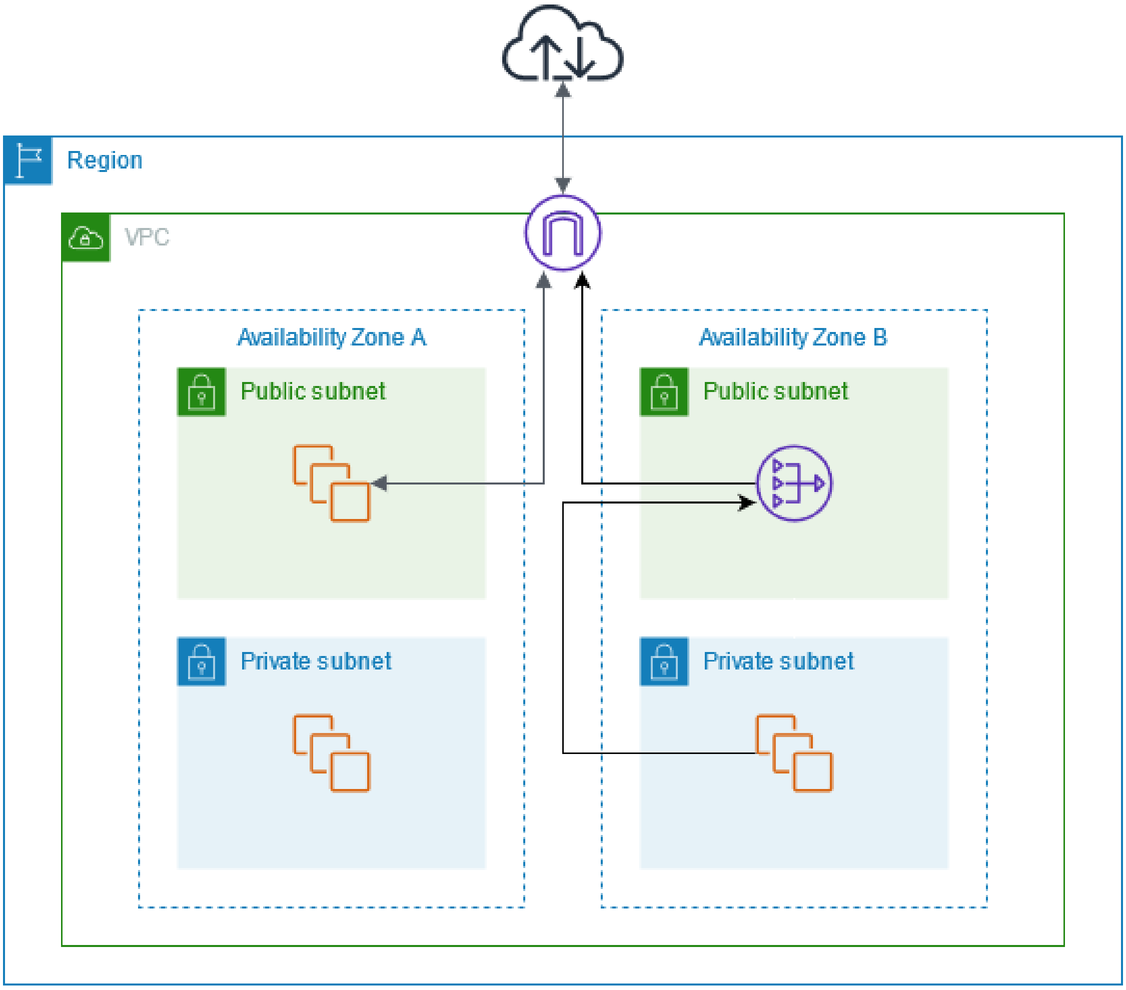
AWS VPC Route Tables - Questions and Answers

Q: What do route tables control in AWS VPC?

- Control network traffic routing within a VPC
- Determine where packets are sent based on destination IP
- Act as routing rules for subnet traffic
- Direct traffic to gateways, interfaces, or connections



Q: What's the difference between default routes and custom routes?

Default Routes:

- Automatically created by AWS
- Cannot be deleted
- Local route enables VPC internal communication
- Main route table comes with every VPC

Custom Routes:

- User-defined routing rules
- Route to Internet Gateway (0.0.0.0/0)
- Routes to NAT Gateways for private subnets
- Routes to VPN/VPC Peering connections
- Routes to Transit Gateways
-

Q: How do subnets relate to route tables?

- Each subnet associates with exactly one route table
- One route table can serve multiple subnets
- New subnets use main route table by default
- Can explicitly associate subnets with custom route tables
- Public subnets typically use tables with internet gateway routes
- Private subnets use tables with NAT gateway routes

Q: How do route priority and longest prefix matching work?

