Q: What happens if two VPCs have overlapping CIDR ranges?

Overlapping VPC CIDRs Example

VPC Name	CIDR Block	Notes
VPC-A	10.0.0.0/16	Covers 10.0.0.0 – 10.0.255.255
VPC-B	10.0.1.0/24	Covers 10.0.1.0 – 10.0.1.255 (overlaps with VPC-A)

Why is this a problem?

- You **cannot create VPC peering** or **Transit Gateway routing** between overlapping CIDRs.
- IP conflicts occur, causing **routing ambiguity** and **connectivity failure**.
- You will get errors during setup in AWS (e.g., "overlapping CIDRs not allowed").

Direct Impact:

VPC Peering Limitations:

- Cannot create VPC peering connection between overlapping VPCs
- AWS rejects peering requests for overlapping CIDR blocks
- No direct communication possible between these VPCs
- Must use alternative connectivity methods

Transit Gateway Restrictions:

- Cannot attach VPCs with overlapping CIDRs to same Transit Gateway
- Routing conflicts prevent proper traffic forwarding
- Network isolation enforced by AWS

(Note: A Transit Gateway acts as a **central network hub that connects your VPCs and on-premises networks to a single gateway**, simplifying network management and scaling. A Transit Gateway acts as a **central network hub that connects multiple VPCs and on-premises networks**, simplifying network management and enabling transitive routing.)

VPN/Direct Connect Issues:

- Routing conflicts in hybrid cloud scenarios
- Cannot advertise overlapping routes
- Traffic routing becomes unpredictable
- May cause connectivity failures

Workaround Solutions:

NAT Gateway Translation:

- Use NAT Gateway for one-way communication
- Translate source IP addresses
- Limited functionality compared to direct peering
- Additional complexity and costs

Application Load Balancer:

- Use ALB as intermediary between VPCs
- Route traffic through load balancer
- Works for HTTP/HTTPS traffic only
- Adds latency and costs

AWS PrivateLink:

- Create VPC endpoints for service communication
- Works with specific AWS services
- Avoids IP address conflicts
- Service-specific solution

Proxy/Bastion Hosts:

- Deploy proxy servers in non-overlapping subnets
- Route traffic through proxy instances
- Manual configuration required
- Additional management overhead

Prevention Best Practices:

- Plan CIDR blocks before VPC creation
- Document IP allocation across organization
- Use centralized IP address management
- Reserve non-overlapping ranges for each team/project
- Consider future connectivity requirements during planning

Q1: What is a major issue caused by overlapping CIDR ranges between two AWS VPCs?

A. Increased storage cost
B. Duplicate IAM roles
C. IP address conflicts and routing ambiguity
D. Reduced compute performance

✅ **Answer: C. IP address conflicts and routing ambiguity**

Q2: Which of the following AWS features will NOT work if two VPCs have overlapping CIDR ranges?

A. EC2 Auto Scaling
B. VPC Peering
C. IAM Role switching
D. S3 Bucket Access

✅ **Answer: B. VPC Peering**