# Experiment-08

## Multiple VPC Networks: Explore benefits of using multiple VPC networks in Google Cloud for organizing and isolating resources.

**Google Cloud**, **Virtual Private Cloud (VPC)** allows you to define and control networking environments for your resources. You can have multiple VPC networks, each isolated from one another or interconnected for specific use cases. Managing multiple VPCs helps you scale, secure, and organize resources efficiently.

### Benefits of Using Multiple VPC Networks

**Resource Isolation & Security**

- **Network Isolation** – You can isolate resources within different VPC networks to improve security and control traffic between services.
- **Private Connectivity** – Each VPC can have private IPs that do not communicate with other VPCs unless explicitly allowed, keeping sensitive data isolated.
- **Granular Firewall Rules** – Define specific firewall rules for each VPC, limiting access to resources within a VPC or between multiple VPCs.

**Organizational Structure & Management**

- **Separation by Department or Service** – Different teams or services (e.g., dev, test, production) can operate within their own VPCs, helping to organize and manage resources based on logical groupings.

- **Custom Subnetting** – Each VPC can have its own subnet structure tailored to the needs of specific projects or services.

**Traffic Control**

- **VPC Peering** – You can allow traffic between two or more VPCs by creating VPC peering connections. This gives you flexibility in managing traffic flow while maintaining network isolation.
- **Shared VPC** – A **Shared VPC** allows multiple projects to connect to a common VPC network, enabling central management of network resources.
- **Private Google Access** – For certain services, you can configure access to Google Cloud services without using public IPs, enhancing security.

**Scaling Flexibility**

- **Scalability for Different Environments** – As projects or environments grow, you can add more VPCs, allowing the architecture to scale without impacting other parts of the system.
- **Cross-Region Connectivity** – Create VPCs in different regions for disaster recovery and global distribution of your resources. Google Cloud provides the ability to set up global VPCs and establish secure connections across regions.

**Enhanced Network Performance**

- **Low Latency Communication** – By grouping resources that need high throughput and low latency within a specific VPC, you can optimize performance for specific workloads.

- **Dedicated Resources** – Certain VPCs can be dedicated to specific high-performance workloads (e.g., compute-intensive tasks), while others may be used for general workloads, ensuring efficient resource use.

## Use Cases for Multiple VPCs

### Multi-Tier Applications

You can deploy **multi-tier architectures** where each tier (e.g., web, app, database) resides in separate VPC networks, enabling better isolation and security between tiers.

### Cross-Region Architecture

You can deploy resources in multiple regions for **disaster recovery** or to meet **local compliance requirements** while maintaining network isolation between regions. For instance, a production VPC in one region and a disaster recovery VPC in another.

### Hybrid Cloud or Multi-Cloud

If you're integrating **on-premises infrastructure** or other **cloud platforms** with Google Cloud, using separate VPCs for each environment allows secure and controlled network communication across different systems.

### Managed Service Integration

You might have **managed services** (like **Cloud SQL** or **BigQuery**) in one VPC while using compute instances or other resources in another, optimizing resource placement.

## Set Up Multiple VPC Networks in Google Cloud

### Step 1: Create a VPC Network

1. Go to **Google Cloud Console → Navigation Menu (☰) → VPC Network → Create VPC Network**.
2. Specify the **name**, **region**, and **subnet configuration** for your VPC.
3. Click **Create**.

### Step 2: Create Additional VPC Networks

1. You can repeat the process to create as many VPCs as needed.
2. Choose **Custom** subnet mode to define your own subnets or **Auto mode** for auto-assigned subnets.

### Step 3: Set Up VPC Peering (Optional)

1. Go to **VPC Network Peering → Create Peering Connection**.
2. Select the **Source VPC** and **Destination VPC**.
3. Define the **network and routes** that can be shared across the VPCs.
4. Click **Create**.

### Step 4: Create Firewall Rules (Optional)

1. Go to **Firewall Rules → Create Firewall Rule**.
2. Define the **source and destination** VPCs, and configure the firewall to allow or deny traffic between the VPCs.

## Step 5: Set Up Shared VPC (Optional)

1. Go to **VPC Networks → Shared VPC → Set up a Shared VPC**.
2. Select the **host project** and **service projects**.
3. Share the VPC resources with other projects.

## Output