**VPC Setup and Peering Connection**

This setup demonstrates the setup of Virtual Private Clouds (VPCs) on a cloud platform, focusing on testing and production environments. The following steps were taken to establish a secure network architecture:

1. VPC Creation:

- Created two VPCs named "Testing" and "Production."

2. Instance Deployment:

- Provisioned two instances in each VPC to simulate testing and production workloads.

3. Subnets and Routing:

- Segmented each VPC into subnets for effective resource management.

- Attached Internet Gateways for outbound internet access.

- Configured route tables to control traffic within the VPCs.

4. VPC Peering:

- Established a VPC peering connection between the "Testing" and "Production" VPCs.

- VPC peering allows secure and direct communication between instances in different VPCs.

Testing VPC Peering

To verify the functionality of the VPC peering connection, the `ping` command was used to test connectivity between instances:

1. from "Testing" VPC:

- Pinged the private IP address of an instance in the "Production" VPC.

2. from "Production" VPC:

- Pinged the private IP address of an instance in the "Testing" VPC.

Successful ping responses confirmed the operational status of the VPC peering connection.

Note: Ensure that security groups and network ACLs are appropriately configured to allow ICMP traffic for the `ping` command to work across instances.

**Conclusion**

This setup ensures a secure and isolated network environment, allowing communication between testing and production workloads while maintaining the necessary level of isolation.