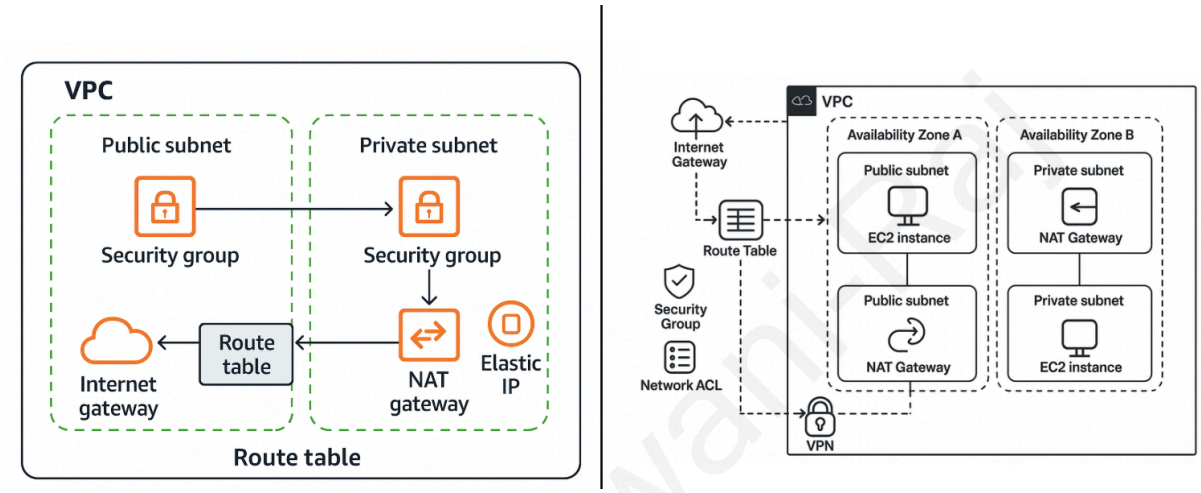
AWS EC2 Short Notes

Includes

✅ **Concise and powerful notes on Amazon VPC**
✅ **34 frequently asked VPC interview questions and answers**
✅ **5 real-world scenario-based VPC questions**



1. Overview of VPC

- **VPC (Virtual Private Cloud)** is a private network within AWS where users can launch and manage AWS resources, such as EC2 instances, RDS databases, and more.
- It provides full control over network configuration, including IP address range, subnets, routing tables, and security settings.
- VPCs enable secure communication between AWS resources while isolating them from external networks.

---

2. Key Components of VPC

Subnets

- A **Subnet** is a range of IP addresses in a VPC, divided into **public** and **private** subnets.
    - **Public Subnets**: Can be accessed directly from the internet (used for resources like web servers).
    - **Private Subnets**: Not accessible from the internet directly (used for databases and application servers).

Raj Nathwani Raj

Route Tables

- A **Route Table** controls the routing of network traffic within a VPC.
- It includes routes that determine where traffic will go based on its destination IP.
- Route tables are associated with subnets, and each subnet must have a route table.

Internet Gateway (IGW)

- An **Internet Gateway** is a horizontally scaled, redundant, and highly available component that allows communication between EC2 instances in your VPC and the internet.
- It must be attached to a VPC to enable internet access for instances in public subnets.

NAT Gateway

- A **NAT Gateway** allows instances in a private subnet to initiate outbound traffic to the internet, while blocking inbound internet traffic.
- It is typically used for software updates or accessing external resources from private instances.

Security Groups

- **Security Groups** act as virtual firewalls for EC2 instances to control inbound and outbound traffic.
    - They are stateful (allowing return traffic automatically).
    - Security groups are applied at the instance level.
    - Can be configured with specific rules, such as allowing traffic from a specific IP or port.

Network Access Control Lists (NACLs)

- **NACLs** control inbound and outbound traffic at the subnet level.
- They are stateless, meaning they do not track the state of connections.
- NACLs allow or deny traffic based on rules like IP address, port, and protocol.

Elastic IP (EIP)

- An **Elastic IP** is a static IPv4 address designed for dynamic cloud computing.
- It can be associated with an EC2 instance or NAT Gateway.
- It is useful when you need a fixed IP address to ensure continuous access to your resources.

VPC Peering

- **VPC Peering** allows two VPCs to communicate with each other as if they are within the same network.
- Peering can occur within the same region (Intra-region VPC Peering) or across different regions (Inter-region VPC Peering).
- No overlapping IP ranges are allowed for VPC Peering.

