Interview Questions on Subnet Architecture

Q: What's the difference between public and private subnets?

Public vs Private Subnets Comparison

Aspect	Public Subnet	Private Subnet
Internet Access	Direct bidirectional internet access	No direct internet access
Route Table	Has route to Internet Gateway (0.0.0.0/0 → IGW)	Routes to NAT Gateway/Instance or VPC endpoints only
Internet Gateway	Directly connected to Internet Gateway	Not directly connected to Internet Gateway
Public IP Assignment	Resources can have public IP addresses	Resources only have private IP addresses
Inbound Traffic	Can receive inbound traffic from internet	Cannot receive inbound traffic from internet
Outbound Traffic	Direct outbound internet access	Outbound access via NAT Gateway/Instance
Security	More exposed to internet threats	More secure, isolated from direct internet access
Use Cases	Web servers, load balancers, bastion hosts	Databases, application servers, internal services
Cost Implications	Lower cost (no NAT Gateway needed)	Higher cost (requires NAT Gateway for internet access)
Visibility	Publicly accessible if security groups allow	Hidden from internet, only accessible internally
Common Resources	Public-facing web applications, CDNs	Backend databases, internal APIs, processing services

Q: What goes in each subnet type?

Public Subnet typically contains:

- Load balancers (Application Load Balancer, Network Load Balancer)
- Web servers that need direct internet access

- Bastion hosts for SSH access
- NAT Gateways (for private subnet internet access)

Private Subnet typically contains:
- Application servers
- Database servers
- Internal microservices
- Backend processing systems

Q: How should you place subnets across Availability Zones?
Think like a hospital system with multiple buildings:
Smart Design:
- Emergency Room in Building A (AZ-1a) AND Building B (AZ-1b)
- Operating Rooms in Building A AND Building B
- Patient Records accessible from both buildings
- If Building A loses power, Building B continues all operations

Poor Design:
- All Emergency Rooms only in Building A
- All Operating Rooms only in Building B
- If either building fails, critical services are unavailable

High Availability Pattern: Create at least one public and one private subnet in each AZ you're using (minimum of 2 AZs).
Example Structure:
- Public Subnet A (AZ-1a): 10.0.1.0/24
- Private Subnet A (AZ-1a): 10.0.2.0/24
- Public Subnet B (AZ-1b): 10.0.3.0/24
- Private Subnet B (AZ-1b): 10.0.4.0/24

This allows you to deploy load balancers, web servers, app servers, and databases across multiple AZs for redundancy.

Why can't I just put everything in one AZ?

Single AZ deployment creates a single point of failure. If that AZ experiences issues (power outage, network problems, hardware failures), your entire application becomes unavailable. Multi-AZ deployment ensures that if one AZ fails, your application continues running from other AZs.

Q: How do you plan subnet CIDRs within a VPC?
Analogy: Think of dividing a large office building into departments:
Your Building (VPC): 1000 total offices available (10.0.0.0/16 = 65,536 IPs)
Department Planning:
- Marketing Department: Offices 1-100 (10.0.1.0/24 = 256 IPs)
- Sales Department: Offices 101-200 (10.0.2.0/24 = 256 IPs)
- IT Department: Offices 201-300 (10.0.3.0/24 = 256 IPs)
- Leave Offices 301-1000 for future expansion

You must plan so no department overlaps with another, and leave room for growth.

VPC CIDR Example: 10.0.0.0/16 (provides 65,536 IP addresses)
Subnet Division Strategy:
Public Subnet AZ-A: 10.0.1.0/24 (256 IPs)
Private Subnet AZ-A: 10.0.2.0/24 (256 IPs)
Public Subnet AZ-B: 10.0.3.0/24 (256 IPs)
Private Subnet AZ-B: 10.0.4.0/24 (256 IPs)
Database Subnet AZ-A: 10.0.5.0/24 (256 IPs)
Database Subnet AZ-B: 10.0.6.0/24 (256 IPs)
Reserved for future: 10.0.7.0/24 - 10.0.255.0/24

Q: What's the math behind CIDR planning?
Technical: CIDR notation uses subnet masks to define network size:

- /16 = 65,536 IP addresses (16 bits for hosts)
- /24 = 256 IP addresses (8 bits for hosts)
- /25 = 128 IP addresses (7 bits for hosts)
- /26 = 64 IP addresses (6 bits for hosts)

AWS reserves 5 IP addresses in each subnet:

- First IP: Network address
- Second IP: VPC router
- Third IP: DNS server
- Fourth IP: Future use
- Last IP: Broadcast address

So a /24 subnet (256 IPs) actually has 251 usable IP addresses.

