1. Basics & Concepts

• What is a VPC?: A Virtual Private Cloud (VPC) is a logically isolated section of the AWS cloud where you can define your own IP address ranges, subnets, and configure routing and security.

• VPC vs Subnet: A VPC is the overall network environment. Subnets divide the VPC into smaller networks within specific Availability Zones.

• Default vs Custom VPC: AWS provides a default VPC for quick deployment. Custom VPC gives more control over network design and security.

• CIDR Block: Classless Inter-Domain Routing (CIDR) defines the IP address range of the VPC. Cannot overlap with other connected networks.

2. Subnets & IP Addressing

• Public vs Private Subnet: Public subnets have a route to an Internet Gateway. Private subnets do not, typically accessed via NAT.

• Choosing CIDR Ranges: Plan for future expansion. Use non-overlapping private ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

• Subnet Sizing: Ensure enough IP addresses. AWS reserves 5 IPs per subnet.

• Multiple Subnets per AZ: Possible for separating workloads or applying different security rules.

3. Internet & NAT Gateways

• Internet Gateway (IGW): Attach to VPC to allow internet access for public subnets.

• NAT Gateway vs NAT Instance: NAT Gateway is managed, scalable, highly available. NAT Instance is self-managed, cheaper for small workloads.

• No Internet in Private Subnet: Ensure route to NAT Gateway in route table. NAT must be in public subnet.

4. Route Tables

• Main vs Custom Route Table: Main table is default for subnets without explicit association. Custom tables allow different routing rules.

• Route Priority: Most specific route is used first.

• Common Routing Issues: Check target type (IGW, NAT, VPC Peering, TGW) and subnet association.

5. Security

• Security Groups vs NACLs: SG = stateful, attached to ENIs. NACL = stateless, subnet-level rules.

• Restricting Access: Limit inbound to specific IPs. Deny all except necessary ports.

• Flow Logs: Enable to capture IP traffic for security audits and troubleshooting.

6. Peering & Hybrid Connectivity

• VPC Peering: Connects two VPCs privately. Cannot have overlapping CIDR ranges. No transitive peering.

• Transit Gateway (TGW): Central hub to connect multiple VPCs and on-premises networks.

• VPN & Direct Connect: VPN = encrypted over public internet. Direct Connect = dedicated private link, faster and more secure.

7. Cost & Best Practices

• Reducing Costs: Delete unused Elastic IPs, NAT Gateways, and VPC endpoints.

• Design for Growth: Plan subnets and CIDR for scaling. Use multiple AZs for HA.

• Monitoring: Use CloudWatch and VPC Flow Logs to monitor traffic and detect anomalies.