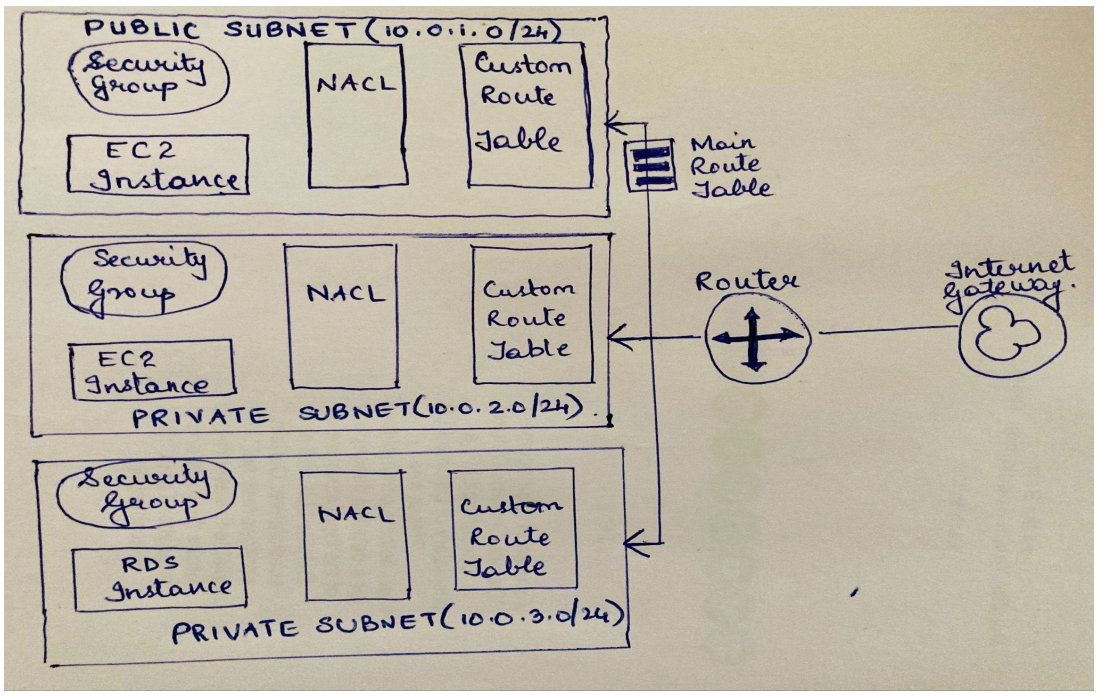
Assignment 3

The basic design of the VPC with 1 public subnet and 2 private subnets with 1 RDS and 1 EC2 instance would be as below:
A **virtual private cloud** (VPC) allows you to specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.A **subnet** is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a **public subnet** for resources that must be connected to the internet, and a **private subnet** for resources that won't be connected to the internet.To protect the AWS resources in each subnet, you use **security groups** and **network access control lists (ACL)**.When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block (example: 10.0.0.0/16). This is the primary **CIDR** block for your VPC.You can add one or more subnets in each Availability Zone of your VPC's region.

Each subnet must be associated with a **route table**, which specifies the allowed routes for outbound traffic leaving the subnet.Every subnet that you create is automatically associated with the **main route table** for the VPC.**Custom Route table** can be created for your VPC.There are two main parts to the route table.

- The destination, which is a range of IP addresses where you want your traffic to go.
- The target, which is the connection through which to send the traffic. In this case, the traffic is routed through the local VPC network.

Internet Gateways allows communication between instances in your VPC and the internet. Create two subnets one is **public** and **private**. You can make the subnet as public by enabling the option of Auto-Assign Public IP by modifying the settings of the subnet, this way the instances created in the public subnet will have public Ip and can access internet. For another subnet you don't have to enable the feature which is listed above still we have to meet another requirement to make it private. Next, you have to modify the route table and add the public subnet in subnet associations and don't select another subnet. This step will ensure that only public subnet can access internet whereas the other subnets cannot access internet because it is not selected in the subnet associations.



The difference in connections as per requirements are specified as follows:

1. **1 private subnet has an RDS instance which is accessible by instances in the other private subnet.**

While the main route table controls the routing for the VPC, one can be more granular about how you want to route the traffic by using the custom route table associated with each of the private subnets. The VPC will use these custom route tables instead of the main route table. By default, each custom route table one creates will have the local route already inside it, allowing communication to flow between all resources and subnets inside the VPC.The destination is the CIDR range of the VPC network and the target will be routed

through VPC network.This combination of destination and target allows traffic to flow freely within the VPC.

2. Instances in the public subnet can communicate with instances in the private subnet

A custom route table is associated with the public subnet. This route table contains an entry that enables instances in the subnet to communicate with other instances in the VPC, and an entry that enables instances in the subnet to communicate directly with the internet. The first local entry is the default entry for communicating with all instances in VPC. It should look something like this:

DESTINATION	TARGET
10.0.0.0/16	local

This combination of destination and target allows instances in the public subset to communicate with instances in the private subset.Also create route rules

3. Instances in the public subnet cannot communicate with the RDS instance.

In this case, you have to set ‘Allow/Deny’ rules in the NACL.NACL rules allow/deny traffic from entering a subnet. The traffic from RDS instance can be denied for the public subnet which will automatically restrict traffic ih that direction.