Q: Why is non-overlapping design critical?

Non-overlapping subnets ensure:

- Routing Clarity: Each IP address exists in exactly one subnet, so routing decisions are unambiguous
- Network Functionality: Overlapping subnets create routing conflicts and communication failures

Q: What are the rules for non-overlapping design?
Design Rules:

- Each subnet must have a unique CIDR block
- Subnet CIDRs must be subsets of the VPC CIDR
- No two subnets can have overlapping IP ranges
- Plan for future growth by reserving unused CIDR blocks

Example of Valid Design:
VPC CIDR: 10.0.0.0/16
Subnet 1: 10.0.1.0/24 (10.0.1.0 - 10.0.1.255)
Subnet 2: 10.0.2.0/24 (10.0.2.0 - 10.0.2.255)
Subnet 3: 10.0.3.0/24 (10.0.3.0 - 10.0.3.255)

What route tables control
Q: What exactly do route tables do?
Route tables are like GPS navigation systems for network traffic:

Think of a delivery company's routing system:

- Each delivery truck (data packet) has a destination address
- The dispatch system (route table) has a list of directions:
    - "For addresses 1000-1999: Take Highway 1"
    - "For addresses 2000-2999: Take Highway 2"
    - "For all other addresses: Take Main Street to the post office"
- Every truck checks the routing list before leaving the warehouse

Q: What information is stored in a route table?
Each route contains:

- **Destination**: CIDR block (e.g., 10.0.0.0/16, 0.0.0.0/0)
- **Target**: Where to send traffic (e.g., Internet Gateway, NAT Gateway, local)
- **Status**: Active or inactive
- **Propagated**: Whether the route was automatically added

VPC Configuration

- **VPC CIDR**: 10.0.0.0/16
- **Public Subnet**: 10.0.1.0/24
- **Private Subnet**: 10.0.2.0/24

Public Route Table

Destination	Target	Purpose
10.0.0.0/16	local	Internal VPC traffic
0.0.0.0/0	igw-1234567890abcdef0	Internet access via Internet Gateway

Associated Subnets: Public Subnet (10.0.1.0/24)

Private Route Table

Destination	Target	Purpose
10.0.0.0/16	local	Internal VPC traffic
0.0.0.0/0	nat-0987654321fedcba0	Internet access via NAT Gateway

Associated Subnets: Private Subnet (10.0.2.0/24)

Route Explanation

Local Route (10.0.0.0/16 → local)

- **Automatically created** for every route table in the VPC
- **Cannot be deleted or modified**
- Enables communication between all subnets within the VPC
- All traffic destined for VPC CIDR range stays within the VPC

Internet Gateway Route (0.0.0.0/0 → igw-xxx)

- **Default route** for internet-bound traffic
- Only present in **public subnet route tables**
- Enables direct internet access for resources in public subnets
- Requires resources to have public IP addresses

NAT Gateway Route (0.0.0.0/0 → nat-xxx)

- **Default route** for private subnet internet access
- Enables outbound internet access while maintaining privacy

- NAT Gateway typically resides in a public subnet
- Provides internet access without exposing private resources

Key Concepts

Route Priority

Routes are evaluated by **most specific match** (longest prefix match):

1. 10.0.1.5/32 (most specific)
2. 10.0.1.0/24
3. 10.0.0.0/16
4. 0.0.0.0/0 (least specific, default route)

Route Table Types

- **Main Route Table**: Default for all subnets not explicitly associated
- **Custom Route Table**: Created for specific routing requirements
- **Subnet Association**: Each subnet can only be associated with one route table

Common Targets

- **local**: VPC internal routing
- **igw-xxx**: Internet Gateway
- **nat-xxx**: NAT Gateway
- **vgw-xxx**: Virtual Private Gateway (VPN)
- **pcx-xxx**: VPC Peering Connection
- **eni-xxx**: Network Interface
- **i-xxx**: EC2 Instance

Q: What are default vs custom routes?

