Virtual Private Cloud (VPC) in AWS

1. Why We Need VPC – For Isolation

In cloud environments like AWS, isolation of resources is a key aspect of security and control. VPC (Virtual Private Cloud) provides a logically isolated section of the AWS cloud where users can launch AWS resources in a virtual network defined by them.

2. Multi-Tenant and Single-Tenant Deployment

When instances are launched on AWS, they are generally deployed in a multi-tenant model, meaning that multiple customers share the same physical hardware. AWS uses a hypervisor to manage this sharing, which separates instances at the virtualization layer. Each AWS account has a unique Account ID, just like Google Cloud uses Project IDs.

In contrast, with a Dedicated Host, you get a single-tenant environment where one host is dedicated to your account only—ideal for companies like Mastercard or Visa where isolation is critical.

3. Logical Segregation – Virtual Private Server (VPS) and Subnets

Logical segregation is achieved using Virtual Private Servers (VPS) and subnets. Think of a physical switch with 16 RJ45 ports. If you use two switches and want to segregate traffic, you can create subnets (e.g., 4-4 subnets per switch). Subnets allow division of the VPC's IP range into smaller logical segments:

1. Public Subnet – Connects to the internet (via Internet Gateway).
2. Private Subnet – Internal only (no Internet access).

4. Internet Gateway (IGW) and Uplink Concept

To allow external internet access, an Internet Gateway (IGW) must be attached to the VPC. If no IGW is attached, the instance remains private and cannot access the internet. In a physical network setup, this is similar to uplinking the last port (16th) on a switch to another switch to connect both.

5. IP Addressing and Subnetting

There are three main classes of IP addresses:

- Class A: 0–126 (/8 subnet mask)
- Class B: 128–191 (/16 subnet mask)
- Class C: 192–223 (/24 subnet mask)

Each IP address consists of 4 octets (e.g., 10.0.0.0).

CIDR (Classless Inter-Domain Routing) allows flexible IP address assignment. For example:

- CIDR Block: 10.0.0.0/24
- Subnet Mask: /24 means 32 - 24 = 8 bits available for hosts

- Number of IPs = 2^8 = 256 addresses (usable: 254)
- IP Range: 10.0.0.0 – 10.0.0.255

6. Routers and Cross-Class Communication

Different IP classes (or networks) cannot communicate with each other unless connected by a router. A router connects multiple networks together and routes traffic between them.

7. OSI Model Layers (Networking Basics)

The OSI Model consists of 7 layers:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

8. Summary

VPC helps in creating isolated environments in AWS where resources can be securely launched and managed. With tools like subnets, internet gateways, and routing, you can control public/private communication, IP addressing, and overall network structure.