preview** **Save changes**

A screenshot of a web browser showing the AWS VPC console. The URL is <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-072fe78af83db3732>. The page displays a success message: "Updated routes for rtb-072fe78af83db3732 / pub-rt-01 successfully". Below this, there are tabs for Routes, Subnet associations, Edge associations, Route propagation, and Tags. The Subnet associations tab is selected. It shows a table with one row: "No subnet associations". You do not have any subnet associations." At the bottom of the page, the AWS navigation bar and a taskbar are visible.

A screenshot of a web browser showing the AWS VPC console. The URL is <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1>EditRouteTableSubnetAssociations:RouteTableId=rtb-072fe78af83db3732>. The page shows the "Edit subnet associations" section for route table rtb-072fe78af83db3732. It lists available subnets (1/6) and selected subnets. The "Selected subnets" section contains one item: "subnet-0ba404c4b8a42e264 / Public Subnet A". The AWS navigation bar and a taskbar are at the bottom.

Route tables (5) Info

Last updated less than a minute ago

Create route table

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-05df9b23b101693d7	-	-	Yes	vpc-04c174d4b9de719d0
pub-rt-01	rtb-072fe78af83db3732	subnet-0ba404c4b8a42e...	-	No	vpc-04c174d4b9de719d0
pub-rt-02	rtb-07f2bd2a4c227f09	subnet-010c8f8c50f63cb...	-	No	vpc-04c174d4b9de719d0
pub-rt-03	rtb-08ed9d2703476e12a	subnet-04b63502c7f3f1...	-	No	vpc-04c174d4b9de719d0

Select a route table

https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-eas... © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 4:58 PM IN 12/9/2025

Private Route Tables Configuration:

Route table rtb-0f11855ffbcad211b | pvt-rt-01 was created successfully.

Details

Route table ID rtb-0f11855ffbcad211b	Main <input checked="" type="checkbox"/> No	Explicit subnet associations -	Edge associations -
VPC vpc-04c174d4b9de719d0 asymmetric-vpc	Owner ID 089204451369		

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

Routes (1)

Filter routes				
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No	Create Route Table

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 4:59 PM IN 12/9/2025

A screenshot of a web browser showing the AWS VPC console. The URL is <https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0f11855ffbcad211b>. The page title is "Edit subnet associations".

Available subnets (1/6)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Public Subnet C	subnet-04b63502c7f3f126c	10.0.32.0/19	-	rtb-08ed9d2703476e12a / pub-rt-
Public Subnet B	subnet-010c8f8c50f63cbf7	10.0.16.0/20	-	rtb-07f2bdf2a4c227f09 / pub-rt-0
Public Subnet A	subnet-0ba404c4b8a42e264	10.0.0.0/24	-	rtb-072fe78af83db3732 / pub-rt-C
Private Subnet B	subnet-02de7ef7692a15d30	10.0.2.0/23	-	Main (rtb-05df9b23b101693d7)
<input checked="" type="checkbox"/> Private Subnet A	subnet-083045bc5258e20f6	10.0.4.0/22	-	Main (rtb-05df9b23b101693d7)
Private Subnet C	subnet-01e3a5cf1ce8fcf	10.0.128.0/19	-	Main (rtb-05df9b23b101693d7)

Selected subnets

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Private Subnet A	subnet-083045bc5258e20f6	10.0.4.0/22	-	Main (rtb-05df9b23b101693d7)

A screenshot of a web browser showing the AWS VPC console. The URL is <https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables>. The page title is "Route tables (8) [Info](#)".

Route tables (8) [Info](#)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
pub-rt-03	rtb-08ed9d2703476e12a	subnet-04b63502c7f3f1...	-	No	vpc-04c174d4b9de719d0
pvt-rt-01	rtb-0f11855ffbcad211b	subnet-083045bc5258e2...	-	No	vpc-04c174d4b9de719d0
pvt-rt-02	rtb-0274e63e322c71ecc	subnet-02de7ef7692a15...	-	No	vpc-04c174d4b9de719d0
pvt-rt-03	rtb-07e2b9fc7ef267092	subnet-01e3a5cf1ce8fc...	-	No	vpc-04c174d4b9de719d0

Select a route table

5. Tagging Resources

Objective

Ensure consistent tagging across all resources for cost allocation and management.

Tagging Configuration

- **Environment:** "production"
- **Owner:** "network-team"
- **Project:** "asymmetric-vpc-build"
- **CostCenter:** "AWS-Networking"
- **Tier:** "public" or "private" based on subnet type.

Steps Taken

1. **Tag Resources:** Applied tags to VPC, subnets, IGW, NAT Gateways, and Route Tables.

Route Table Tags:

The screenshot shows the AWS VPC console with the URL <https://us-east-1.console.aws.amazon.com/vpcconsole/home/?region=us-east-1#ManageRouteTableTags:RouteTableId=rtb-07f2bdf2a4c227f09>. The page title is "Manage tags for rtb-07f2bdf2a4c227f09". The interface displays a list of tags assigned to the route table, including:

Key	Value - optional
Name	pub-rt-02
Environment	production
Owner	network-team
Project	asymmetric-vpc-build
CostCenter	AWS-Networking
Tier	public

At the bottom of the list, there is a blue "Add new tag" button. The browser's address bar shows the full URL, and the status bar at the bottom right indicates the date and time as "12/9/2025 5:05 PM".

The screenshot shows the AWS VPC console interface. The top navigation bar includes tabs for 'VPC' and 'Route tables'. Below the navigation, the URL is 'us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#ManageRouteTableTags:RouteTableId=rtb-07f2bdf2a4c227f09'. The main content area is titled 'Manage tags for rtb-07f2bdf2a4c227f09'. It displays a table of tags with columns for 'Key' and 'Value - optional'. The tags listed are:

Key	Value - optional
Name	pub-rt-02
Environment	production
Owner	network-team
Project	asymmetric-vpc-build
CostCenter	AWS-Networking
Tier	public

An 'Add new tag' button is located at the bottom left of the tag list. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

Subnet Tags:

The screenshot shows the AWS VPC console interface, similar to the previous one but for a subnet. The top navigation bar includes tabs for 'VPC' and 'Subnets'. Below the navigation, the URL is 'us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#ManageSubnetTags:subnetId=subnet-0ba404c4b8a42e264'. The main content area is titled 'Manage tags for subnet-0ba404c4b8a42e264'. It displays a table of tags with columns for 'Key' and 'Value - optional'. The tags listed are:

Key	Value - optional
Name	Public Subnet A
Environment	production
Owner	network-team
Project	asymmetric-vpc-build
CostCenter	AWS-Networking
Tier	public

An 'Add new tag' button is located at the bottom left of the tag list. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	Private Subnet A
Environment	production
Owner	network-team
Project	asymmetric-vpc-build
CostCenter	AWS-Networking
Tier	private

Add new tag

You can add 44 more tags

6. Conclusion

This document now reflects a revised architecture where internet access for private subnets is handled without the use of NAT Gateways. Instead, **VPC Endpoints** are used for specific AWS service access, and **VPC Peering** may be used for internet access from a connected VPC. This setup reduces costs associated with NAT Gateways while still ensuring private subnets can reach required services.

7. VPC Resource Flow:

