**1. What is AWS VPC?**

**Answer:** Amazon VPC lets you **provision a logically isolated section of AWS** where you can launch AWS resources in a virtual network that you define.

**2. What are the key components of a VPC?**

**Answer:**

* **Subnets (Public/Private)**
* **Route Tables**
* **Internet Gateway (IGW)**
* **NAT Gateway / Instance**
* **Security Groups**
* **Network ACLs (NACLs)**
* **Elastic IPs (EIP)**

**3. What is the default VPC?**

**Answer:** A **pre-created VPC** in each region with a public subnet, internet gateway, and route table — so users can launch instances without configuring networking.

**4. What is the CIDR block in a VPC?**

**Answer:** Classless Inter-Domain Routing block, defines the **IP address range** of your VPC. Example: 10.0.0.0/16 supports 65,536 IPs.

**5. Difference between Public and Private Subnet?**

**Answer:**

* **Public Subnet**: Has a route to the **Internet Gateway**.
* **Private Subnet**: No route to IGW. Used for internal services (DBs, backend).

**6. What is an Internet Gateway?**

**Answer:** A **horizontally scaled, redundant gateway** that enables internet communication for instances in a VPC.

**7. What is a NAT Gateway?**

**Answer:** Allows **instances in a private subnet** to access the internet **outbound**, while preventing inbound internet access.

**8. What is the use of a Route Table in VPC?**

**Answer:** Controls **traffic flow** for subnet(s) by mapping destination CIDR blocks to targets (IGW, NAT, VGW, etc.)

**9. What are Security Groups in VPC?**

**Answer:** Virtual firewalls at the **instance level**, **stateful**, allow inbound and outbound rules.

**10. What are Network ACLs?**

**Answer:** Subnet-level firewalls, **stateless**, support **allow and deny** rules.

**11. Difference between Security Group and NACL?**

**Answer:**

| **Feature** | **Security Group** | **NACL** |
| --- | --- | --- |
| Level | Instance | Subnet |
| Stateful | Yes | No |
| Rules | Allow only | Allow/Deny |
| Applies to | ENIs | Entire Subnet |

**12. Can you assign multiple subnets in different AZs to the same VPC?**

**Answer:** Yes. A VPC can span **multiple Availability Zones**, each with its own subnets.

**13. Scenario: EC2 in private subnet needs internet access. Solution?**

**Answer:**

* Attach a **NAT Gateway** in a **public subnet**.
* Update private subnet’s route table to forward 0.0.0.0/0 to NAT GW.

**14. What is VPC Peering?**

**Answer:** Enables **communication between two VPCs** using private IPs. No transit routing. One-to-one connection.

**15. Can VPCs in different regions be peered?**

**Answer:** Yes. It's called **Inter-Region VPC Peering**, but **latency and data transfer charges** apply.

**16. What is a Virtual Private Gateway (VGW)?**

**Answer:** A gateway attached to your VPC for **VPN or Direct Connect connections** to your on-premises network.

**17. What is a Transit Gateway (TGW)?**

**Answer:** A **central hub** that connects multiple VPCs and on-prem networks using **a single attachment** per VPC.

**18. What is VPC Flow Logs?**

**Answer:** Captures **IP traffic logs** going to and from network interfaces in your VPC. Useful for **monitoring and troubleshooting**.

**19. What is Elastic IP (EIP)?**

**Answer:** A **static IPv4 address** allocated to your account. Can be remapped across instances for **failover** scenarios.

**20. Can a subnet be in more than one AZ?**

**Answer:** No. **Each subnet is scoped to a single AZ**.

**21. Scenario: You need VPC-to-VPC communication in 10+ accounts. What’s the best solution?**

**Answer:** Use **Transit Gateway** instead of peering for **scalability and central management**.

**22. How to make a private subnet truly private?**

**Answer:**

* No IGW route
* No NAT Gateway
* No direct access from internet-facing Load Balancers

**23. Scenario: You need a web server (public) and DB (private). How to set it up?**

**Answer:**

* Public subnet with IGW for web server
* Private subnet with no IGW for DB
* Security Group: Web allows 80/443, DB allows only MySQL (3306) from web server

**24. How do you share VPCs across accounts?**

**Answer:** Use **AWS Resource Access Manager (RAM)** to **share subnets and VPCs** between accounts.

**25. What is the default limit of VPCs per region? Can you increase it?**

**Answer:** Default: **5 VPCs per region**. Yes, limit can be increased via AWS support.

**26. How does a VPC Endpoint work?**

**Answer:** Allows **private connectivity to AWS services** like S3 or DynamoDB without using the internet.

**27. Difference between Interface and Gateway VPC Endpoints?**

**Answer:**

* **Interface Endpoint**: Uses ENI for services like SSM, SNS
* **Gateway Endpoint**: Route-table-based access (e.g., S3, DynamoDB)

**28. How to prevent EC2 instances in public subnet from being accessed over the internet?**

**Answer:**

* Remove 0.0.0.0/0 IGW route
* Adjust security group to deny inbound traffic

**29. Can a single instance belong to multiple subnets?**

**Answer:** No. An EC2 instance is launched in **a single subnet**, but can have **multiple ENIs** (each in different subnets).

**30. How do you isolate environments (dev, test, prod) in a single VPC?**

**Answer:**

* Use **separate subnets**
* Apply **different route tables, NACLs, and security groups**
* Consider separate **VPCs or accounts** for strict isolation

**31. What is IPAM in AWS?**

**Answer:** **IP Address Manager** – Helps plan, track, and manage **IP address allocations** across VPCs and accounts.

**32. Scenario: Your VPC CIDR block is exhausted. How to fix?**

**Answer:** Use **VPC CIDR block expansion** to add a **secondary CIDR range**.

**33. What happens if you delete a route table or IGW?**

**Answer:**

* Routes will be lost, connectivity breaks.
* Instances may not reach the internet.

**34. How do you protect VPC resources from public access?**

**Answer:**

* Use **Private Subnets**
* Apply strict **security groups/NACLs**
* Use **VPC Endpoints** instead of IGW
* Enable **flow logs + GuardDuty**

**35. Scenario: VPC Peering created but EC2s can’t communicate. Why?**

**Answer:**

* Routes not added in route tables
* Security group doesn’t allow traffic
* Overlapping CIDRs
* NACL blocking traffic

**36. Can you create a VPC without an IGW?**

**Answer:** Yes. It becomes **private-only**. You can use it for internal-only workloads or connect via **VPN/Direct Connect**.

**37. What is the MTU for VPC traffic?**

**Answer:** Default **1500 bytes**. For **enhanced networking (ENA)**: up to **9001 bytes** (jumbo frames).

**38. What is Subnet Auto-assign Public IP setting?**

**Answer:** When enabled, **instances launched in the subnet get a public IP automatically**.

**39. How to allow cross-region access to resources without peering?**

**Answer:**

* Use **AWS PrivateLink**
* Use **Transit Gateway + VPN/Direct Connect**
* Use **Global Accelerator**

**40. How can you log traffic to/from a specific ENI or subnet?**

**Answer:** Enable **VPC Flow Logs**, choose ENI/subnet/VPC scope, and send logs to **CloudWatch or S3**.