AWS VPC – Full Notes

🔹 What is Amazon VPC?

Amazon Virtual Private Cloud (VPC) is a **logically isolated** section of the AWS cloud where you can launch AWS resources in a **custom-defined virtual network**.

It gives you full control over:

- IP address ranges
- Subnets
- Routing
- Network access
- Internet connectivity

Think of a VPC as your **own private data center** in the cloud.

🔹 Key Components of VPC

Component	Description
VPC	Isolated virtual network
Subnet	A range of IPs in a VPC (public or private)
Route Table	Controls traffic routing in/out of subnets
Internet Gateway (IGW)	Enables internet access for the VPC
NAT Gateway/Instance	Enables private subnets to access the internet
Elastic IP (EIP)	Static public IP for AWS resources
Security Groups	Virtual firewalls for EC2
Network ACLs (NACLs)	Optional stateless firewall for subnets
DHCP Options Set	Define custom DNS/DHCP behavior
VPC Peering	Connect VPCs to share resources
Transit Gateway	Central hub for connecting VPCs and on-premises networks

---

🔹 CIDR and IP Addressing

- CIDR: Classless Inter-Domain Routing (e.g., 10.0.0.0/16)

- A VPC supports IP ranges from /16 to /28
- Subnets are created from this CIDR block
- 5 IP addresses in each subnet are **reserved**:
  - .0 (network ID)
  - .1 (VPC router)
  - .2 (DNS)
  - .3 (future use)
  - .255 (broadcast)

🔹 Subnets

- **Public Subnet**: Has a route to the Internet Gateway
- **Private Subnet**: No direct access to the internet
- **Subnets are AZ-specific** — you must create one per Availability Zone (AZ)

Best practice: Have **multiple subnets across multiple AZs** for high availability.

🔹 Internet Gateway (IGW)

- Provides outbound **and inbound** internet access to public subnets
- Must be **attached to the VPC**
- Requires **route table entry** like 0.0.0.0/0 → IGW

🔹 NAT Gateway vs NAT Instance

Feature	**NAT Gateway**	**NAT Instance**
Managed	✅ Yes	❌ No (manual setup)
Availability	Highly available (in AZ)	EC2 instance (failover needed)
Performance	Scales automatically	Limited by instance type
Cost	Higher	Lower (for light use)
Use Case	Production	Dev/test/small workloads

🔹 Route Tables

- **Each subnet** must be associated with **one route table**

- The **main route table** is used by default unless overridden
- Route targets include:
  - Internet Gateway (IGW)
  - NAT Gateway
  - VPC Peering
  - Transit Gateway
  - Virtual Private Gateway (for VPNs)

🔹 Security Groups vs NACLs

Feature	**Security Group**	**NACL**
Operates at	Instance level	Subnet level
Stateful	✅ Yes	❌ No
Rules	Allow only	Allow and deny
Default behavior	Deny all inbound, allow all outbound	Allow all
Use case	Per-resource firewall	Optional subnet firewall

🔹 VPC Peering

- Connects **two VPCs** privately using AWS backbone
- **No transitive peering**: VPC A ↔ VPC B ↔ VPC C does **not** mean A ↔ C
- Works **within or across regions**
- Must update **route tables and security groups** manually

🔹 AWS Transit Gateway

- Connects **multiple VPCs and on-prem networks**
- Acts as a **central hub** (hub-and-spoke model)
- **Scalable, efficient, and transitive**
- Recommended for **large-scale networks**

🔹 VPC Endpoints

Type	**Description**
Interface Endpoint	Private link to AWS services over ENI (Elastic Network Interface)
Gateway Endpoint	For **S3 and DynamoDB**, routes traffic via the gateway inside the VPC

Benefits:

- **No public IP needed**
- Avoids **internet exposure**
- Reduces **data transfer costs**

🔹 VPC Flow Logs

- Capture **network traffic logs** at the **VPC, subnet, or ENI** level
- Sent to **CloudWatch Logs** or **S3**
- Useful for:
    - Security audits
    - Troubleshooting
    - Compliance

🔹 VPN and Direct Connect

Feature	**Description**
Site-to-Site VPN	Encrypted tunnel over public internet to on-prem
Direct Connect	Dedicated fiber connection to AWS (lower latency, more reliable)
Customer Gateway (CGW)	On-prem device or software that connects to AWS
Virtual Private Gateway (VGW)	AWS side of the VPN connection

🔹 Default VPC vs Custom VPC

Feature	**Default VPC**	**Custom VPC**
Created automatically	✅ Yes	❌ No (user-defined)
Public Subnet	✅ Yes	❌ No (must define)
CIDR Range	172.31.0.0/16	Customizable

Feature	Default VPC	Custom VPC
Best for	Quick tests	Production workloads

🔹 Monitoring & Logging

- Use **VPC Flow Logs** for network traffic
- Monitor **NAT Gateway metrics** via **CloudWatch**
- Audit **route table changes** via **AWS Config**
- Use **CloudTrail** for all VPC-level API actions

🔹 Best Practices for VPC

✅ Always use **Custom VPCs** for production

✅ Split into **Public and Private Subnets**

✅ Deploy across **multiple AZs**

✅ Use **NAT Gateway** for private subnets

✅ Apply **least privilege** to security groups

✅ Use **VPC Flow Logs** to monitor traffic

✅ Use **Network ACLs** for stateless rules

✅ Prefer **Transit Gateway** for multi-VPC networks

✅ Tag resources for visibility and automation

✅ Protect against misconfiguration with **AWS Config** rules

🔹 Common Use Cases

Use Case	VPC Feature Used
Host a public web app	Public subnet + IGW
Secure backend services	Private subnet + NAT Gateway
Connect office to AWS	Site-to-site VPN / Direct Connect
Connect multiple environments	VPC Peering or Transit Gateway
Private access to AWS services	VPC Endpoints