VPC Peering

- **What it is:** A private, point-to-point network link between two VPCs so instances can talk over **private IPs** (IPv4/IPv6).
- **Where it works:** Same or different **accounts**; same or different **Regions** (inter-Region peering).
- **Key limits:**
  - **No transitive routing** (A↔B and B↔C doesn't make A↔C).
  - **CIDR blocks must not overlap.**
  - You **can't** route traffic from the internet, a VPN, or Direct Connect **through** a peering connection ("edge-to-edge" not supported).
  - **Security groups cannot reference SGs in another VPC** over peering; use CIDR rules.

- Identify **VPC IDs** and **CIDRs** (e.g., VPC-A `10.0.0.0/16`, VPC-B `10.1.0.0/16`).
- Decide which **subnets/route tables** need to talk (every **subnet** uses a **route table**).
- Note **accounts/Regions** involved:
  - **Same account & Region:** easiest; can auto-accept.
  - **Cross-account:** the peer owner must accept.
  - **Inter-Region:** works; uses AWS backbone (still no transitive routing).
- Decide on **DNS needs** across VPCs (e.g., resolve private hostnames/Route 53 PHZ across peers).

A) Create the peering connection

1. Open **VPC Console** → **Peering connections** → **Create peering connection**.
2. Choose **Requester VPC**.
3. Set **Accepter VPC** (same account/Region, different account, or different Region).
4. (Optional) Add tags.
5. **Create**.

B) Accept the request

- **Same account:** select the new peering connection → **Actions** → **Accept request**.
- **Cross-account:** the peer account owner logs in and accepts from their VPC console.

C) Add routes (both sides)

For every subnet that needs to talk to the other VPC:

1. **VPC** → **Route tables** → pick the route table used by your subnets.
2. **Edit routes** → **Add route**:
   - **Destination:** the peer VPC's **CIDR** (e.g., `10.1.0.0/16`).
   - **Target:** the **Peering connection** (e.g., `pcx-…`).
3. Repeat on the **other VPC's** route tables with your CIDR.

D) Update security controls

- **Security Groups:** allow traffic **from the peer VPC's CIDR** (e.g., allow TCP/5432 from `10.0.0.0/16`).
- **NACLs (if used):** allow the same traffic in/out.

E) Enable cross-VPC DNS (optional but common)

If you need to resolve private hostnames across VPCs (e.g., EC2 private DNS or Route 53 PHZ):

1. Go to **Peering connections → Select your pcx → Actions → Edit DNS settings**.
2. Enable **Allow DNS resolution from remote VPC** on **both** sides.
3. If using **Route 53 Private Hosted Zones** across VPCs, either:
   - Associate the PHZ with **both** VPCs (preferred), **or**
   - Use split-horizon/nameserver forwarding if association isn’t viable.