Raj Nathwani Raj

VPN Connections

- **VPN Connections** provide secure communication between your AWS VPC and an on-premises network over the internet.
- Commonly used to extend a corporate network to AWS.

DHCP Options Set

- **DHCP (Dynamic Host Configuration Protocol)** Options set defines parameters like domain names and DNS servers for instances in the VPC.
- This enables instances to automatically receive network settings when they are launched.

VPC Endpoints

- A **VPC Endpoint** allows private connections between your VPC and AWS services (e.g., S3, DynamoDB).
- There are two types:
    - **Interface Endpoints**: Uses Elastic Network Interfaces (ENIs) for communication.
    - **Gateway Endpoints**: Used to route traffic to S3 or DynamoDB within the VPC.

---

3. VPC Features

Isolation

- VPCs are isolated from each other by default, providing a secure environment for your resources.
- Resources in one VPC cannot directly communicate with resources in another unless explicitly configured (e.g., through VPC Peering).

Customizable Network Topology

- VPC allows users to choose their **IP address range** (CIDR block), create subnets, configure route tables, and set up gateways for routing.
- Provides complete control over the network layout, enabling you to meet specific security and performance needs.

Security

- **Security Groups**: Act as firewalls to control traffic at the instance level.
- **NACLs**: Provide an additional layer of security by controlling traffic at the subnet level.
- **Private Subnets**: For sensitive data or application servers that should not be directly accessible from the internet.

Scalability

Raj Nathwani Raj

- VPCs allow you to scale resources like EC2 instances, load balancers, and databases as your needs grow.
- You can dynamically add more subnets, resources, and services within your VPC.

Cost-Effectiveness

- You pay only for the resources you use within your VPC, such as the NAT Gateway, Elastic IPs, and data transfer.
- VPC resources like subnets and route tables are free of cost, and charges are only applicable for specific services (e.g., data transfer or Elastic IP).

---

4. Common Use Cases for VPC

1. **Secure Network Environment**
    - Create a private, secure network to launch AWS resources like EC2, RDS, etc., with controlled access to the internet.
2. **Hybrid Cloud**
    - Extend your on-premises network to the cloud with VPN or Direct Connect, ensuring secure communication between your data center and AWS resources.
3. **Web Applications**
    - Use public subnets for front-end web servers and private subnets for back-end databases and application servers, ensuring that only authorized traffic reaches the backend resources.
4. **Multi-Tier Architectures**
    - Deploy multi-tier architectures where each layer (web, application, and database) is isolated in separate subnets for better security and manageability.

---

5. VPC Best Practices

1. **Use Private Subnets for Sensitive Resources**:
    - Place databases and application servers in private subnets to protect them from direct internet access.
2. **Use Security Groups and NACLs**:
    - Define specific rules to restrict traffic to/from instances and subnets based on the least privilege principle.
3. **Monitor Traffic with Flow Logs**:
    - Use **VPC Flow Logs** to capture and analyze network traffic for debugging, monitoring, and compliance purposes.
4. **Separate Network Layers**:
    - Divide your VPC into multiple subnets based on the roles of the resources (e.g., separate subnets for web servers, databases, etc.).
5. **Use VPC Peering for Inter-VPC Communication**:

Raj-Nathwani-Raj

    - Use VPC Peering to allow secure communication between different VPCs (e.g., between dev and prod environments).
6. **Enable DNS Resolution and Hostnames**:
    - Use DNS within your VPC to allow instances to resolve domain names without needing external DNS servers.

---

6. VPC Limitations

1. **VPC Peering Limitations**
    - VPC Peering has limits on the number of active peer connections (which can vary by region).
2. **IP Address Range**
    - A VPC has a maximum CIDR block size (a limit on the number of IP addresses available). Once exceeded, you can't add more.
3. **Route Tables**
    - There is a limit to the number of routes you can add to a route table, so careful planning is needed for large-scale deployments.
4. **NAT Gateway Costs**
    - NAT Gateways incur hourly and data processing charges, making them more expensive than using a simple NAT instance.

---

7. Conclusion

VPC is an essential part of AWS that provides control over your network configuration. It allows you to deploy and manage AWS resources securely, while offering flexibility in networking, routing, and resource management. By following best practices and ensuring proper segmentation and security, you can build highly available, scalable, and secure applications within AWS.

Raj-Nathwani-Raj

vpc Interview Question and Answers

1. What is an Amazon Virtual Private Cloud (VPC), and how do we use it in AWS?

Amazon VPC is like your private network inside AWS. It gives you full control over your cloud network. You can decide IP address ranges, create subnets, route traffic, and secure your resources.

