Cross Region VPC Connection

✅ Step 1: Prepare VPCs

- Go to AWS Console
- Create two VPCs in different regions (e.g.):
  VPC-A in us-east-1 → 10.0.0.0/16
  VPC-B in eu-west-1 → 10.1.0.0/16
- Ensure the CIDRs do not overlap
- Create subnet in each VPC
- Make Route Table for both VPC
- Associated subnet with route table
- Attach IGW to Both Subnet and route it on specific route table

---

✅ Step 2: Create Peering Connection (From VPC-A)

1. Go to VPC Dashboard in us-east-1
2. Click Peering Connections > Create Peering Connection
3. Fill the form:
   - Name tag (optional)
   - Requester VPC: Select VPC-A
   - Account: My account
   - Region: eu-west-1
   - Accepter VPC ID: Select VPC-B
4. Click Create Peering Connection

✅ Step 3: Accept the Peering (In VPC-B)

1. Switch to region eu-west-1
2. Go to Peering Connections
3. You'll see a pending request
4. Select it → Click Accept Request

✅ Step 4: Update Route Tables

For VPC-A (us-east-1):

1. Go to Route Tables
2. Select route table for VPC-A subnets
3. Edit routes

   Destination: 10.1.0.0/16 (VPC-B)
   Target: Peering Connection ID (e.g., pcx-123456)

For VPC-B (eu-west-1):

1. Do the same
2. Destination: 10.0.0.0/16
3. Target: Peering Connection ID

✅ Step 5: Modify Security Groups

1. Go to EC2 > Security Groups
2. Add inbound rules in both VPCs to allow traffic:
   - Type: All traffic / ICMP / SSH (your choice)
   - Source: Other VPC's CIDR block

✅ Step 6: Test the Peering Connection

1. Launch EC2 in each VPC (in private/public subnets)
2. From EC2 in VPC-A:
   ping <private IP of EC2 in VPC-B>
3. Vice verse with VPC-B