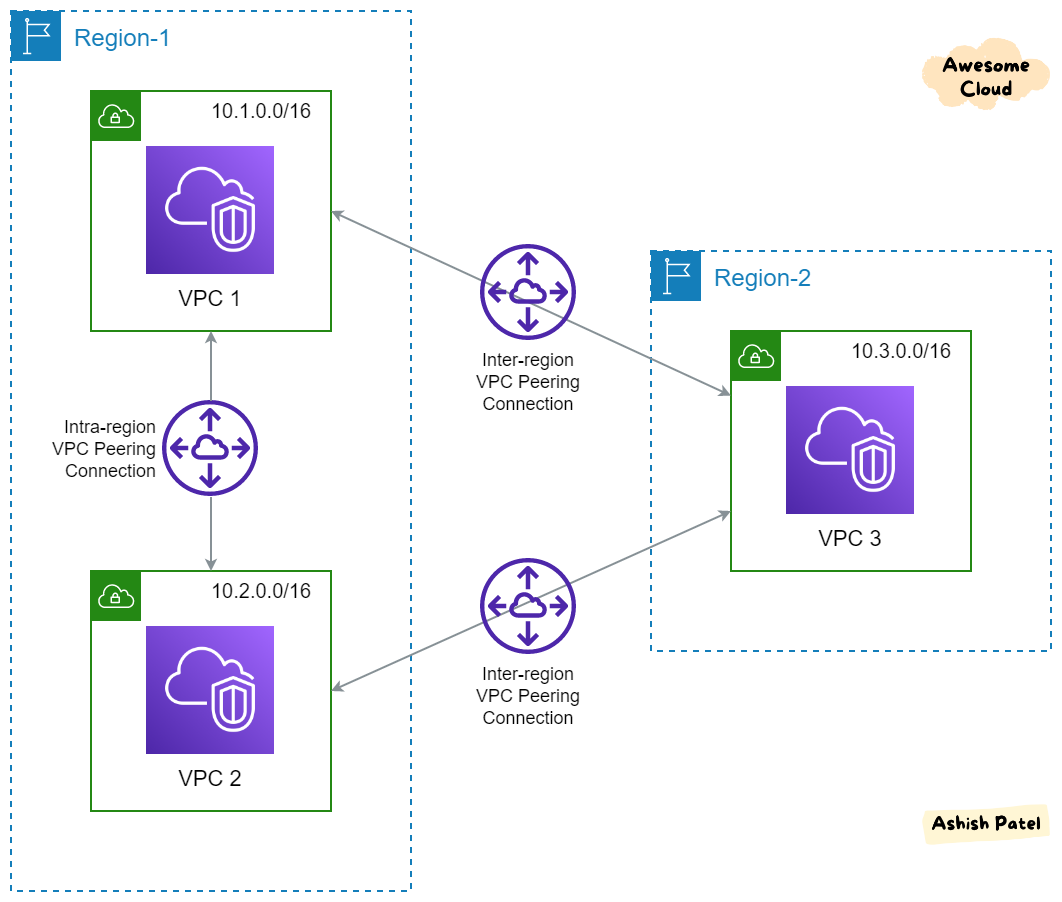
**VPC PEERING DOC - THEORY**



## What is VPC Peering? 🧩

A **VPC peering connection** links two Virtual Private Clouds (VPCs), enabling them to communicate over private IPv4/IPv6 as if within the same network—without VPNs, NAT, internet gateways, or extra hardware. It supports peering **within the same AWS account**, **across accounts**, and **between regions** (inter-region peering). All traffic stays on AWS’s private backbone and is **encrypted end-to-end**, with no single point of failure or bandwidth bottleneck

URL : <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html?>

## How It Works – Key Concepts :

**One-to-one**: Each peering connects exactly two VPCs. There's no transitive routing—VPC A↔B and A↔C does **not** allow B↔C traffic.

**Non-overlapping CIDRs**: You must configure VPCs with distinct CIDR blocks.

**High performance**: Low latency, high throughput via AWS backbone.

## ****Cost****: No charge to create; data transfer fees apply for cross-AZ and cross-region traffic URL : <https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-peering.html?> Use Cases

**Secure inter-VPC communication**: Access shared services (like databases) or authenticate centrally without the public internet.

**Cross-region resilience**: Replicate critical data across regions for disaster recovery or high availability

**Multi-account architecture**: Maintain isolated VPCs per team/account while enabling controlled communication.

**Cost optimization**: Avoid NAT or VPN costs by routing directly via private networks

## Limitations & Considerations

**No transitive routing**: Each desired VPC pair needs its own peering.

**Peering limits**: Up to 125 peering connections per VPC

**Route management**: Must manually add routes in each VPC’s route table.

**Security group rules**: Cannot reference SGs by ID across regions—use CIDR blocks instead

**Billing**: Cross-AZ/data transfer costs apply—standard rates

## Impact on EC2 Instances

There’s **no special configuration** needed on EC2 instances themselves—after peering and route table updates, they can communicate over private IPs. Ensure:

**Route tables** in each subnet include a route to the peer VPC via the peering connection.

**Security groups and NACLs** permit inbound/outbound traffic to/from the peer CIDR.

**DNS resolution** of private hostnames works across VPCs (optional).

There’s no performance degradation or instance instability due to peering—EC2s function as usual  
  
  
  
  
  
IMPORTANT URL’s :   
  
 Peering limitations & scenarios : [https://docs.aws.amazon.com/vpc/latest/peering/peering-scenarios.html?](https://docs.aws.amazon.com/vpc/latest/peering/peering-scenarios.html?utm_source=chatgpt.com)   
  
Billing for Cross account vpc peering : https://repost.aws/questions/QUtev59SLXQamxKMKpk6VMCw/billing-for-cross-account-vpc-peering?