We use VPC to launch AWS services like EC2, RDS, and Lambda in a secure and isolated environment. This helps protect our applications from unauthorized access and manage traffic flow better.

---

2. What are the key components of a VPC?

- **Subnets**: Smaller networks inside your VPC.
- **Route Tables**: Control traffic direction.
- **Internet Gateway (IGW)**: Lets instances connect to the internet.
- **NAT Gateway**: Allows private instances to access internet.
- **Security Groups**: Act like virtual firewalls for EC2.
- **Network ACLs (NACLs)**: Firewall for the whole subnet.
- **VPC Peering / Transit Gateway**: For connecting VPCs.
- **DHCP Option Set**: Assigns IP and DNS settings.
- **VPC Endpoints**: Connect to AWS services privately.

---

3. What is a subnet in VPC, and what are the different types of subnets?

A subnet is a small section of your VPC where you can place your resources.

- **Public Subnet**: Connected to internet through IGW. EC2s here can talk to internet.
- **Private Subnet**: No direct internet access. Used for databases or backend services.

---

4. Explain the purpose of Internet Gateway (IGW), NAT Gateway, and Route Table in a VPC.

- **Internet Gateway**: Lets EC2 instances in public subnet access internet.
- **NAT Gateway**: Lets private subnet instances access the internet **only for outbound** (like updates).
- **Route Table**: Tells the subnet where to send traffic (e.g., local, IGW, NAT).

---

5. What happens when you delete a VPC in AWS?

- All resources inside (subnets, gateways, route tables, etc.) get deleted.
- EC2 instances are terminated.
- Data in those instances will be lost unless backed up.
- You cannot recover the VPC once deleted.

---

6. Can you connect two VPCs together? How is it done?

Yes, using **VPC Peering** or **Transit Gateway**:

- VPC Peering creates a direct link between two VPCs.
- You must update route tables to allow communication.
- Works within same or different AWS accounts.

Raj-NathWani-Raj

7. What are the limitations or restrictions of VPC peering?

- No **transitive peering** (A–B and B–C doesn't mean A–C can talk).
- Cannot peer VPCs with **overlapping CIDR blocks**.
- Has **regional limitations** (use inter-region peering carefully).
- Need to manage **many connections** in large networks.

---

8. How can you secure a VPC and protect its resources?

- Use **Security Groups** to control EC2 traffic.
- Use **NACLs** for subnet-level traffic control.
- Enable **VPC Flow Logs** to monitor traffic.
- Place sensitive resources in **private subnets**.
- Use **IAM roles and policies** for access control.

---

9. What is the difference between Security Groups and Network ACLs in a VPC?

Feature	Security Group	Network ACL
Level	Instance level	Subnet level
Type	Stateful	Stateless
Rules	Allow only	Allow and Deny
Return Traffic	Automatically allowed	Must allow separately

Use SGs for EC2, NACLs for subnets.

---

10. What is DHCP (Dynamic Host Configuration Protocol) in a VPC?

DHCP automatically assigns:

- IP addresses
- DNS settings
- Domain names

In AWS, you can customize DHCP options for your VPC to use custom DNS servers.

Raj-Nathwani-Raj

---

11. Can you launch an EC2 instance without using a VPC?

No. Now all EC2 instances launch **inside a VPC**. AWS used to have EC2-Classic, but it is no longer supported.

Even if you don't create a VPC, AWS provides a **default VPC** in each region.

---

12. How does traffic from a private subnet reach the internet using a NAT Gateway?

1. EC2 in private subnet sends request to internet.
2. Traffic goes to **NAT Gateway** (in public subnet).
3. NAT Gateway forwards it to **Internet Gateway**.
4. Response comes back through NAT to EC2.

---

13. How do you design a VPC for fault tolerance and high availability?

- Use **multiple Availability Zones (AZs)**.
- Create subnets in **each AZ**.
- Use **Load Balancer** across AZs.
- Use **Auto Scaling Groups**.
- Put critical services in **private subnets**.
- Use **Route 53** for DNS failover.

---

14. What is a VPC endpoint, and what are the types: Interface Endpoint and Gateway Endpoint?

- **VPC Endpoints** allow private connection to AWS services without internet.

Types:

1. **Interface Endpoint**: ENI that connects to services like SSM, CloudWatch.
2. **Gateway Endpoint**: For S3 and DynamoDB. Added to route table.

---

15. How do you monitor traffic in a VPC?

- Enable **VPC Flow Logs**.
- Use **CloudWatch Logs**.
- Use **CloudTrail** to track API activity.
- Third-party tools like Datadog can help too.