Analogy: Think of office building directory signs:

Default Routes = Standard Building Signage:

- "All offices 200-299: Take Elevator to Floor 2"
- "All offices 300-399: Take Elevator to Floor 3"
- These are automatically created when floors are built

Custom Routes = Special Direction Signs:

- "For VIP Conference Room: Take executive elevator"
- "For deliveries: Use service elevator to loading dock"
- "For emergencies: Exit via stairwell to parking garage"
- These are added based on special needs
-

Default Routes: Automatically created by AWS:

- Local route for VPC CIDR (e.g., 10.0.0.0/16 → local)
- Enables communication within the VPC

Custom Routes: Manually added routes:

- Internet access: 0.0.0.0/0 → Internet Gateway
- Private internet: 0.0.0.0/0 → NAT Gateway
- Cross-VPC: 172.16.0.0/16 → VPC Peering Connection
- On-premises: 192.168.0.0/16 → VPN Gateway

Q: Can I modify or delete default routes?

The local route for your VPC CIDR cannot be modified or deleted - it's automatically managed by AWS. You can add custom routes and modify the main route table, but the local route always remains to enable intra-VPC communication.

Relationship between subnets and route tables

Q: How do subnets and route tables work together?

Route Table Association: Each subnet must be associated with exactly one route table. Multiple subnets can share the same route table if they need identical routing behavior.
Inheritance: If you don't explicitly associate a subnet with a route table, it uses the VPC's main route table by default.

Q: What are common route table patterns?

Common Patterns:

- Public Route Table: Shared by all public subnets, contains route to Internet Gateway
- Private Route Table: Shared by private subnets, contains route to NAT Gateway
- Database Route Table: For database subnets, may have no internet access routes
- Custom Route Tables: For specific routing requirements (VPN, peering, etc.)

Route priority and longest prefix matching

Q: How does routing decide which path to take when multiple routes match?

Analogy: Think of address matching for package delivery:
A package addressed to "123 Oak Street, Springfield, Illinois, USA" matches multiple delivery rules:

- Rule 1: "All USA packages → Main distribution center" (broad match)
- Rule 2: "All Illinois packages → Chicago hub" (more specific)
- Rule 3: "All Springfield packages → Local depot" (most specific)
- Rule 4: "123 Oak Street → Direct delivery" (exact match)

The delivery system chooses Rule 4 because it's the most specific match.

Longest prefix matching means the route with **the most specific (longest) network** prefix wins:
Route Priority Example:
Routes in table:
- 0.0.0.0/0 → Internet Gateway (matches everything)
- 10.0.0.0/16 → Local (matches VPC traffic)
- 10.0.1.0/24 → NAT Gateway (matches specific subnet)
- 10.0.1.100/32 → VPC Endpoint (matches specific IP)

For destination 10.0.1.100, the /32 route wins because it has the longest prefix (most specific match).

Q: What happens if two routes have the same prefix length?

AWS uses a priority order when prefix lengths are equal:

1. Local routes (highest priority)
2. Static routes (manually added)
3. Propagated routes (from VPN/Direct Connect)

Within the same category, AWS may use other factors or load balance, but this scenario is rare in practice.

9. Internet Connectivity Components

Internet Gateway (IGW) - what it does

Q: What exactly does an Internet Gateway do?

An Internet Gateway (IGW):

- Enables Internet Access: Provides a connection between your VPC and the internet, allowing bidirectional communication
- Highly Available: Redundant and highly available by design - AWS manages the availability
- Stateless: Simply routes traffic and performs NAT - doesn't maintain connection state

Q: How many Internet Gateways can I attach to a VPC?

Each VPC can have only one Internet Gateway attached at a time. However, you can detach an IGW from one VPC and attach it to another. The IGW itself can only be attached to one VPC at a time.

Q: What's required for an instance to access the internet through an IGW?

For internet access via IGW, an instance needs:

1. A public IP address or Elastic IP address
2. Be in a subnet with a route to the Internet Gateway (0.0.0.0/0 → IGW)
3. Security groups and NACLs must allow the desired traffic
4. The instance's operating system must be configured to use the traffic

NAT Gateway/Instance for private subnet internet access

Q: Why do private subnets need NAT Gateways?

