



# Creating a Private Subnet

SH

shilpa\_i\_kale@yahoo.com

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the 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**  
 256 IPs

▼ Tags - optional

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is an isolated or private section of the entire AWS. It is useful because resources deployed in VPC are private to the account and cannot be accessed by outside world.

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet.

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

One thing I didn't expect in this project is that the IPv4 CIDR block range should be different for each subnet.

## This project took me...

This project took me 2 hrs including demo, documentation and understanding the concept.

## Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet while private subnets are completely isolated from internet by default.

Having private subnets are useful because keeping resources away from the internet is extremely important for confidential resources.

My private and public subnets cannot have the same IPv4 CIDR block i.e. the same range of ip addresses. The CIDR block for every subnet must be unique and cannot overlap with another subnet.

SH

shilpa\_i\_kale@yahoo.c...

NextWork Student

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

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the 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**  
 256 IPs  
< > ^ ▼

▼ Tags - optional

## A dedicated route table

By default, my private subnet is associated with default route table of VPC which has access to internet through internet gateway.

I had to set up a new route table because my default route table had access to internet through internet gateway. I wanted to have only private access.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic inside VPC.

Route tables (1/3) <a href="#">Info</a>						
<a href="#">Create route table</a>						
<a href="#">Actions</a> <a href="#">Last updated</a> less than a minute ago						
Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	
-	rtb-029d750ddda3dddfaf2	-	-	Yes	vpc-09afe716642db711e	<a href="#">Actions</a>
<input checked="" type="checkbox"/> NextWork Public Route Table	rtb-09f1c7e03b1564b40	subnet-0c1ce3d8f9d462...	-	Yes	vpc-0ea996a744f197a11   <a href="#">Next</a> .	<a href="#">Actions</a>
<input type="checkbox"/> NextWork Private Route Table	rtb-04797720c9bcc938e	subnet-04430e67822957...	-	No	vpc-0ea996a744f197a11   <a href="#">Next</a> .	<a href="#">Actions</a>

## A new network ACL

By default, my private subnet is associated with the default Network ACL of VPC.

I set up a dedicated network ACL for my private subnet because a network ACL becomes crucial in the event of security breaches where traffic that has compromised my public subnet can get access to my private subnet if I've network ACL allowing traffic.

My new network ACL has two simple rules - inbound and outbound denying all the traffic.

The screenshot shows the AWS Network ACLs page with the following details:

**Success Message:** You have successfully updated subnet associations for acl-0d49963df695b1bb9 / NextWork Private NAACL.  
► Details

**Network ACLs (1/3) Info**

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-09ffbed0226302a5a	3 Subnets	Yes	vpc-09afe716642db711e
<input checked="" type="checkbox"/> NextWork Public NAACL	acl-0e9f535dd21547ee1	subnet-0c1ce3d8f9d462278 / NextWork Public ...	Yes	vpc-0ea996a744f197a11 / NextW...
<input type="checkbox"/> NextWork Private NAACL	acl-0d49963df695b1bb9	subnet-04430e678229572b3 / NextWork Priva...	No	vpc-0ea996a744f197a11 / NextW...



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

# The place to learn & showcase your skills

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