Raj-Nathwani-Raj

16. How do you troubleshoot network connectivity issues in a VPC?

Check:

1. **Security Group rules**.
2. **NACL rules**.
3. **Route tables**.
4. **Is IGW or NAT present?**
5. **Check VPC Flow Logs**.
6. **Ping or curl** from EC2 to test.

---

17. Can a single VPC span across multiple AWS regions?

No. A VPC is **limited to one region**.

If you want to connect VPCs in different regions, use **inter-region VPC peering** or **Transit Gateway**.

---

18. What is a Transit Gateway, and how does it work in AWS networking?

- It's like a **central hub** for connecting multiple VPCs and on-prem.
- Supports **transitive routing**.
- Simplifies connections. No need for multiple peering links.
- Scalable and highly available.

---

19. How can you migrate resources from one VPC to another?

1. Create **AMI** of your EC2 and launch in new VPC.
2. Use **Snapshots** for volumes and RDS.
3. Move **Elastic IPs**, **Security Groups**, and other settings.
4. Use **Terraform or CloudFormation** to recreate architecture.

---

20. What is a CIDR block in a VPC, and how is it used?

CIDR (Classless Inter-Domain Routing) defines **IP range** of your VPC.

Example: 10.0.0.0/16 means 65,536 IPs. You divide this block into subnets.

---

21. What is the maximum number of subnets you can create in a VPC?

It depends on your CIDR block.

Raj-Nathwani-Raj

- A /24 subnet gives 256 IPs.
- You can create **up to 200 subnets** per VPC by default.

---

22. Can a subnet be placed in more than one Availability Zone?

No. A subnet is always limited to **one Availability Zone**. You must create multiple subnets (in different AZs) for high availability.

---

23. What happens if a subnet does not have a route to the internet?

- EC2 instances in that subnet **cannot access the internet**.
- Useful for **private or secure workloads** like databases.

---

24. If an EC2 instance in a private subnet cannot access the internet, what would you check?

1. Is **NAT Gateway** present?
2. Is **route table** sending traffic to NAT?
3. Is **Security Group** allowing outbound traffic?
4. Is **Subnet** in correct AZ?

---

25. How can two VPCs in different AWS regions communicate with each other?

Use:

- **Inter-region VPC Peering**
- **Transit Gateway** with inter-region support

Update **route tables and security groups** to allow communication.

---

26. How can a Lambda function access an RDS database located in a private subnet?

- Attach Lambda to the **same VPC and subnet** as RDS.
- Make sure **Security Group** of Lambda can connect to RDS port.
- No public internet is needed.

---

27. How can an EC2 instance and an RDS instance communicate privately within a VPC?

Raj-Nathwani-Raj

- Place both in **private subnets**.
- Allow EC2 in RDS **Security Group**.
- Ensure correct **route tables and NACLs**.

---

28. What happens if you accidentally delete the Internet Gateway from a public subnet?

- EC2 instances **lose internet access**.
- No outbound or inbound traffic from the internet.
- To fix, **recreate IGW** and attach to VPC again.

---

29. If VPC peering is configured but traffic is not flowing, what would you troubleshoot?

1. Check **route tables** in both VPCs.
2. Check **Security Groups and NACLs**.
3. Make sure **CIDR blocks don't overlap**.
4. Ensure **correct port access**.

---

30. How many Internet Gateways can be attached to a single VPC?

Only **one Internet Gateway** per VPC is allowed. You can't attach more than one.

---

31. What is the difference between VPC Peering and Transit Gateway?

- VPC Peering: Simple, 1-to-1 connection.
- Transit Gateway: Central hub for many VPCs.
- Peering doesn't support transitive routing; Transit Gateway does.

---

32. How does a VPC handle DNS resolution and hostname assignments?

- Uses built-in **Amazon DNS server**.
- EC2 gets **private and public DNS names**.
- Can use **Route 53 private hosted zones**.
- DHCP Option Set lets you customize DNS behavior.

---

33. Can you share subnets across AWS accounts? How is it done?

Yes, using **AWS Resource Access Manager (RAM)**:

Raj-Nathwani-Raj

1. Owner shares subnet using RAM.
2. Other account can launch resources into it.
3. Cannot delete or manage the VPC.

---

34. How can you connect an AWS VPC to an on-premise network?

Options:

1. **Site-to-Site VPN**: Quick, uses internet.
2. **AWS Direct Connect**: Private link, fast and reliable.
3. **Transit Gateway**: For many VPCs and networks.

Scenario-Based AWS VPC Interview Questions

Scenario 1: Public and Private Subnet Setup

This is a common setup where we divide a VPC into two subnets: public and private.