Analogy: Think of NAT Gateway like a personal shopping service for hotel guests:

Hotel Scenario:

- VIP guests (private subnet resources) want to stay completely private
- They don't want to go shopping themselves (no direct internet access)
- They call concierge service (NAT Gateway) with shopping requests
- Concierge goes out to stores (internet), buys items, brings them back
- Stores never see or interact with the VIP guests directly
- Guests get what they need, but maintain complete privacy
-

NAT Gateway provides:

- Outbound Internet Access: Allows private subnet resources to initiate connections to the internet (for updates, API calls, etc.)
- Inbound Protection: Internet cannot initiate connections to private resources - only outbound connections are allowed
- Network Address Translation: Translates private IP addresses to the NAT Gateway's public IP for outbound traffic
- High Availability: AWS-managed service that's highly available within an AZ

Q: What's the difference between NAT Gateway and NAT Instance?

NAT Gateway:

- AWS-managed service
- Higher performance (up to 45 Gbps)
- Automatic failover within AZ
- No security groups (uses NACLs only)
- More expensive but less management overhead

NAT Instance:

- Self-managed EC2 instance
- Performance depends on instance type
- Manual failover configuration required

- Can use security groups
- Lower cost but requires more management

Q: Where should I place NAT Gateways for high availability?

For high availability, deploy one NAT Gateway in each AZ where you have private subnets. Configure route tables so that private subnets route to the NAT Gateway in the same AZ. This ensures that if one AZ fails, private subnets in other AZs can still access the internet.

How routing determines internet accessibility

Q: How do route tables determine if a subnet can access the internet?

Technical: Internet accessibility is determined by route table entries:

Public Subnet Route Table:

Destination Target

10.0.0.0/16 Local (VPC traffic stays local)

0.0.0.0/0 IGW-xxxxx (Internet traffic goes to IGW)

Private Subnet Route Table:

Destination Target

10.0.0.0/16 Local (VPC traffic stays local)

0.0.0.0/0 NAT-xxxxx (Internet traffic goes to NAT Gateway)

Isolated Subnet Route Table:

Destination Target

10.0.0.0/16 Local (Only VPC traffic allowed)

Q: What determines the type of internet connectivity?

The presence and target of the 0.0.0.0/0 route determines internet connectivity type:

- IGW target = bidirectional internet access (public)
- NAT target = outbound-only internet access (private)
- No 0.0.0.0/0 route = no internet access (isolated)

Q: Can I change a subnet from public to private?

Yes, you can change subnet types by modifying the route table association:

- To make public subnet private: Associate it with a route table that routes 0.0.0.0/0 to NAT Gateway instead of IGW
- To make private subnet public: Associate it with a route table that routes 0.0.0.0/0 to IGW instead of NAT Gateway
- Remember that instances also need appropriate IP addresses (public/private) to function correctly

1. Which of the following subnets requires a NAT Gateway or NAT Instance to access the internet?

A. Public Subnet

B. Private Subnet

C. Default Subnet

D. DMZ Subnet

✅ **Answer:** B

---

2. What does the CIDR block 0.0.0.0/0 represent in a route table?

A. Only internal AWS traffic
B. All private IP addresses
C. All traffic to the internet
D. VPC-local traffic

✅ **Answer:** C

---

3. What is the difference between a NAT Gateway and a NAT Instance?
A. NAT Gateway is cheaper than NAT Instance
B. NAT Instance provides automatic scaling
C. NAT Gateway is a managed service, whereas NAT Instance is self-managed
D. NAT Gateway can be used for inbound traffic

✅ **Answer:** C

---

4. How do you make a subnet public in AWS?
A. Assign an Elastic IP to each instance
B. Attach a NAT Gateway
C. Associate a route table that routes 0.0.0.0/0 to an Internet Gateway
D. Launch instances with public AMIs
✅ **Answer:** C

---

5. What happens if a private subnet does NOT have access to a NAT Gateway or NAT Instance?
A. Instances can access the internet
B. Instances can access only VPC-local and internal services
C. Instances become public automatically
D. The subnet is converted into a public subnet
✅ **Answer:** B