Priority Order:

1. Local routes (VPC CIDR) - highest priority
2. Longest prefix match - more specific routes win
3. Propagated routes (VPN/Direct Connect)
4. Static routes
5. Default route (0.0.0.0/0) - lowest priority

Example:

- 10.0.0.0/16 (local)
- 10.0.1.0/24 → NAT Gateway
- 0.0.0.0/0 → Internet Gateway
- Traffic to 10.0.1.50 uses NAT Gateway (/24 most specific)

CIDR Blocks and Routing Example:

Suppose you are working inside an AWS **VPC** with the following:

- **VPC CIDR**: 10.0.0.0/16 → The overall private network space.
- **Subnet CIDR**: 10.0.1.0/24 → A specific subnet (could be private).
- You have route table entries like:
    1. 10.0.0.0/16 → **local** (default for internal communication)
    2. 10.0.1.0/24 → **NAT Gateway** (used for private subnet to access internet)
    3. 0.0.0.0/0 → **Internet Gateway** (used for public subnet internet access)

Key Concepts:

CIDR Match Specificity

When multiple routes could apply to a destination IP, **the most specific route wins**, i.e., the one with the **longest prefix match** (smallest subnet).

CIDR	Prefix Length	Specificity
10.0.0.0/16	16 bits	less specific
10.0.1.0/24	24 bits	**more specific**

💡 **Routing Scenario:**
🗒 **Route Table:**

Destination	Target
10.0.0.0/16	local
10.0.1.0/24	NAT Gateway
0.0.0.0/0	Internet Gateway

Now, traffic is going to → 10.0.1.50
Let's see what happens:

1. 10.0.1.50 falls under:
   - 10.0.0.0/16 ✅
   - 10.0.1.0/24 ✅
2. **Both routes match**, but:
   - /24 is **more specific** than /16
3. So traffic to 10.0.1.50 uses the **NAT Gateway**, not local routing.

Q: What does an Internet Gateway (IGW) do?

- Provides internet access to VPC resources
- Horizontally scaled, redundant, and highly available
- Performs one-to-one NAT for instances with public IPs
- Allows bidirectional internet communication
- Must be attached to VPC to function
- Only one IGW per VPC allowed
- No bandwidth constraints or availability risks
- Free of charge (no additional costs)
- Both way

Q: What are NAT Gateway/Instance for private subnet internet access?

NAT Gateway:

- AWS-managed service for outbound internet access
- Allows private subnet resources to reach internet
- Blocks inbound connections from internet
- Highly available within single AZ
- Supports IPv4 traffic only
- Scales automatically up to 45 Gbps
- Charged hourly plus data processing fees
- Only outbound

NAT Instance:

- EC2 instance configured for NAT functionality
- User-managed alternative to NAT Gateway
- Requires manual scaling and availability management
- Can use security groups
- Supports port forwarding
- Less expensive but more management overhead
- Can become single point of failure

Q: How does routing determine internet accessibility?

Public Subnet Internet Access:

- Route table has 0.0.0.0/0 → Internet Gateway
- Instance needs public IP or Elastic IP
- Security groups allow required traffic
- NACLs permit traffic flow

Private Subnet Internet Access:

- Route table has 0.0.0.0/0 → NAT Gateway/Instance
- NAT device sits in public subnet
- NAT device has route to Internet Gateway
- Only outbound internet connections allowed
- No direct inbound access from internet

Routing Requirements:

- Default route (0.0.0.0/0) must point to appropriate gateway
- Local routes handle VPC internal traffic
- Most specific route wins (longest prefix matching)
- Missing internet route = no internet access
- Route propagation affects traffic flow

Q1. What is the main function of a route table in a VPC?

A. Encrypt data before transmission
B. Determine where network traffic is directed
C. Assign IP addresses to EC2 instances
D. Monitor VPC traffic logs

✅ **Correct Answer:** B

Q2. What is the default route in a VPC used for local communication?

A. 0.0.0.0/0
B. 127.0.0.1
C. 10.0.0.0/8
D. local
✅ **Correct Answer:** D

Q3. One subnet can be associated with how many route tables at a time?

A. Only one

B. Multiple
C. Zero
D. Depends on region
✅ **Correct Answer:** A

Q4. What is the purpose of an Internet Gateway (IGW) in AWS VPC?
A. To connect private subnets to the internet
B. To enable EC2 instances in public subnets to communicate with the internet
C. To monitor internal VPC traffic
D. To manage VPN connections
✅ **Correct Answer:** B

Q5. Which route must be present in the route table for internet access via IGW?
A. 192.168.0.0/16 → IGW
B. 0.0.0.0/0 → Internet Gateway
C. 10.0.0.0/16 → local
D. 172.31.0.0/16 → NAT
✅ **Correct Answer:** B

Q6. Can an Internet Gateway be attached to more than one VPC at a time?
A. Yes
B. No

✅ **Correct Answer:** B

Q7. What does a NAT Gateway allow instances in a private subnet to do?
A. Accept inbound traffic from the internet
B. Communicate with the internet for outbound traffic
C. Host websites
D. Get dynamic Ips

✅ **Correct Answer:** B

Q8. Where must a NAT Gateway be deployed?
A. In the private subnet
B. In the same subnet as the EC2 instance
C. In a public subnet with a route to IGW
D. Anywhere in the VPC

✅ **Correct Answer:** C

Q9. Which route configuration allows private subnet instances to use a NAT Gateway?
A. 0.0.0.0/0 → IGW
B. 0.0.0.0/0 → NAT Gateway
C. 10.0.0.0/16 → NAT Gateway
D. None of the above

✅ **Correct Answer:** B