



# Creating a Private Subnet



ucbethuel

The screenshot shows the AWS Management Console interface for creating a new subnet. The top navigation bar includes 'VS', a search bar, and a 'Europe (Ireland)' dropdown. The main navigation path is 'VPC > Subnets > Create subnet'. Below this, the 'IPv4 CIDR' field is set to '10.0.0.0/16'. The 'Subnet settings' section is titled 'Specify the CIDR blocks and Availability Zone for the subnet.' It contains three fields: 'Subnet name' (set to 'NextWork Private Subnet'), 'Availability Zone' (set to 'Europe (Ireland) / euw1-az3 (eu-west-1b)'), and 'IPv4 subnet CIDR block' (set to '10.0.1.0/24'). A note at the bottom right of the subnet settings section indicates '256 IPs'.

OR

ucbethuel  
NextWork Student

[nextwork.org](http://nextwork.org)

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is Amazon Virtual Private Cloud, which help us connect internal resource together, without been exposed to the internet by default.

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet, private route table and NACL

## One thing I didn't expect in this project was...

One thing I didn't expect in this project is clearer understanding.

## This project took me...

This project took me 1 hour, 30 min

OR

ucbethuel  
NextWork Student

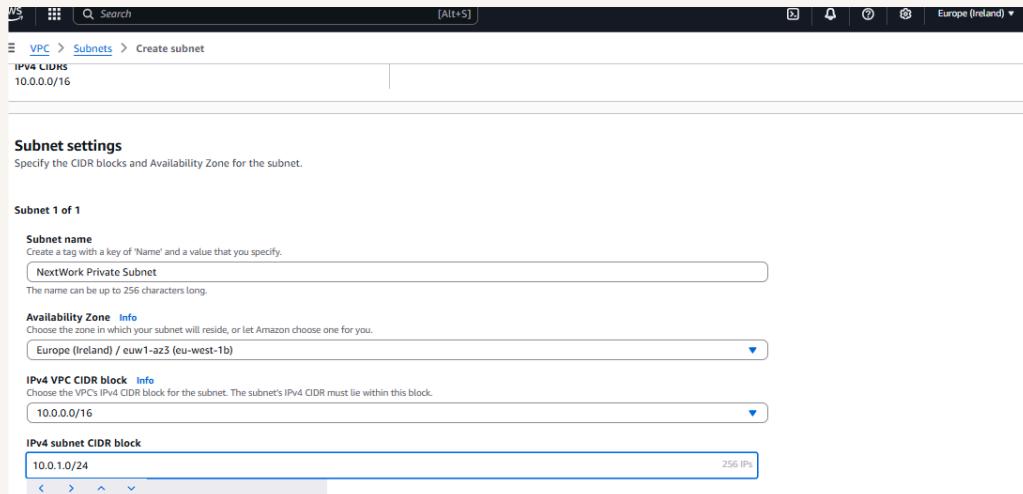
[nextwork.org](http://nextwork.org)

# Private vs Public Subnets

The difference between public and private subnets is that public subnet is exposed to the internet while private is only meant for internal connection.

Having private subnets are useful because it helps us connect user data without exposing it to the internet.

My private and public subnets cannot have the same CIDR block.



OR

**ucbethuel**  
NextWork Student

[nextwork.org](http://nextwork.org)

# A dedicated route table

By default, my private subnet is associated with the Network route table earlier connected.

I had to set up a new route table because so to associate my new private subnet and making it private.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows communication internally.

The screenshot shows the AWS Route Tables page with the following details:

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner
NextWork Public Route Table	rtb-0d085ada6005e8060	subnet-01977e47d1bdce...	-	Yes	vpc-0d950959f5c7e1d69   Next...	19K
-	rtb-0f851a340ff39266c	-	-	Yes	vpc-0847bc65412d751f1	19K
NextWork Private Route Table	rtb-0f85c174747e9bac5	subnet-0800ae4b86359e...	-	No	vpc-0d950959f5c7e1d69   Next...	19K

Below the table, the "rtb-0d085ada6005e8060 / NextWork Public Route Table" details are shown:

- Details tab is selected.
- Routes, Subnet associations, Edge associations, Route propagation, and Tags tabs are available.

OR

ucbethuel  
NextWork Student

[nextwork.org](http://nextwork.org)

# A new network ACL

By default, my private subnet is associated with My previous NextWork Network ACL created in the last class.

I set up a dedicated network ACL for my private subnet because, i have to set up the applicable rules that will make the subnet private.

My new network ACL has two simple rules - 1. Block all inbound traffic. 2. Block all Outbound traffic.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny



[nextwork.org](https://nextwork.org)

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