📌 **Situation:**

You want to host a web application. The web server (EC2) should be in the public subnet, and the database (RDS) should be in the private subnet for better security.

✅ **Steps:**

1. **Create a VPC – For example, 10.0.0.0/16.**
2. **Create two subnets:**
    - **Public subnet (e.g., 10.0.1.0/24)**
    - **Private subnet (e.g., 10.0.2.0/24)**
3. **Attach an Internet Gateway to the VPC.**
4. **Update route table of the public subnet:**
    - **Add a route to `0.0.0.0/0` via the Internet Gateway**
5. **Keep private subnet's route table empty for internet to block outside access.**
6. **Launch EC2 in public subnet for web server with a public IP.**
7. **Launch database (RDS) in private subnet, no public IP.**

Raj-Nathwani-Raj

🎯 **Benefit:**

- **Web server is accessible to the world.**
- **Database is secure, only reachable from inside the VPC.**

Scenario 2: Inter-VPC Communication

This scenario explains how two VPCs can talk to each other.

📌 **Situation:**

You have two applications in different VPCs (e.g., VPC-A and VPC-B) and they need to exchange data.

✅ **Solutions:**

1. **Use VPC Peering:**
    - **Create a peering connection between VPC-A and VPC-B.**
    - **Accept the peering request from the other side.**
    - **Add routes in both route tables to allow traffic.**
    - **Example: In VPC-A, route to VPC-B's CIDR via the peering connection.**
2. **Use Transit Gateway (if you have many VPCs):**
    - **Attach all VPCs to a Transit Gateway.**
    - **Manage routing centrally.**

❗ **Limitations with VPC Peering:**

- **No transitive routing (VPC-A can't reach VPC-C through VPC-B).**
- **CIDR blocks must not overlap.**

Scenario 3: Limiting Access Using Security Groups

This is about controlling which resources can talk to each other.

Raj-Nathwani-Raj

📌 **Situation:**

You want only one EC2 instance to access your RDS database. All other instances must be blocked.

✅ **Steps:**

1. **Create Security Group A for EC2 instance.**
2. **Create Security Group B for RDS.**
3. **In Security Group B (RDS):**
    - **Allow inbound access on port 3306 (MySQL) only from Security Group A.**
4. **Don't allow traffic from anywhere else.**

🎯 **Result:**

Only EC2 with Security Group A can access the database. Others are blocked, even if they are in the same subnet.

Scenario 4: EC2 in Private Subnet Needs Software Updates

Instances in private subnet can't access the internet directly. But sometimes, they need to download updates or install packages.

📌 **Situation:**

Your EC2 in private subnet needs to update software using internet (like `yum update`, `apt-get install`, etc.)

✅ **Solution:**

Use a NAT Gateway to give internet access outbound only.

1. **Create a NAT Gateway in public subnet.**
2. **Allocate and attach an Elastic IP to the NAT Gateway.**
3. **In the route table of the private subnet, add:**
    - **`0.0.0.0/0` route pointing to the NAT Gateway**

Raj-Nathwani-Raj

4. **EC2 instance can now send traffic to internet, but no one from internet can reach it.**

🎯 **Benefit:**

- **Software updates are possible.**
- **Still safe from outside attacks.**

Scenario 5: Application Fails to Connect to Database in Private Subnet

You deployed a web app, but it cannot connect to the backend database in the same VPC.

📌 **Possible Causes & Fixes:**

1. **Security Group Issue:**
    - **The RDS security group must allow inbound traffic from the EC2's security group on the correct port (e.g., 3306).**
2. **Subnet Routing:**
    - **Make sure both EC2 and RDS are in subnets with proper routes.**
    - **No special route is needed for communication inside a VPC, but subnets must not block internal traffic.**
3. **NACL (Network ACL):**
    - **Check if NACLs are blocking traffic between subnets. Allow rules should exist for required ports.**
4. **Database Endpoint:**
    - **Confirm that the EC2 is trying to connect to the correct RDS endpoint (hostname or IP).**
5. **DNS Resolution:**
    - **If DNS hostnames are disabled in the VPC, EC2 won't resolve RDS name. Enable DNS in VPC settings.**
6. **No Internet Required:**

Raj-Nathwani-Raj

- **Since both are in the same VPC, you don’t need Internet Gateway or NAT Gateway.**

🛠️ **Final Fix:**

- **Update security group rules.**
- **Double check subnet and route table.**
- **Check correct endpoint and port.**
- **Verify no firewall (NACL) is blocking.**

Raj-Nathwani-Raj