Networking for Developers (AWS)

1. AWS Cloud and VPC

- **AWS Cloud**: Provides cloud services to host applications and resources.
- **VPC (Virtual Private Cloud)**: A private network within AWS that allows you to isolate and manage your resources.

2. Creating a VPC

- **CIDR Block**: Define an IP address range for your VPC using Classless Inter-Domain Routing (CIDR).
    - **Example**:
        - `10.0.0.0/24`
            - The first part (10.0.0.0) is the network address.
            - The `/24` indicates that the first 24 bits are the network part; thus, the last octet (0-255) can be used for hosts.
            - Range: `10.0.0.1 - 10.0.0.254`.
        - `10.0.0.0/16`
            - Allows for two octets for hosts.
            - Range: `10.0.0.1 - 10.0.255.254`.

3. Subnets within VPCs

- **Subnets**: Defined sets of IP addresses within the VPC.
    - **Private Subnets**: Used for resources that should not be public.
    - **Public Subnets**: Used for resources that need to be accessible from the internet.
- **Best Practice**: Create **2 public** and **2 private subnets** across different Availability Zones for disaster recovery.

4. Launching EC2 Instances

- Once a subnet is created, you can launch EC2 instances within it.

5. Security Groups

- **Security Groups**: Act as a virtual firewall to control inbound and outbound traffic.
    - Example: Allow SSH connections to your EC2 instances.

6. Gateways

- **Gateways** connect your VPC to other networks.
    - **Internet Gateway**: Enables connectivity from your VPC to the internet.
        - Create an internet gateway and attach it to your VPC.

7. Route Tables

- Each subnet requires a route to the internet via the internet gateway.
    - Create a route table:
        - Associate it with the VPC and specific subnets.
        - Add a route:
            - For public subnets, set `0.0.0.0/0` targeting the internet gateway.
            - Save your changes.

8. SSH Access to Private Instances

- To connect to a private EC2 instance via SSH:
    1. Create a private instance in the private subnet.
    2. Set up a new Private Security Group with SSH rules.
    3. Transfer the SSH key to a public server using SCP.
    4. SSH into the public server, then connect to the private instance.

9. NAT Gateway

- **NAT Gateway (Network Address Translation)**: Allows internal instances to connect to external services while preventing external services from initiating connections to private servers.
    - Create a NAT Gateway in the **public subnet** (which has a route to the internet).
    - In the private subnet's route table, add a route to the NAT Gateway (`0.0.0.0/0`).

10. NACLs and Security Groups

- **NACLs (Network Access Control Lists)**: Serve as a virtual firewall for entire subnets.
- **Security Groups**: Function as virtual firewalls for individual EC2 instances.
    - **Stateful**: Any changes to inbound rules automatically apply to outbound rules.